

FOUNDATIONS  
OF THE  
THEORY  
OF  
ALGEBRAIC  
NUMBERS

HANCOCK

Vol. I

MACMILLAN



HIRSCHWALDSCH  
BUCHHANDLUNG  
BERLIN NW 7  
UNTER DEN LINDEN 68

[www.rcin.org.pl](http://www.rcin.org.pl)



16 - 1932  
III

S. Kichetecy







FOUNDATIONS OF THE  
THEORY OF ALGEBRAIC NUMBERS

GABINET MATEMATYCZNY  
Towarzystwa Naukowego Warszawskiego





THE MACMILLAN COMPANY  
NEW YORK • BOSTON • CHICAGO • DALLAS  
ATLANTA • SAN FRANCISCO

MACMILLAN & CO., LIMITED  
LONDON • BOMBAY • CALCUTTA  
MELBOURNE

THE MACMILLAN COMPANY  
OF CANADA, LIMITED  
TORONTO



uw

Kat.

# FOUNDATIONS OF THE THEORY OF ALGEBRAIC NUMBERS

BY

HARRIS HANCOCK, PH.D. (Berlin), DR.SC. (Paris),

PROFESSOR OF MATHEMATICS IN  
THE UNIVERSITY OF CINCINNATI

VOLUME I

INTRODUCTION TO THE GENERAL THEORY

PUBLISHED WITH THE AID OF  
THE CHARLES PHELPS TAFT MEMORIAL FUND  
UNIVERSITY OF CINCINNATI

~~GABINET MATEMATYCZNY  
Towarzystwa Naukowego Warszawskiego~~

~~L. inw. 656~~

New York

THE MACMILLAN COMPANY

1931

opis nr. 46878

COPYRIGHT, 1931,  
BY THE BOARD OF DIRECTORS  
OF THE UNIVERSITY OF CINCINNATI

---

All rights reserved—no part of this book may be reproduced in any form without permission in writing from the publisher, except by reviewers who wish to quote brief passages in connection with a review written for inclusion in magazines or newspapers.

---

Set up and printed.  
Published December, 1931.



4656/i

SET UP AND PRINTED BY THE LANCASTER PRESS, INC.  
PRINTED IN THE UNITED STATES OF AMERICA



## INTRODUCTION

The purpose of the present treatise is to offer an approach to a higher and more generalized arithmetic through a systematic study of the algebraic numbers. By virtue of the simplicity of its foundations and the rigor of its deductions, arithmetic stands alone in the beauty and harmony of its truths. A divine gift, it offers proof that the mind is a reality attested by the sciences on the one hand, and the philosophies on the other. The province of arithmetic in this high position between science and philosophy, is both to serve and to be served in the quest of higher truths.

The earlier investigators in the theory of numbers made the rational integer the basis of their endeavor and, resting upon this foundation, their theories were advanced in a remarkable manner to very great heights. These heights naturally become the more elevated, the broader and wider the bases are made. The present work proposes to show how the field of rational numbers is broadened by the introduction of the algebraic numbers and how thereby the realm of rationality is extended. In this "widening of the field of arithmetic" by the introduction of algebraic quantities, by the employment of rational functions of algebraic quantities, and similar extensions, many difficulties have been encountered and, in particular, difficulties that are found in the treatment of the algebraic numbers themselves. In connection with the overcoming of these difficulties and smoothing the paths of ascent, whether it be to a higher number theory or to a more exact science, or to a deeper and purer phi-

losophy, it is the part of the expositor to exhibit the power of a generalized arithmetic in its simplicity, its rigor, its harmony, and its charm. As indicated in the beginning, the purpose of this treatise is to help in making the theory of algebraic numbers more accessible, more attractive, and less difficult.

Soon after the introduction of the algebraic numbers as a study in themselves by Gauss, Jacobi, and others, a serious difficulty appeared in that, unlike the rational integers, they did not admit a *unique* factorization. This very perplexing condition was later overcome in part by Kummer's discovery of the *ideal numbers*, which, although of a somewhat fictitious nature, are *not* "mere fiction." As Kummer would express it, they are like certain chemical compounds which have their reality in their combinations. There exists here a marked analogy with Plato's "doctrine of idea and number" which must again give new thought to the modern philosopher.

In mathematics these ideal numbers served as a starting point for the remarkable discoveries made by two of Kummer's followers: Dedekind, on the one hand, with the theory of moduls and ideals; Kronecker, on the other, with the methodical use (employ) of the theory of forms with indeterminate coefficients and of the modular systems. The exploitation of these two great theories is in the main the object of the present work.

The author had the good fortune, while a student in the University of Berlin, to hear the lectures of Frobenius on the Dedekind Theory and those of Kronecker, the last he ever gave, on his own work. Every method known to the author has been used to simplify the exposition which often involved proving anew fundamental theorems and formulas as they arose. If he has inadvertently made omissions and inaccuracies, it is hoped that the general



theory follows in such form that the reader can supply the defects. As an example of these difficulties, Dedekind himself declared that there always seemed to him to be a gap (*Lücke*) or at least a questionable point (*zweifelhafte Stelle*) in the foundation of the theory of ideals as given by Kronecker in his *Grundzüge*. It may be proved, however, that by the introduction of a fifth postulate (in addition to Dedekind's four), the difficulty is obviated. This fifth postulate is the generalized Gaussian Lemma, proved independently by Kronecker, Dedekind, Hurwitz, and others.

A central point of both the Kronecker and Dedekind theories is found in the treatment of the divisors of the discriminant. Here again exceptional cases arose which were of an exceedingly baffling nature. Both Kronecker and Dedekind wished to establish a theorem by means of which a certain conformity between the ideal divisors of a prime integer  $p$  on the one hand, and the factorization of a fixed rational integral function, modulo  $p$ , on the other, was set forth. This theorem proved by Kummer for the case of cyclotomic realms was conjectured by him to be the key to the general theory. It was found, however, that this conformity fails when  $p$  is a so-called irregular divisor of the discriminant. If one considers only the algebraic numbers themselves and applies the highest scientific method in their handling, as was done by Dedekind, there remain lurking difficulties. Such and other obstacles impeded the publication of Kronecker's *Grundzüge* and were the subject of repeated notes in the *Göttingen Abhandlungen* by Dedekind.

These difficulties were finally overcome by Hensel, who, by the introduction of the "fundamental form" and the "fundamental equation" of Kronecker, proved in their generality certain theorems which Dedekind found

necessary for a satisfactory exposition of his theory. In this treatment, the modular systems of Kronecker render a valuable if not indispensable service. It is fortunate that for the most part the difficulties found in the Dedekind theory are different from those of the Kronecker theory, so that a combination of the two gives a satisfactory exposition of the whole. Thus, through the united efforts of two of the world's greatest mathematicians was the theory of algebraic numbers established upon a firm basis, free from defect.

It is here presented from a heuristic point of view with the hope that through this mode of treatment the innate relation of the general number theory to the function theory, algebra, algebraic (Abelian) integrals, and other branches of mathematics will be further developed and eventually generalized into a united arithmetized entity, the one contributing to the advancement of the other. Thus would Kronecker's belief be realized, a belief that is cherished by others in increasing numbers. In this realization, mathematics becomes as much the philosophy of thought as an apparatus of computation and thus too the confines of philosophy may in their turn be extended into something like an exact science. This generalized theory, while reaching to the highest arithmetical heights, becomes a profound mathematical-philosophical study, and its application to the sciences, as in the case of a related mathematical theory in Einstein's work, is a natural consequence. A similar theory emanating from an extended philosophic study which had its initial conception in something similar to Plato's doctrine of idea and number, if applied to mathematics, might conceivably lead to analogous results.

The Dedekind theory was systematically worked out by Dedekind and, difficult though it be even in his final



presentation, the extent of the ideas which he wished to convey may be fathomed. Further advances in his work seem possible in many directions. Kronecker, a man of independent fortune, had little experience as a lecturer. As he wrote no text-book, his work, while more comprehensive than Dedekind's and possibly susceptible of vast extensions, remains to be put in systematic form with an emphasis upon the clarity of its exposition.

The present work, while it follows more closely the Dedekind treatment which is purely arithmetical, sets forth the final fundamental results from both these entirely different standpoints, in that the ideals and moduls of Dedekind are put in juxtaposition with the fundamental forms and equations of Kronecker, the discriminant and order-modul being their common vantage ground. And thus it is brought about that the "methodical means of help derived from the indeterminate coefficients" with an intermingling of functions of many variables, does not appear foreign in a subject where the pure number concept is paramount. While the Dedekind theory is presented in its entirety, the Kronecker theory is everywhere emphasized. If this has been done effectually, it will appear that the work of even so great a mathematician as Hurwitz adds but little that is new to the subject. His contributions, which are given in a separate chapter, offer a synoptic review of many of the previous results.

The classic theory of quadratic realms, interesting and instructive in themselves, serves as a stepping stone from the usual theory of rational integers to the general theory of algebraic numbers. This theory, founded upon the lectures of Hilbert, has been thoroughly worked over by Reid, *The Elements of the Theory of Numbers*, and by Sommer, *Vorlesungen über Zahlentheorie*. Their results

are incorporated in and form a part of the first volume. This volume is intended as an introduction to the general theory which is given in the second volume. The reader, having acquired through the study of the quadratic realms the meaning and significance of such terms as norms, units, moduls, ideals, divisibility, unique factorization, etc., will naturally wish to see this theory extended to wider fields of investigation in the more general realms of rationality. Accordingly, the second volume is devoted to the presentation of this general theory.

The author has inserted in the text many historical notes and references which may be of service for those who wish to go deeper into the subject, as well as for university students who may be required to make reports on particular phases of the work. For this purpose frequent references are also made to the works mentioned below, which give a very exhaustive history of the subject: "Report on the Theory of Numbers" by H. J. S. Smith, *Collected Works*, Vol. I, pp. 38-364; *History of the Theory of Numbers*, in three volumes, by L. E. Dickson (Carnegie Institution, Washington, D. C.); Appendix to David Hilbert's *Die Theorie der algebraischen Zahlkörper*, *Deutsche Math. Vereinigung*, Vol. 4, Berlin, 1897. The latter report was brought up to date (1923) with the inclusion of omissions, in a supplementary *Report on Algebraic Numbers* (The National Academy of Sciences, Washington, D. C.) by Professors Dickson, Mitchell, Vandiver, and Wahlin.

The subject matter of the first volume is found in the Table of Contents, which follows.

I wish to express to The Macmillan Company and to their able representative, Mr. F. T. E. Sutphen, my appreciation of their uniform courtesy from the reading of the manuscript to its execution in book form.



I offer my profound thanks to Professor William T. Semple, to Mrs. Louise Taft Semple, and to the other members of the Charles Phelps Taft Memorial Fund for bearing the entire expense of the publication of this work and for their interest in the Department of Mathematics in the University of Cincinnati.

HARRIS HANCOCK.

CINCINNATI, OHIO,  
November, 1931.



# TABLE OF CONTENTS

## CHAPTER I

### PRELIMINARY NOTIONS

ARTICLE		PAGE
1.	Reducible and Irreducible Functions . . . . .	1
2.	Realms or Domains . . . . .	1
3.	Congruence of Two Functions with Respect to a Modulus . . . . .	2
4.	The Gaussian Lemma . . . . .	3
5-7.	Primitive Functions; Divisors . . . . .	4
8.	Theorem Regarding the Factors of an Integral Func- tion . . . . .	6
9-10.	Theorems Regarding Functions with Integral Coeffi- cients, Where the Coefficient of the Highest Power of $x$ Is Unity . . . . .	6
11-12.	The Irreducibility of Certain Functions . . . . .	9
13.	Schönemann's Theorem . . . . .	11
14-17.	Algorithm of the Greatest Common Divisor . . . . .	12
18.	Lagrange's Interpolation Formula . . . . .	15
19-21.	The Resultant of Two Integral Functions . . . . .	16
22.	The Discriminant $\Delta$ . . . . .	18
23.	An Interesting Form for $\Delta$ . . . . .	19
24.	The Factorization of a Rational Integer Is Unique..	20
25.	A Theorem in Rational Integers . . . . .	22
26.	A Fundamental Theorem in Linear Forms. The Minkowski Theorem. Hilbert's Proof . . . . .	22
27.	Hurwitz's Proof of This Theorem . . . . .	31

## CHAPTER II

### THE GENERAL NOTION OF REALMS OF RATIONALITY

28.	Functions Irreducible in One Realm, Reducible in Another . . . . .	37
29.	Definitions: Realms of Integrity. Prime Functions.	40



ARTICLE		PAGE
30.	Divisibility of a Function $f(x, u)$ by a Prime Function $P(u)$ .....	42
31.	If the Product $f(x, u) g(x, u)$ of Two Integral Functions in $x$ and $u$ is Divisible by a Prime Function $P(u)$ , One of the Functions Is Divisible by $P(u)$ .	42
32-3.	Divisors of Functions. Primitive Functions. Their Properties. Fundamental Theorems .....	43
34-5.	Further Theorems Regarding Divisibility by Prime Functions .....	46
36.	Functions That Are Relatively Prime. Primitive Functions in Several Variables. The Factorization of a Function Into Its Irreducible Factors...	48
37.	The Greatest Common Divisor .....	49
38.	The Reduction of a Function into Its Irreducible Factors .....	49
39.	A Function Which Has a Root in Common with an Irreducible Function Is Divisible by the Latter..	52
40-1.	Theorems Regarding the Roots of Irreducible Equations .....	52

## CHAPTER III

## ALGEBRAIC REALMS OF RATIONALITY

42.	Stock Realms. References to Hermite, Cantor, and Lindemann .....	55
43.	Algebraic Quantities. Their Conjugates. The Realm $\Re(x)$ , Where $x$ Is an Algebraic Number .....	55
44.	Adjunction of Algebraic Quantities to Stock Realms. Expression for All Quantities of $\Re(x)$ .....	56
45.	Conjugate Realms. A Realm That <i>Contains</i> Another Realm .....	57
46-9.	The Greatest Common Divisor and the Least Common Multiple of Realms. Galois Realms. Normal Realms .....	58
50.	Proof of an Important Theorem by Weber .....	62
51.	Theorem Expressed in the Formula $\Re(x, y) = \Re(t)$	63
52.	Another Proof .....	64
53.	The <i>Norm</i> of a Realm $\Re(x)$ . Further Theorems Re-	

# TABLE OF CONTENTS

XV

ARTICLE		PAGE
	garding Normal or Galois Realms. Theorems of Gauss, Abel, and Kummer.....	66
54.	Further Developments of the Idea of Algebraic Realms. Linearly Independent Quantities.....	68
55.	A Criterion for the Same.....	69
56.	Theorems in Determinants.....	70
57.	Further Definition of Algebraic Realms.....	71
58-9.	The Spur and the Norm of an Algebraic Number...	73
60.	Finite Realms of Rationality. Algebraic Realms from Another Point of View.....	76
61.	Primitive Quantities Determine Their Realms of Rationality. Kronecker's "Gattung".....	77
62.	The <i>Basis</i> of a Realm. Its Properties. Coördinates of a Number.....	79
63-4.	The Discriminant of $n$ Quantities; Properties of the Same.....	80
65-9.	Divisors of Realms of Rationality.....	83
70.	An Algebraic Realm Has Only a Finite Number of Divisors.....	88
71.	Divisor Realms.....	89
72-4.	Realms Reduced with Respect to a More General Realm than the Stock Realm.....	89
75.	The Greatest Common Divisor of Two Realms....	92
76.	Important Property of Normal or Galois Realms...	93
77-8.	The Relative Equality of Two Realms.....	95
79.	The Norm of a Realm Defined: The Norm of the Product of Several Realms.....	96
80.	The L. C. M. and G. C. D. of Normal Realms Are Normal Realms.....	99
81.	Simple Realms. A Connected Chain of Normal Divisors.....	100
82-3.	Such a Chain Is Unique. Theorem of Camille Jordan.....	101
84.	Fundamental Theorem Due to Galois.....	104
85.	Cubic Realms of Rationality.....	105
86.	Biquadratic Realms.....	107

## CHAPTER IV

## ALGEBRAIC INTEGERS

ARTICLE		PAGE
87.	Algebraic Numbers. Algebraic Integers . . . . .	110
88.	Reproduced through Addition, Subtraction, and Multiplication . . . . .	112
89.	The Spur and the Norm of an Algebraic Number. Theorems in Division . . . . .	115
90.	Algebraic Units . . . . .	117
91.	Reproduced through Multiplication and Division. Associate Numbers . . . . .	119
92.	Congruences . . . . .	120

## ALGEBRAIC INTEGERS OF A FIXED REALM

93.	Basis of All Integers of a Fixed Realm . . . . .	121
94.	The Discriminant. The Fundamental Invariant ( <i>Grundzahl</i> ). Minimal Basis . . . . .	126
95.	The Index of a Number. Fundamental Theorems Regarding the Same . . . . .	128
96.	The <i>Different</i> of a Number. Its Relation with the Discriminant. Hilbert's Presentation of Algebraic Integers through a Fixed Basis . . . . .	129

## QUADRATIC REALMS

97-8.	Quadratic Realms. Integers Therein . . . . .	133
99.	The Units of a Quadratic Realm. Pell's Equation . . . . .	136

## CUBIC REALMS

100.	Illustrations of Previous Definitions . . . . .	139
101.	Fundamental Theorem in Determinants . . . . .	142
102.	A Basis of Cubic Realms Due to Woronoj . . . . .	145
103.	The Discriminant, Spur, and Norm of Numbers in Cubic Realms . . . . .	150
104.	A Theorem in Determinants . . . . .	153

## CYCLOTOMIC REALMS

105.	Cyclotomic Realms. The Irreducible Equation $(x^p - 1)/(x - 1) = 0$ . . . . .	155
106.	The Roots of Such an Equation. The Discriminant . . . . .	157



ARTICLE		PAGE
107.	Basis of All Integers. Interesting Formulas Connecting the Same	159

## CHAPTER V

THE MODULS OF DEDEKIND. DIVISIBILITY.  
GENERALIZED NOTIONS OF DIVISION

108.	Euclid's Algorithm	161
109.	Applicable in Certain Realms	164
110.	Its Failure	165
111.	The Dedekind Modul	166
112.	Factorization No Longer Unique	169
113.	The Conception of Divisibility Extended. Complexes of Numbers	170
114.	The Moduls Defined through Linear Forms	173
115.	Another Definition of a Modul	174
116.	Equality of Two Moduls	176
117.	Least Common Multiple of Moduls	177
118-9.	Greatest Common Divisor of Moduls	179
120.	Theorems	182
121.	Multiplication of Moduls by Algebraic Integers	183
122.	The Product of Moduls	185
123.	The Above When One Modul Is Finite	186
124.	Finite Moduls	188
125-6.	Multiplication and Powers of Moduls	188
127-8.	A Fundamental Theorem Due to Dedekind. Theorem in Moduls	191
129.	The Quotient of Two Moduls	193
130-2.	Theorems as to the Extent the Usual Rules of Multiplication Are Applicable to Moduls	195
133.	The Order-Modul—"Art"—"Species"—"Ordnung"	204
134.	Congruences with Regard to Moduls	205
135.	Complexes That Are Not Moduls	206
136.	The Complete System of Representatives of the Modul $a$ with Respect to the Modul $b$	208
137-40.	The Symbol $(a, b)$ . Its Properties	209
141.	Generalization of Fermat's Theorem	215
142.	The Number of Moduls That Are Multiples of $a$ and Divisors of $b$ , if $b > a$ and $(a, b) \neq 0$	217

ARTICLE		PAGE
143.	The Condition that Two Congruences Be Simultaneously Satisfied.....	218

## CHAPTER VI

## FINITE MODULS

144.	A Basis Consisting of a Finite Number of Independent Elements.....	220
145.	A Linearly Independent System of Elements.....	221
146.	The Order or Degree of a Modul.....	222
147-8.	Fundamental Theorem Regarding the Orders of Moduls.....	222
149.	A System of Incongruent Residues of One Modul with Respect to Another.....	231
150.	The Symbol $(a, b)$ Expressed through a Determinant	236
151.	If $b > a$ , and if One Modul Is Finite, the Other Also Is Finite.....	236
152.	Further Theorems in Determinants.....	237
153.	The Quotient $(a, b)$ by $(b, a)$ Expressed as a Determinant.....	239
154.	Consequences That Follow from the Above Relation	241
155.	Theorem Regarding Two Bases of the Same Modul.	241
156.	Further Fundamental Theorems in Moduls.....	243
157.	Computation of the Integer $(a, b)$ .....	245
158.	The G. C. D. and L. C. M. of Finite Moduls. The Product and Quotient of Such Moduls.....	247

## CHAPTER VII

## ALGEBRAIC MODULS

159.	Definitions. Unit Moduls.....	248
160-2.	Algebraic Integers Defined by Algebraic Moduls. The Order-Modul $a^\circ$ .....	249
163.	A Theorem Which Simplifies the Whole Modul Theory.....	253

MODULS OF THE  $n$ TH ORDER IN REALMS OF THE  $n$ TH DEGREE

164.	Multiplication of a Modul by an Integer so as to Be Divisible by a Modul.....	257
------	---	-----

# TABLE OF CONTENTS

xix

ARTICLE		PAGE
165.	Fundamental Theorems Regarding the L. C. M., G. C. D., Product, etc. of Such Moduls . . . . .	259
166.	The Discriminants and Basal Elements . . . . .	260
167.	The Relation $(a, b)^2\Delta(a) = (b, a)^2\Delta(b)$ . . . . .	262
168.	The Norm . . . . .	263
169.	The Algebraic Integers of a Finite Realm Form a Finite Modul . . . . .	266
170.	The Modul $\mathfrak{o}$ Is Its Own Order-Modul . . . . .	267

## COMPLEMENTARY BASES AND COMPLEMENTARY MODULS IN A REALM OF THE $n$ TH DEGREE

171-2.	Complementary Moduls and Complementary Bases. The Spur. Relation among the Discriminants. Definitions. A Beautiful Theorem Due to Dede- kind . . . . .	268
173-4.	Complementary Bases . . . . .	271
175.	Theorems in Determinants . . . . .	274
176-7.	Relations among the Spurs . . . . .	274
178.	Important Consequences . . . . .	276
179-80.	Further Theorems $(a, b) = (b', a')$ , $(a + b)' = a' - b'$ $(a - b) = a' + b'$ . . . . .	277

## CHAPTER VIII

### THE MODULAR SYSTEMS OF KRONECKER

181.	The Conception of Congruence. Equivalence of Lin- ear Forms. Divisibility. Modular Systems De- fined . . . . .	280
182.	Realms of Rationality as Defined by Kronecker . . . . .	284
183.	The Discussion Limited to Rational Integers and Ra- tional Integral Functions with Integral Coefficients . . . . .	285
184.	Properties of Modular Systems. Composition or Multiplication. Theory of Integral Forms . . . . .	287
185.	Modular Systems of the First Kind. Condition for Such Systems. The G. C. D. of Modular Systems . . . . .	288
186.	Pure Modular Systems. Systems of Second Kind. Mixed Systems . . . . .	288
187.	Equivalence of Modular Systems . . . . .	293



ARTICLE	PAGE
188.	An Important Theorem Due to Kronecker. . . . . 294
189.	Reduced Modular Systems. . . . . 297
190.	Quantities That Are Relatively Prime to a Modular System. Units with Respect to a Modular System. Generalization of the Fermat Theorem. . . . . 300
191.	Decomposition of Systems of the Second Kind into Their Simplest Elements. Reduced Systems. . . . . 302
192.	The Simplest Forms for the System $(p^h, f_1(x), f_2(x), \dots, f_r(x))$ . . . . . 303
193.	Canonical Forms for Such Systems. . . . . 305
194.	The Decomposition of a Function $F(x)$ into Its Irreducible Factors (Modulo $p$ ). . . . . 312
195.	Prime Modular Systems. Divisibility of a Function by a Prime Modular System. Units. Divisibility of a Product by a Prime Modular System. . . . . 315
196.	Theorems Relative to Prime Modular Systems. . . . . 317
197.	Theorems for the Reduction of Pure Modular Systems of the Second Kind. Incongruent Units. Congruences with Respect to Prime Modular Systems. Roots. . . . . 319
198.	Factorization of the Function $x^{p^n} - x$ with Respect to the Modulus $p$ . . . . . 323
199-200.	Integral Functions in Many Variables. Modular Systems for Such Functions. . . . . 326
201.	The System $(p, x^{p^r} - x)$ . . . . . 329
202.	A Theorem Due to Hensel. . . . . 331

## CHAPTER IX

NOTIONS INTRODUCTORY TO THE THEORY  
OF IDEALS

203-4.	Two Simple Illustrations. . . . . 334
205.	The Factorization of 21 is Not Unique in the Realm $\mathfrak{R}(\sqrt{-5})$ . The Kummer Ideal Numbers. A Correlation between Forms and Complex (Algebraic) Integers. The Dedekind "Ideal". . . . . 337

# TABLE OF CONTENTS

xxi

ARTICLE		PAGE
THE IDEALS OF THE QUADRATIC REALMS		
206.	Definitions. Divisibility. Principal Ideal. Equality of Two Ideals. Product of Ideals. Basis. Canonical Form .....	340
207.	Applications .....	344
208.	Realms in Which There Exist Only Principal Ideals.	346
209.	The Congruences with Respect to an Ideal. The Norm of an Ideal. Conjugate Ideals .....	347
210.	A Complete System of Residues with Respect to an Ideal .....	351
211.	Finite Number of Ideal Factors of an Ideal .....	353
UNIQUE FACTORIZATION OF IDEALS		
212.	Introduction of Several Lemmas. The Greatest Common Divisor of Two Ideals .....	355
213.	Theorem Regarding the Product of Ideals by a Prime Ideal .....	356
214.	The Unique Factorization of Ideals .....	356
215.	A Practical Criterion for Determining When an Ideal Is Prime. Expression of Any Ideal Through Two Elements .....	356
216.	The Ideal Factors of a Rational Prime Integer .....	358
EQUIVALENCE OF IDEALS. CLASSES OF IDEALS		
217.	The Equivalence of Ideals. Equivalent Ideals Form a Class .....	364
218.	The Number of Ideal Classes Is Finite. An Ideal in Every Class Whose Norm $\equiv  \sqrt{D} $ .....	366
219.	A Criterion for Determining When Ideals Are Equivalent .....	368
220.	Theorems in Quadratic Forms .....	371
221.	The Function $\Phi(a)$ . Theorems Regarding This Function .....	372
222.	Fermat's Theorem for Ideals .....	376
223.	General Congruences. Roots .....	378
224.	Primitive Numbers with Respect to a Prime Ideal. Numbers That <i>Belong</i> to a Given Exponent. Theorems Regarding the Same .....	379

ARTICLE		PAGE
225.	Wilson's Theorem for Ideals.....	382
226.	Linear Congruences with Respect to Ideals. Theorems Regarding Them.....	384
QUADRATIC CONGRUENCES AND THE SYMBOL $\left(\frac{\alpha}{p}\right)$		
227.	Quadratic Congruences.....	388
228.	The Number of Quadratic Incongruent Residues (Modulo $p$ ).....	390
229.	Theorem Regarding the Divisors of 2 in the Realm $\Re(\sqrt{m})$ . Quadratic Congruences in Which the Modulus Is an Ideal.....	393
230.	Units of the Quadratic Realm.....	396
231.	Application of the Minkowski Theorem.....	397
232.	Units in Real Realms.....	401
233.	The Dirichlet Theorem.....	404
234.	Realms in Which There Are an Odd Number of Classes. Important Theorem.....	405
235.	The Number of Ideal Classes of a Realm Whose Discriminant Is an Odd Prime.....	407
236.	The Hilbert Number-Rings. Definitions. Bases. Norms. Conjugate Ideals. Products of Ideals.....	409
237.	Condition That a Realm Ideal be a Ring Ideal. Ring Leader. Regular Ring Ideals.....	411
238.	Decomposition of Ring Ideals into Their Prime Ring Ideal Factors. Equivalence of Such Ideals. Units.....	413

## CHAPTER X

## THE QUADRATIC LAW OF RECIPROCITY AND ITS ANALOGUE IN THE QUADRATIC REALMS

239.	Introductory Statement Regarding the Law of Reciprocity.....	417
240.	The Limiting Cases of This Law as Found in the Realms $\Re(\sqrt{-1})$ , $\Re(\sqrt{2})$ , $\Re(\sqrt{-2})$ . The Expression of a Prime Integer $p$ in the Form of the Sum of Two Squares.....	417
241.	The Congruence $x^2 - 2 \equiv 0$ (Modulo $p$ ).....	420



TABLE OF CONTENTS

xxiii

ARTICLE		PAGE
242.	Concerning the Congruence $x^2 + 2 \equiv 0$ (Modulo $p$ )	422
243-4.	The Quadratic Law of Reciprocity for Rational Prime Integers. Historical Notes and Proof of the General Theorem	422
245.	A Generalized Form of This Law Due to Jacobi	429
246.	Expression of Integers through Sums of Squares in the Realms $\Re(\sqrt{-1})$ , $\Re(\sqrt{-2})$ , $\Re(\sqrt{-3})$ and $\Re(\sqrt{2})$	429

HILBERT'S SYMBOL FOR NORM-RESIDUES

247.	A Theorem Regarding Quadratic Residues	433
248-51.	The Signs to be Associated with the Hilbert Symbol	437
252.	The Character-System of an Ideal	449
253.	Ideals of the Same Class Have the Same Character-System	451
254.	Distribution of Ideal Classes into Genuses	452
255-6.	A Product Theorem Connected with the Units of a Character-System	454
257.	The Ambiguous Classes. Hilbert's System of <i>Independent</i> Ambiguous Classes	460
258.	Ambiguous Ideals Which Are Divisors of the Discriminant of a Quadratic Realm	461
259.	Ambiguous Classes That Do Not Contain Ambiguous Ideals	465
260.	The Number of Ambiguous Classes in a Quadratic Realm	467
261.	The Existence of the Genuses	469
262.	Expression of a Class of a Principal Genus as a Square of a Class of the Realm	473

APPLICATION OF THE EXISTENCE THEOREM OF THE GENUSES

263.	Theorem Regarding the Norm of the Fundamental Unit	475
------	--	-----

## CHAPTER XI

APPLICATION OF THE THEORY OF IDEALS OF  
QUADRATIC REALMS TO A DISCUSSION OF  
FERMAT'S THEOREM

ARTICLE		PAGE
264.	Remarks of L. E. Dickson, Kronecker, and Legendre. Kummer's Discovery that All Algebraic Integers Defined by the $n$ th Roots of Unity May Be Uniquely Factored through Prime Ideal Factors. His Attempts at Proof of the Fermat Theorem and the General Law of Reciprocity. Fermat's Method of Infinite Descent . . . . .	481
265.	The Legendre-Fermat Proof that the Diophantine Equation $x^4 + y^4 = z^2$ cannot Be Solved . . . . .	483
266.	Legendre's Proof that $x^3 + y^3 = z^3$ Does Not Admit Solution . . . . .	485
267.	The Kummer Proof that This Equation May Not Be Solved in the Realms $\Re(i)$ and $\Re(\omega)$ . . . . .	489
268.	The Equation $\alpha^4 + \beta^4 = \gamma^2$ Cannot Be Solved in $\Re(i)$ . . . . .	492
269.	Interesting Consequences Due to Hurwitz and Kronecker . . . . .	494
270.	An Important Theorem Due to Kummer. Vandiver's Recent Work . . . . .	496

## CHAPTER XII

CORRELATION BETWEEN THE THEORY OF QUADRATIC  
FORMS AND THE IDEALS OF QUADRATIC REALMS

271.	Forms That Are <i>Properly</i> Primitive and <i>Improperly</i> Primitive. The Discriminant of a Form. Substitutions with Determinant $+1$ and $-1$ Statement of the Fundamental Problems of the Theory of Quadratic Forms . . . . .	497
272.	Kummer's Statement that the Treatment of the Numbers in Quadratic Realms Was Identical with the Theory of Quadratic Forms. Kummer's Ideal Numbers . . . . .	499
273.	Correlation between a Prime Ideal and a Quadratic Form . . . . .	501

# TABLE OF CONTENTS

xxv

ARTICLE		PAGE
274-5.	Principal Ideals and Principal Forms.....	502
276.	Arbitray Ideals and Correlated Forms in the Realms $\Re(\sqrt{m})$ , $m \equiv 1 \pmod{4}$ .....	507
277.	Ambiguous Ideals in Real Realms.....	509
278.	The Presentation of a Rational Integer through a Form.....	510
279.	Other Bases of an Ideal and the Associated Form..	511

## ARBITRARY IDEALS AND FORMS

280-2.	Arbitrary Ideals and Forms in Imaginary (Article 281), and in Real (Article 282) Realms.....	513
--------	--	-----

## MULTIPLICATION OF IDEALS AND THE COMPOSITION OF FORMS

283.	Reciprocal Relations of Quadratic Forms and Ideals	521
284.	Correlation among Ideals and Quadratic Forms....	524
285.	Fundamental Theorem Regarding the Composition of Forms and the Multiplication of Ideals.....	526

## CHAPTER XIII

### GEOMETRIC PRESENTATION OF IDEALS

#### IMAGINARY REALMS

286.	Definitions. Lattice-Points. Lattices. Meshes. Lat- tice-Points and the Basis of All Integers of a Quadratic Realm.....	530
287.	Principal Ideals and Systems of Lattices. The Ideal (1) and the Fundamental Lattice.....	533
288.	The Number of Lattice-Points That Lie Within a Mesh.....	536
289.	The Lattice-Points of an Arbitrary Ideal. A Com- plete Set of Incongruent Integers (Modulo $i$ ). The Number $N(i)$ . Similar Lattices and Equivalent Ideals.....	537
290.	Units of the Realm and Symmetric Properties of Lattice Points.....	540
291.	The Number of Ideal Classes of a Realm and the Distribution of Lattice-Points into Similar Classes	540

ARTICLE		PAGE
REAL REALMS		
292.	Pseudometric Geometry. Distance. Angle. Area. Minimal Lines. Inclination of a Radius. Fundamental Relations among Hyperbolic Functions. The Standard Curve. The Hyperbola. Property of Its Asymptotes. Area Defined.....	541
293.	The Fundamental Lattice. The Lattice-Points of a Principal Ideal. Proper and Improper Turning and Reflection about an Asymptote. Minimal Lines. Complex Angle.....	545
294.	The Geometric Meaning of the Units of a Real Realm	548

## CHAPTER XIV

## THE CUBIC REALMS

295.	Fundamental Properties of a Realm.....	553
296.	The Sum, Difference, and Product of Integers.....	554

## THE DISCRIMINANT OF AN INTEGER OF THE REALM

297.	The Different and Discriminant of an Integer.....	556
298.	The Discriminants of All Numbers of a Realm Have the Same Sign. An Equation Whose Discriminant Equals Unity.....	558
299.	The Basis of All Integers of the Realm.....	559
300.	The Ideals of the Realm. An Integer $\alpha$ Has Only a Finite Number of Factors. The Factorization as Such Is <i>Not</i> Unique. Ideals Defined. Unit Ideals	560
301.	Normal Basis.....	561
302.	Multiplication of Ideals.....	563
303.	Equivalent Ideals. Ideal Classes. The Minkowski Theorem. Ideals, Each of Which Is a Representative of a Definite Class.....	564
304.	Proof of the Fundamental Theorem: If $\mathfrak{a}$ Is an Arbitrary Ideal, Another Ideal $\mathfrak{b}$ May Be Determined Such That $\mathfrak{ab}$ Is a Principal Ideal.....	569
305.	If All Integers of $\mathfrak{b}$ Are Divisible by $\alpha$ , Then $\mathfrak{b}$ Is Divisible by $\alpha$ . Prime Ideals: If the Product of Two Ideals Is Divisible by a Prime Ideal, One of the	



# TABLE OF CONTENTS

xxvii

ARTICLE		PAGE
	Factors is Divisible by It. Unique Factorization: In Every Ideal $\alpha$ Which Is Not a Principal Ideal, Two Integers $\alpha$ and $\alpha_1$ May Be Found Such That $\alpha \equiv (\alpha, \alpha_1)$ . . . . .	572
306.	The Norm of an Ideal. The Distribution of All Integers of the Realm into $N(\alpha)$ Incongruent (Modulo $\alpha$ ) Classes . . . . .	574
307.	The Norm of the Product of Two Ideals . . . . .	576
308.	The Determination of the Norm. The <i>Degree</i> of a Prime Ideal . . . . .	577
309.	Theorems of Minkowski for the Presentation of the Ideal Classes . . . . .	577
310.	Derivation of the Prime Ideals. The Expression of a Rational Prime Integer $p$ as the Product of Three Prime Ideals . . . . .	580
311.	The Case Where $p$ Is a Divisor of the Discriminant of the Realm. Theorems of Dedekind . . . . .	583
THE UNITS OF THE REALM $\mathfrak{R}(\theta)$		
312.	The Units of a Realm . . . . .	584
313.	Dirichlet's Theorem Regarding Such Units . . . . .	586
314.	Minkowski's Proof of the Dirichlet Theorem . . . . .	589
	INDEX . . . . .	597



FOUNDATIONS OF THE  
THEORY OF ALGEBRAIC NUMBERS





## CHAPTER I

### PRELIMINARY NOTIONS

ART. 1. **Reducible and Irreducible Functions.** It has been seen in algebra that an algebraic function of the  $n$ th degree

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

may always be resolved into its linear factors in the form

$$f(x) = a_n (x - x_1)(x - x_2) \dots (x - x_n),$$

where  $x_1, x_2, \dots, x_n$  are the  $n$  roots of the function. But this distribution into linear factors ceases if the coefficients are subjected to certain conditions: for example, the coefficients of  $f(x)$  being all real, it may be required that the coefficients of its factors be all real. In this case we may resolve  $f(x)$  into factors of the first and second degree, since a function of the second degree with negative discriminant is irreducible, if we demand that the roots be real. One may further impose the condition that the coefficients of the factors of  $f(x)$  be integers, it being supposed that the coefficients of  $f(x)$  are integral. Functions which under such and similar conditions are resolvable into factors, are said to be *reducible*; if they may not be resolved into factors, they are called *irreducible*.

By "function" we shall always mean "algebraic function" unless it is expressly stated to the contrary.

ART. 2. **Realms.** Any system of an infinite number of numbers or quantities constitute a *realm* or *domain*. For example, all integers form a realm, also all fractions constitute a realm. It is evident that the latter realm is more

extended, that is, embraces more quantities than the former. If the coefficients of a given function  $f(x)$  all belong to one and the same realm, we may ask: Is  $f(x)$  reducible into factors whose coefficients belong to the same realm? If this is the case, the function is said to be *reducible* in this realm, otherwise *irreducible*. For example, if the realm in question includes all quantities real and complex, then all functions are reducible except the linear functions; but if the realm includes only real quantities, then all functions are reducible except the linear functions and the quadratic functions with negative discriminant.

**ART. 3. Congruence of Two Functions with Respect to a Modulus.** Let

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

be an integral function in  $x$  with integral coefficients. If the coefficients  $a_0, a_1, \dots, a_n$  are all divisible by the positive integer  $k$ , we say that  $f(x)$  is divisible by  $k$ .

It is seen then that

$$f(x) = kg(x),$$

where  $g(x)$  is also an integral function with integral coefficients. The function  $f(x)$  is therefore a *multiple* of  $k$  when and only when all the coefficients of  $f(x)$  are divisible by  $k$ . Let

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$$

be two integral functions with integral coefficients. If the difference  $f(x) - g(x)$  is divisible by  $k$ , the two functions  $f(x)$  and  $g(x)$  are said to be *congruent* with respect to the modulus  $k$  and this fact is indicated by the notation

$$f(x) \equiv g(x) \pmod{k}.$$

From this congruence it follows that

$$a_\nu \equiv b_\nu \pmod{k} \quad (\nu = 0, 1, 2, \dots, n);$$

or

$$a_\nu = b_\nu + c_\nu k \quad (\nu = 0, 1, 2, \dots, n),$$

where the  $c$ 's are integers. It follows also that

$$f(x) = g(x) + kh(x),$$

where  $h(x)$  like  $f(x)$  and  $g(x)$  is an integral function with integral coefficients.

**ART. 4. The Gaussian Lemma.** After these introductory remarks we may next prove the following theorem (stated by Gauss, *Dis. Arith.*, Art. 43):

**THEOREM.** *If the product of two integral functions with integral coefficients is divisible by a prime integer  $p$ , one of the factors is divisible by  $p$ .* Denote the two integral functions by

$$f(x) = a_0 + a_1x + \dots + a_nx^n + \dots,$$

$$g(x) = b_0 + b_1x + \dots + b_mx^m + \dots;$$

and let their product be the integral function

$$\phi(x) = f(x)g(x) = c_0 + c_1x + c_2x^2 + \dots,$$

where

$$c_0 = a_0b_0, \quad c_1 = a_0b_1 + b_0a_1, \quad \dots$$

To prove the theorem it is only necessary to show that if  $f(x)$  or  $g(x)$  is *not* divisible by  $p$  then  $\phi(x)$  is *not* divisible by  $p$ . Suppose of the coefficients that appear in  $f(x)$  that  $a_0, a_1, \dots, a_{n-1}$  are divisible by  $p$ ; and of the coefficients in  $g(x)$  suppose that  $b_0, b_1, \dots, b_{m-1}$  are divisible by  $p$  while  $a_n$  and  $b_m$  are *not* divisible by  $p$ .

The coefficient of  $x^{n+m}$  in  $\phi(x)$  is

$$c_{n+m} = a_0b_{n+m} + a_1b_{n+m-1} + a_2b_{n+m-2} + \dots \\ + a_nb_m + a_{n+1}b_{m-1} + \dots + a_{n+m}b_0.$$

All of these terms are divisible by  $p$  except  $a_nb_m$ . It follows that  $c_{n+m}$  is not divisible by  $p$  and consequently also that  $\phi(x) = f(x)g(x)$  is not divisible by  $p$ .

The theorem when extended to the product of any number of functions is: *A product of several integral*

*functions with integral coefficients is only divisible by the prime integer  $p$  when and only when one of the functions is divisible by  $p$ .* The theorem is also true for functions of several variables, and may be proved as above, if the functions are arranged according to a definite sequence of the powers of the variables.

**ART. 5. Primitive Functions; Divisors.** If the coefficients of an integral function are integers and have  $t$  as their greatest common divisor,  $t$  is called *the divisor* of the function; and if this divisor is unity, the function is said to be *primitive*. Accordingly, a *primitive function is an integral function in the variable with integral coefficients that have no common divisor other than unity*. We may also speak of the *divisor* of fractional coefficients. Let

$$f(x) = c_0 + c_1x + c_2x^2 + \dots$$

be an integral function with fractional coefficients  $c_0, c_1, \dots$ ; and let  $s$  be the least common multiple of the denominators of these fractions. It follows that  $c_0 = b_0/s, c_1 = b_1/s, \dots$ , where  $b_0, b_1, \dots$  are integers. Further let  $r$  be the greatest common divisor of  $b_0, b_1, \dots$ , so that  $b_0 = d_0r, b_1 = d_1r, \dots$ , where  $d_0, d_1, \dots$  are integers. Denote  $r/s$  by  $t$ . We thus have  $c_0 = td_0, c_1 = td_1, \dots$ . As above,  $t$  is said to be the *divisor* of the function. It has the property that all the coefficients  $c_0/t, c_1/t, \dots$  are integers which have no common divisor other than unity.

It may be proved as follows that there is only one such divisor  $t$ . For suppose that  $t'$  were another. We would then have  $c_0 = t'd'_0, c_1 = t'd'_1, \dots$ , where  $d'_0, d'_1, \dots$ , are integers. Since  $d_0, d_1, \dots$  are integers whose greatest common divisor is unity, we may determine other integers  $x_0, x_1, \dots$  such that

$$x_0d_0 + x_1d_1 + \dots = 1.$$



It follows, since  $td_0 = c_0 = t'd'_0$ , etc., that

$$t(x_0d_0 + x_1d_1 + \dots) = t'(d'_0x_0 + d'_1x_1 + \dots).$$

Hence  $t/t' = d'_0x_0 + d'_1x_1 + \dots = k$ , say, where  $k$  is an integer. It is thus seen that  $t' = t/k$  and also that  $f(x)/t' = kf(x)/t$ ; and it further follows that the coefficients of  $f(x)$  when this function is divided by  $t'$  are all divisible by the integer  $k$ . That  $f(x)/t'$  be a primitive function we must accordingly have  $k=1$  or  $t=t'$ . Note that the quotient of *any* integral function by its divisor is a *primitive* function.

ART. 6. *The product of two or more primitive functions is a primitive function.* For if  $f(x)$  and  $g(x)$  are two primitive functions and if  $f(x)g(x) = h(x)$ , the coefficients of  $h(x)$  are integers; and if they have a common divisor  $t$ , then  $t$  is also an integer. Further decomposing  $t$  into its prime factors, these prime factors are divisors of either  $f(x)$  or  $g(x)$ ; but as both  $f(x)$  and  $g(x)$  are primitive functions, these factors must all be unity (Art. 4) and therefore  $t$  must be unity.

ART. 7. *The divisor of a product of two or more functions is equal to the product of the divisors of these functions.* Let  $f(x)$  and  $g(x)$  be integral functions with rational coefficients and suppose that

$$f(x)g(x) = h(x).$$

Let  $\alpha$  and  $\beta$  be the divisors of  $f(x)$  and  $g(x)$  so that  $f(x) = \alpha f_1(x)$ ,  $g(x) = \beta g_1(x)$  where  $f_1(x)$  and  $g_1(x)$  are primitive functions. Further let  $\gamma$  be the divisor of  $h(x)$  so that  $h(x) = \gamma h_1(x)$ ,  $h_1(x)$  being a primitive function. We then have

$$\frac{\gamma}{\alpha\beta} h_1(x) = f_1(x)g_1(x).$$

Since on the right hand  $f_1(x)g_1(x)$  is a primitive function,

its divisors must be unity. It follows that

$$\gamma = \alpha \cdot \beta.$$

*Another form of the same theorem.* If  $f(x)$  is an integral function with integral coefficients and if  $g(x)$  is a primitive function; then if  $\frac{f(x)}{g(x)}$  is an integral function of  $x$ , its coefficients are integral also. The coefficients in this fraction must be rational numbers, since division is a rational operation.

We may therefore write  $\frac{f(x)}{g(x)} = th(x)$ , where  $h(x)$  is a primitive function. It follows that  $f(x) = th(x)g(x)$ .

Since the coefficients of  $f(x)$  are integral, it is seen that  $t$  is an integer and consequently the coefficients of  $\frac{f(x)}{g(x)}$  are integers.

**ART. 8.** *If an integral function whose coefficients are integers is resolvable into a product of two integral functions with rational coefficients, it may also be resolved into a product of two integral functions with integral coefficients.*

For let  $f(x) = g(x)h(x)$  and write  $g(x) = \beta g_1(x)$  where  $\beta$  is the divisor of  $g(x)$  so that  $g_1(x)$  is a primitive function. It follows that  $f(x)/g_1(x) = \beta h(x)$ , where  $\beta h(x)$  is an integral function with integral coefficients (Art. 7).

From this it also follows that if an integral function with integral coefficients is not resolvable into the product of two integral functions with integral coefficients, it cannot be resolved into two such functions with rational coefficients; or, if an integral function is irreducible in the realm of all integers, it is also irreducible in the realm of all rational numbers.

**ART. 9.** Let  $f(x)$  be an integral function whose coefficients are integers and suppose that the coefficient

of the highest power of  $x$  is unity; further let  $g(x)$  be a divisor of  $f(x)$  where  $g(x)$  is also an integral function of  $x$  having unity as the coefficient of the highest power of  $x$ . We may show <sup>1</sup> that the other coefficients of  $g(x)$  are also integers. For let

$$g(x) = b_0 + b_1x + \dots + 1 \cdot x^s.$$

Let  $\beta$  be the divisor of  $g(x)$ , so that  $b_0/\beta, b_1/\beta, \dots, 1/\beta$  are integers without a common divisor other than unity. Write  $1/\beta = b$ , where  $b$  is an integer. Since  $f(x)$  is divisible by  $g(x)$  and since  $g(x) = \beta g_1(x)$ , where  $g_1(x)$  is a primitive function, it follows that  $f(x)/g_1(x) = \chi(x)$ , where (Art. 7)  $\chi(x)$  is an integral function with integral coefficients. Let  $c$  be the coefficient of the highest power of  $x$  in  $\chi(x)$ .

Comparing the coefficients in

$$f(x) = g_1(x)\chi(x),$$

it is seen that

$$1 = b \cdot c.$$

As both  $b$  and  $c$  are integers, it follows that  $b = c = 1 = \beta$  and consequently the coefficients of  $g(x)$  are integral.

The above may be expressed differently as follows:

**THEOREM.** *If*

$$f(x) = 1 \cdot x^t + a_{t-1}x^{t-1} + \dots + a_1x + a_0,$$

and

$$g(x) = 1 \cdot x^s + b_{s-1}x^{s-1} + \dots + b_1x + b_0,$$

the  $a$ 's and  $b$ 's being rational; if further,

$$f(x)g(x) = h(x) = x^{s+t} + c_{s+t-1}x^{s+t-1} + \dots + c_1x + c_0,$$

then the  $c$ 's cannot all be integers, unless the  $a$ 's and  $b$ 's are all integers.

**ART. 10.** If the function  $g(x)$  is of the first degree in  $x$ , say

$$g(x) = x - r,$$

<sup>1</sup> See Gauss, *Dis. Arith.*, Art. 42.

where  $r$  is a rational number; if further  $f(x)$  of the preceding is divisible by  $g(x)$ , then from above  $r$  must be an integer. If however  $f(x)$  is divisible by  $x-r$ , then  $r$  is a root of  $f(x)=0$ . It follows that *if in  $f(x)=0$ , all the coefficients are integers and if the coefficient of the highest power of  $x$  is unity, then the rational roots must all be integral.*

We have thus a simple method of determining all the rational roots of the equation

$$F(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0,$$

where the  $a$ 's are integers. For multiply this equation by  $a_0^{n-1}$  and then write  $a_0x = y$ . We have

$$y^n + a_1y^{n-1} + a_0a_2y^{n-2} + \dots + a_0^{n-1}a_n = 0,$$

an equation in which the coefficient of the highest power of  $y$  is unity, the other coefficients being integers. To determine whether this equation has integral roots, write for  $y$  the integer  $r$ ; then, since all the terms except the last has  $r$  as a factor, it follows also that  $a_0^{n-1}a_n$  must be divisible by  $r$ , if  $r$  is a root of the equation. From this it is seen that all the roots of the equation in  $y$  that are rational are integers that are divisors of  $a_0^{n-1}a_n$ . Since  $a_0x = y$ , we have only to divide these roots by  $a_0$  to have the rational roots of the equation in  $x$ .

**FUNDAMENTAL THEOREM.** *If all the coefficients of the functions*

$$A(x) = a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m$$

and

$$B(x) = b_0x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n$$

are rational, and if all the coefficients of their product

$$C(x) = c_0x^{m+n} + c_1x^{m+n-1} + \dots + c_{m+n}$$

are rational integers, then all the products  $a_i b_k$  are rational integers. For, if  $a$  and  $b$  are the divisors of  $A(x)$  and  $B(x)$ , the integer  $c$  being the divisor of  $C(x)$ , it is evident



that  $a_i b_k$  has the form  $aa'_i \cdot bb'_k = ca'_i b'_k$ , where  $ab = c$  and where  $a'_i$  and  $b'_k$  are integers due to the property of the divisors  $a$  and  $b$ . This theorem is also due to Gauss. \*

ART. 11. The *irreducibility* of certain special functions may be considered next.

THEOREM. Let  $f(x)$  be an integral function whose coefficients are integers and let  $p$  be a prime integer. In  $f(x)$  suppose that the coefficient of the highest power of  $x$  is not divisible by  $p$  and suppose further that the constant term is not divisible by  $p^2$ . The function  $f(x)$  is irreducible, if all the other coefficients are divisible by  $p$  including the constant term.

Let

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n,$$

where  $a_0, a_1, \dots, a_n$  are integers such that  $a_n$  is not divisible by  $p$  while  $a_0, a_1, \dots, a_{n-1}$  are divisible by  $p$ , and further  $a_0$  is not divisible by  $p^2$ .

Suppose that  $f(x)$  is resolvable into factors, and write

$$f(x) = (b_0 + b_1x + b_2x^2 + \dots + b_r x^r)(c_0 + c_1x + \dots + c_s x^s),$$

where the coefficients are integral (Art. 8). Equating coefficients of the highest power of  $x$ , it is seen that

$$a_n = b_r \cdot c_s \quad \text{and} \quad a_0 = b_0 c_0.$$

Since  $a_n$  is not divisible by  $p$ , it follows that neither  $b_r$  nor  $c_s$  is divisible by  $p$ . From the second relation since  $a_0$  is divisible by  $p$  but not by  $p^2$ , it follows that either  $b_0$  or  $c_0$ , but not both of these numbers, is divisible by  $p$ . Suppose then that  $c_0$  is divisible by  $p$ . We have at once the following congruence

$$f(x) \equiv a_n x^n \equiv (b_0 + b_1x + b_2x^2 + \dots + b_r x^r)(c_1x + c_2x^2 + \dots + c_s x^s) \pmod{p}.$$

Hence  $b_0 c_1 \equiv 0 \pmod{p}$  and since  $b_0 \not\equiv 0 \pmod{p}$  it follows that  $c_1 \equiv 0 \pmod{p}$ . The term  $c_1x$  may consequently be dropped from the above congruence. Con-

tinuing this process it is seen that all the  $c$ 's would be divisible by  $p$ . But  $c_s$  is not divisible by  $p$ .

• We therefore meet with a contradiction when we assume that  $f(x)$  may be resolved into factors.

This theorem is usually ascribed <sup>1</sup> to Eisenstein, as it is proved by him in the paper "Ueber die Irreduktibilität," etc. (*Crelle*, Bd. 39, p. 160). It is proved, however, by Schönemann (*Crelle*, Bd. 32, p. 100).

ART. 12. An interesting application of the preceding theorem is to prove that the function  $(x^p - 1)/(x - 1)$ ,  $p$  a prime integer, is irreducible. It may be noted that the division of a circle into  $p$  equal parts depends upon this fact. We have at once

$$(1) \quad (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1.$$

With Eisenstein (*op. cit.* p. 167) write  $x = 1 + z$ , so that

$$x^k = 1 + kz + k(k-1)/2!z^2 + \dots + kz^{k-1} + z^k.$$

Observing that

$$n(n+1) = \frac{1}{3}[n(n+1)(n+2) - (n-1)n(n+1)],$$

$$(n-1)n = \frac{1}{3}[(n-1)n(n+1) - (n-2)(n-1)n],$$

$$\dots = \dots$$

$$1 \cdot 2 = \frac{1}{3}(1 \cdot 2 \cdot 3 - 0 \cdot 1 \cdot 2),$$

it is seen that

$$n(n+1) + (n-1)n + \dots + 1 \cdot 2 = \frac{1}{3}n(n+1)(n+2),$$

and similarly

$$n(n+1)(n+2) + \dots + 2 \cdot 3 \cdot 4 + 1 \cdot 2 \cdot 3 = \frac{1}{4}n(n+1)(n+2)(n+3),$$

etc. Function (1) becomes when equated to zero

$$p + p(p-1)/2!z + p(p-1)(p-2)/3!z^2 + \dots + pz^{p-2} + z^{p-1} = 0.$$

<sup>1</sup> For example by Netto in his *Algebra*, p. 56; and by Koenigsberger, *Crelle*, Bd. 115, p. 53. See *Report on Algebraic Numbers* (p. 32) by Dickson, Mitchell, Vandiver, Wahlin. In the future this report will be referred to as the *Report on Algebraic Numbers*.



it is seen that while  $1 \equiv a_{p^n - p^{n-1}} \pmod{p}$ , all the other  $a$ 's are  $\equiv 0 \pmod{p}$ . It follows that  $a_{p^n - p^{n-1}}$  is *not* divisible by  $p$  and since the constant term  $a_0$  is *not* divisible by  $p^2$ , the given function is irreducible.

It may be noted that the division of a circle into  $p^n$  equal parts depends upon the solution of the above equation.

**ART. 14. The Algorithm of the Greatest Common Divisor.** Let  $f(x)$  and  $f_1(x)$  be integral functions with integral coefficients, the degree of  $f(x)$  being greater than or equal to the degree of  $f_1(x)$ . Through division it is seen that

$$f(x) = Q(x)f_1(x) + R(x),$$

where  $Q(x)$  and  $R(x)$  are integral functions in  $x$ , whose coefficients are rational but in general not integral. The degree of  $R(x)$  is less than that of  $f_1(x)$ . We may write  $Q(x) = q_1(x)/s$ ,  $R(x) = -f_2(x)/s$ , where  $s$  is an integer so chosen that the coefficients of both  $q_1(x)$  and  $f_2(x)$  are integral.

The above equation is consequently

$$\left. \begin{array}{l} \text{Euclid's scheme} \\ \text{Liber IX, 20} \end{array} \right\} \begin{cases} sf(x) = q_1(x)f_1(x) - f_2(x); \text{ and similarly} \\ s_1f_1(x) = q_2(x)f_2(x) - f_3(x), \\ \dots\dots\dots = \dots\dots\dots \\ s_{r-2}f_{r-2}(x) = q_{r-1}(x)f_{r-1}(x) - f_r(x), \\ s_{r-1}f_{r-1}(x) = q_r(x)f_r(x). \end{cases}$$

Since the degree of  $f_{i+1}(x)$  is less than that of  $f_i(x)$  ( $i = 2, 3, \dots, r-1$ ) and as this degree can not be a negative integer, it follows that there must be a function  $f_r(x)$  which is a divisor of  $s_{r-1}f_{r-1}(x)$  as indicated. This function  $f_r(x)$  is an integral function with integral coefficients being of course an integer when its degree in  $x$  is zero.



ART. 15. Any of the polynomials  $f_2(x), f_3(x), \dots, f_r(x)$  may be expressed as linear homogeneous functions of  $f(x)$  and  $f_1(x)$ ; for note that

$$f_\lambda = q_{\lambda-1}f_{\lambda-1} - s_{\lambda-2}f_{\lambda-2},$$

where the functional sign is used to represent the function. Writing for  $f_{\lambda-1}$  its value, we have

$$\begin{aligned} f_\lambda &= (q_{\lambda-1}q_{\lambda-2} - s_{\lambda-2})f_{\lambda-2} - s_{\lambda-3}q_{\lambda-1}f_{\lambda-3} \\ &= [q_{\lambda-1}q_{\lambda-2}q_{\lambda-3} - s_{\lambda-2}q_{\lambda-3} - s_{\lambda-3}q_{\lambda-1}]f_{\lambda-3} \\ &\quad - [q_{\lambda-1}q_{\lambda-2} - s_{\lambda-2}]s_{\lambda-4}f_{\lambda-4} \\ &\quad \dots \dots \dots \\ &= \psi_{\lambda-1}f_1 - \phi_{\lambda-1}f. \end{aligned}$$

To determine <sup>1</sup> the recursion-formulas for  $\psi_{\lambda-1}$  and  $\phi_{\lambda-1}$  we note that

$$f_{\lambda+2} = q_{\lambda+1}f_{\lambda+1} - s_\lambda f_\lambda.$$

In this formula write

$$f_\lambda = \psi_{\lambda-1}f_1 - \phi_{\lambda-1}f, \quad f_{\lambda+1} = \psi_\lambda f_1 - \phi_\lambda f.$$

It follows that

$$f_{\lambda+2} = [\psi_\lambda q_{\lambda+1} - s_\lambda \psi_{\lambda-1}]f_1 - [\phi_\lambda q_{\lambda+1} - s_\lambda \phi_{\lambda-1}]f;$$

and consequently

$$\left. \begin{aligned} \psi_{\lambda+1} &= q_{\lambda+1}\psi_\lambda - s_\lambda \psi_{\lambda-1} \\ \phi_{\lambda+1} &= q_{\lambda+1}\phi_\lambda - s_\lambda \phi_{\lambda-1} \end{aligned} \right\} \quad (2)$$

Further since

$$\begin{aligned} f_1 &= \psi_0 f_1 - \phi_0 f = 1 \cdot f_1 - 0 \cdot f, \\ f_2 &= \psi_1 f_1 - \phi_1 f = q_1 f_1 - s f, \end{aligned}$$

it is seen that

$$\begin{aligned} \psi_0 &= 1, & \phi_0 &= 0, \\ \psi_1 &= q_1, & \phi_1 &= s, \\ \psi_2 &= q_1 q_2 - s_1, & \phi_2 &= s q_2, \\ \psi_3 &= q_1 q_2 q_3 - s_2 q_1 - s_1 q_3, & \phi_3 &= s q_2 q_3 - s s_2, \\ \dots &= \dots & \dots &= \dots \end{aligned}$$

<sup>1</sup> See Netto, *Algebra*, p. 65.

ART. 16. If we eliminate  $q_\lambda$  from the formulas

$$\psi_\lambda = q_\lambda \psi_{\lambda-1} - s_{\lambda-1} \psi_{\lambda-2},$$

$$\phi_\lambda = q_\lambda \phi_{\lambda-1} - s_{\lambda-1} \phi_{\lambda-2},$$

we have

$$\phi_\lambda \psi_{\lambda-1} - \psi_\lambda \phi_{\lambda-1} = s_{\lambda-1} [\phi_{\lambda-1} \psi_{\lambda-2} - \psi_{\lambda-1} \phi_{\lambda-2}].$$

And since  $\phi_1 \psi_0 - \psi_1 \phi_0 = s$ , it follows that

$$\phi_\lambda \psi_{\lambda-1} - \psi_\lambda \phi_{\lambda-1} = s_{\lambda-1} s_{\lambda-2} \cdots s_1 s,$$

or

$$\begin{aligned} \frac{\phi_\lambda}{\psi_\lambda} &= \frac{s_{\lambda-1} s_{\lambda-2} \cdots s}{\psi_\lambda \psi_{\lambda-1}} + \frac{\phi_\lambda - 1}{\psi_\lambda - 1} \\ &= \frac{s_{\lambda-1} s_{\lambda-2} \cdots s}{\psi_\lambda \psi_{\lambda-1}} + \frac{s_{\lambda-2} \cdots s}{\psi_{\lambda-1} \psi_{\lambda-2}} + \cdots + \frac{s}{\psi_1 \psi_0}. \end{aligned}$$

From the relation

$$f_1 \psi_\lambda - f \phi_\lambda = f_{\lambda+1},$$

we have

$$f_1/f = \phi_\lambda/\psi_\lambda + f_{\lambda+1}/f\psi_\lambda.$$

If we put  $\lambda = r$ , then since  $f_{r-1} = 0$ , it follows that

$$f_1/f = s/\psi_0 \psi_1 + s s_1/\psi_1 \psi_2 + \cdots + s s_1 \cdots s_{r-1}/\psi_{r-1} \psi_r.$$

ART. 17. It is important to determine the degrees of the functions  $\psi_i(x)$  and  $\phi_i(x)$  ( $i = 1, 2, \dots, r-1$ ). Let the degrees of  $f(x)$  and  $f_1(x)$  be respectively  $n$  and  $n - n_1$  where ( $n_1 \geq 0$ ). Denoting the degree of any function  $g(x)$  by  $[g]$ , we have  $[f] = n$ ,  $[f_1] = n - n_1$ ,  $\dots$ ,  $[f_\lambda] = n - n_\lambda$ ,  $\dots$ ,  $[f_r] = n - n_r$ , where  $0 \leq n_1 < n_2 < n_3 < \cdots < n_r \leq n$ . It follows at once from the formulas of Art. 14 that

$$\begin{aligned} [q_1] &= n_1, [q_2] = n_2 - n_1, \dots, \\ [q_\lambda] &= n_\lambda - n_{\lambda-1}, \dots, [q_r] = n_r - n_{r-1}, \end{aligned}$$

and from Art. 15 that

$$\begin{aligned} [\psi_1] &= n_1, [\psi_2] = n_2, \dots, [\psi_\lambda] = n_\lambda, \dots, [\psi_{r-1}] = n_{r-1}; \\ [\phi_1] &= 0, [\phi_2] = n_2 - n_1, \dots, \\ [\phi_\lambda] &= n_\lambda - n_1, \dots, [\phi_{r-1}] = n_{r-1} - n_1. \end{aligned}$$

From above it was seen that

$$n_{r-1} < n_r \leq n, \text{ so that } n_{r-1} - n_1 \leq n - n_1 - 1.$$

We may therefore assert: *If the function  $f_r(x)$  is the greatest common divisor of the two functions  $f(x)$  and  $f_1(x)$ , we may always determine two functions  $\psi_{r-1}(x)$  and  $\phi_{r-1}(x)$  such that*

$$f_1(x)\psi_{r-1}(x) - f(x)\phi_{r-1}(x) = f_r(x),$$

where the degree of  $\psi_{r-1}(x)$  is at most  $n-1$  and that of  $\phi_{r-1}(x)$  is at most  $n-n_1-1$ .

**ART. 18. Lagrange's Interpolation<sup>1</sup> Formula.** Suppose that  $f(x)$  is an integral function of the  $n$ th degree with rational coefficients. If for  $n+1$  different values ascribed to the variable, say  $x_0, x_1, \dots, x_n$  the  $n+1$  values of the function  $f(x_0), f(x_1), \dots, f(x_n)$  are known, then  $f(x)$  may be completely determined. For write

$$f_i(x) = f(x_i) \times \frac{(x-x_0)(x-x_1)\dots(x-x_n)}{(x_i-x_0)(x_i-x_1)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)} \cdot \frac{1}{x-x_i} \quad (i=0, 1, \dots, n),$$

and note that  $f_i(x)$  is equal to  $f(x_i)$  for  $x=x_i$  and is zero for the other  $n$  ascribed values of  $x$ . For brevity, put

$$(x-x_0)(x-x_1)\dots(x-x_n) = \phi(x).$$

We then have

$$f_i(x) = f(x_i) \frac{\phi(x)}{(x-x_i)\phi'(x_i)}.$$

Further write

$$F(x) = \sum_{i=0}^{i=n} f_i(x) = \sum_{i=0}^{i=n} f(x_i) \frac{\phi(x)}{\phi'(x_i)(x-x_i)}.$$

It is seen that  $f(x)$  is identical with  $F(x)$ , since two

<sup>1</sup> Lagrange's *Oeuvres*, T. 7, p. 285; see also Hermite, "Sur l'interpolation," *Comp. Rendus*, 1859, T. 48, p. 62. The word is used by Wallis, *Arithmetica Infinitorum*, Oxford, 1655.

functions of the  $n$ th degree which are equal for  $n+1$  values of the variable are identically equal.

ART. 19. **The Resultant.** Let

$$f(x) = a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m$$

$$= a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)$$

$$g(x) = b_0x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n$$

$$= b_0(x - \beta_1)(x - \beta_2) \dots (x - \beta_n)$$

be two integral functions in  $x$  with rational coefficients. It is required to find the condition that the two functions have a common divisor. As this divisor must be at least of the first degree in  $x$ , we must derive the condition that the two equations

$$f(x) = 0 \quad \text{and} \quad g(x) = 0$$

have at least one common root.

It follows that one of the quantities  $\alpha$  must equal one of the quantities  $\beta$  and consequently also that

$$0 = R_{f,g},$$

where we define  $R_{f,g}$  as the product of the following  $m \cdot n$  differences of roots:

$$R_{f,g} = a_0^n b_0^m (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \dots (\alpha_1 - \beta_n)$$

$$(\alpha_2 - \beta_1)(\alpha_2 - \beta_2) \dots (\alpha_2 - \beta_n)$$

$$\dots \dots \dots$$

$$(\alpha_m - \beta_1)(\alpha_m - \beta_2) \dots (\alpha_m - \beta_n)$$

$$= a_0^n g(\alpha_1)g(\alpha_2) \dots g(\alpha_m)$$

$$= (-1)^{m \cdot n} b_0^m f(\beta_1)f(\beta_2) \dots f(\beta_n).$$

The expression  $R_{f,g}$  is called the *resultant* of the two functions  $f(x)$  and  $g(x)$  and its vanishing is the condition that the two functions have a common factor.

ART. 20. The resultant may be expressed as an integral function of the coefficients of  $f(x)$  and  $g(x)$  in determinative form as follows:



Form  $n$  identical equations by multiplying the expression

$$a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m - f(x) \equiv 0$$

respectively by  $x^{n-1}, x^{n-2}, \dots, x, 1$ ; and then form  $m$  other equations by multiplying

$$b_0x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n = 0$$

respectively by  $x^{m-1}, x^{m-2}, \dots, x, 1$ . The  $m+n$  equations as shown on insert facing this page, thus present themselves.

These  $m+n$  equations are satisfied by the values  $x = \beta_1, x = \beta_2, \dots, x = \beta_n$ . If then we write  $t = f(x)$ , it is seen that the determinant

$a_0, a_1, a_2, \dots$	$a_{m-2}, a_{m-1}, a_m - t, 0, 0, 0, \dots, 0, 0$
$0, a_0, a_1, \dots$	$a_{m-3}, a_{m-2}, a_{m-1}, a_m - t, 0, 0, \dots, 0, 0$
$0, 0, a_0, \dots$	$a_{m-4}, a_{m-3}, a_{m-2}, a_m - t, 0, 0, \dots, 0, 0$
.....	
$a_0, a_1, \dots$	$0, \dots, a_{m-1}, a_m - t$
$b_0, b_1, b_2, \dots$	$b_{n-1}, b_n, 0$
$0, b_0, b_1, \dots$	$b_{n-2}, b_{n-1}, b_n$
.....	
$0, 0, 0, \dots$	$b_0, b_1, b_2, \dots, b_n, 0$
$0, 0, 0, \dots$	$0, b_0, b_1, \dots, b_{n-1}, b_n$

is a function of the  $n$ th degree in  $t$ , whose roots are

$$t_1 = f(\beta_1), t_2 = f(\beta_2), \dots, t_n = f(\beta_n).$$

The product of the roots in this equation is equal to the constant term divided by the coefficient of  $t^n$ . The coefficient of  $(-t)^n$  is  $(-1)^{m \cdot n} b_0^m$ , while the constant term is  $D$ , where

$$D = \begin{vmatrix} a_0, a_1, a_2, \dots & a_m, 0, 0, \dots, 0, 0 \\ 0, a_0, a_1, \dots & a_{m-1}, a_m, 0, \dots, 0, 0 \\ 0, 0, a_0, \dots & a_{m-2}, a_{m-1}, a_m, \dots, 0, 0 \\ \dots & \dots \\ 0, 0, 0, \dots & a_0, a_1, a_2, \dots, a_{m-1}, a_m \\ b_0, b_1, b_2, \dots & b_{n-1}, b_n, 0, \dots, 0, 0 \\ 0, b_0, b_1, \dots & b_{n-2}, b_{n-1}, b_n, \dots, 0, 0 \\ \dots & \dots \\ 0, 0, 0, \dots & b_1, b_2, b_3, b_4, \dots, b_n, 0 \\ 0, 0, 0, \dots & b_0, b_1, b_2, b_3, \dots, b_{n-1}, b_n \end{vmatrix}$$

It follows that

$$\frac{D}{(-1)^{m \cdot n} b_0^m} = f(\beta_1) f(\beta_2) \cdots f(\beta_n),$$

or

$$\begin{aligned} D &= (-1)^{m \cdot n} b_0^m f(\beta_1) f(\beta_2) \cdots f(\beta_n) = R_{f, g} \\ &= a_0^n g(\alpha_1) g(\alpha_2) \cdots g(\alpha_m). \end{aligned}$$

ART. 21. In the determinant  $D$  multiply the first column by  $x^{m+n-1}$ , the second by  $x^{m+n-2}$ , the third by  $x^{m+n-3}$ ,  $\cdots$ , the next to last by  $x$ , and add all these columns thus multiplied to the last column. If the determinant is then developed with respect to the elements of this last column, it is seen that

$$D = R_{f, g} = f(x)G(x) + g(x)F(x),$$

where  $F(x)$  and  $G(x)$  are definite integral functions in  $x$ , the degree of  $F(x)$  being equal to or less than  $m-1$ , while the degree of  $G(x)$  is at most  $n-1$ . Note that if  $f(x)$  and  $g(x)$  had a common factor, then this factor must be a divisor of  $D$ . And hence,  $D$  being a constant, must be zero, when  $f(x)$  and  $g(x)$  contain a function of  $x$  as a divisor. See also Lagrange's *Addition to Euler's Algebra*, Sect. 4.

ART. 22. **The Discriminant.** If we write

$$\begin{aligned} f(x) &= a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m \\ &= a_0 (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) \\ g(x) &= f'(x), \end{aligned}$$

then from Art. 19 (since here  $n = m - 1$ )

$$R_{f, f'} = a_0^{m-1} f'(\alpha_1) f'(\alpha_2) \cdots f'(\alpha_m).$$

If we put

$$\phi(x) = \frac{f(x)}{a_0} = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m),$$

and write

$$\begin{aligned} \Delta(\alpha_1, \alpha_2, \dots, \alpha_m) &= \prod_{i,j} (\alpha_i - \alpha_j)^2 \binom{i=1, 2, \dots, m-1}{j=2, 3, \dots, m} \\ &= (-1)^{\frac{(m-1)m}{2}} \phi'(\alpha_1)\phi'(\alpha_2)\dots\phi'(\alpha_m) \\ &= (-1)^{\frac{(m-1)m}{2}} \frac{f'(\alpha_1)f'(\alpha_2)\dots f'(\alpha_m)}{a_0^m}, \end{aligned}$$

it follows that

$$R_{f,f'} = (-1)^{\frac{m(m-1)}{2}} a_0^{2m-1} \Delta(\alpha_1, \alpha_2, \dots, \alpha_m).$$

Now if  $R_{f,f'} = 0$ , then is

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_m) = 0,$$

which is the condition that  $f(x)$  and  $f'(x)$  have a common root, and that is, that  $f(x)$  have a *multiple* root. The quantity  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_m)$  is called the *discriminant* of  $f(x)$ .

We also have as in Art. 21

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_m) = f(x)\Phi(x) + f'(x)\Psi(x),$$

where the degree of  $\Phi(x)$  is at most  $m-2$ , while the degree of  $\Psi(x)$  is at most  $m-1$ .

**ART. 23. An Interesting Expression for  $\Delta$ .** Consider the sum of terms

$$\begin{aligned} S &= \alpha_0^k \phi'(\alpha_1)\phi'(\alpha_2)\dots\phi'(\alpha_m) + \alpha_1^k \phi'(\alpha_0)\phi'(\alpha_2)\dots\phi'(\alpha_m) \\ &\quad + \dots + \alpha_m^k \phi'(\alpha_0)\phi'(\alpha_1)\dots\phi'(\alpha_{m-1}), \end{aligned}$$

where  $\phi(x)$  is defined in the preceding article, and note that  $\phi'(\alpha_0)$  is divisible by  $\alpha_0 - \alpha_1$  as is also  $\phi'(\alpha_1)$ . It is further seen that all the terms in  $S$  are divisible by  $(\alpha_0 - \alpha_1)^2$  except the first two and these two terms may be written

$$(\alpha_0 - \alpha_1)\phi'(\alpha_2)\phi'(\alpha_3)\dots\phi'(\alpha_m) [\alpha_1^k(\alpha_0 - \alpha_2)\dots(\alpha_0 - \alpha_m) - \alpha_0^k(\alpha_1 - \alpha_2)\dots(\alpha_1 - \alpha_m)].$$

The quantity within the brackets vanishes for  $\alpha_1 = \alpha_0$  and is therefore divisible by  $\alpha_0 - \alpha_1$  and consequently

$S$  is divisible by  $(\alpha_0 - \alpha_1)^2$ . Similarly it may be shown that  $S$  is divisible by

$$\begin{aligned} \Delta(\alpha_0, \alpha_1, \dots, \alpha_m) &= \prod_{i,j} (\alpha_i - \alpha_j)^2 \binom{i=0, 1, \dots, m-1}{j=1, 2, \dots, m} \\ &\hspace{15em} i < j \\ &= (-1)^{\frac{m(m-1)}{2}} \phi'(\alpha_0) \phi'(\alpha_1) \dots \phi'(\alpha_m). \end{aligned}$$

Since the dimension of  $S$  in the quantities  $\alpha_0, \alpha_1, \dots, \alpha_m$  is  $m^2 + k$  while that of  $\Delta$  is  $m^2 + m$ , it follows, since  $S$  is divisible by  $\Delta$ , that  $S = 0$  for  $k = 0, 1, \dots, m - 1$ , and consequently  $S/\Delta = 0$  for these values of  $k$ . On the other hand  $S/\Delta = \text{constant}$  for  $k = m$ . If then we write  $S = \Delta \cdot C$  and equate like powers  $\alpha_0^{m^2+m}$ , it is seen that  $C = 1$  and that

$$S = \Delta.$$

**ART. 24. The Fundamental Theorem.** In the theory of rational integers, the fundamental theorem is that every integer admits factorization into its prime factors in only one way. The proof of this theorem depends upon the Euclid Algorithm. This algorithm for the determination of the greatest common divisor of two integral functions of  $x$  was given in Art. 14.

For two positive integers  $a$  and  $b$  a similar method is as follows (Euclid, Liber VII, 2): We may take  $b$  less than  $a$ . If  $q$  is the quotient of the division of  $a$  by  $b$ , and if  $r$  is the remainder, we may write

$$a = bq + r,$$

and similarly,

$$b = rq_1 + r_1,$$

$$r = r_1q_2 + r_2,$$

.....

.....

$$r_{n-2} = r_{n-1}q_n + r_n.$$

Since  $r > r_1 > r_2 > \dots > r_n$ , the  $r$ 's being positive integers, we finally reach a remainder  $r_n$  which is either unity or zero.



If  $r_n = 1$ , the two integers  $a$  and  $b$  are relatively prime and by proceeding as in Art. 15, two integers  $m$  and  $n$  may be found such that

$$ma + nb = 1.$$

If  $r_n = 0$  and  $r_{n-1} > 1$ , it is seen that  $r_{n-2}$  is divisible by  $r_{n-1}$  as are also  $r_{n-3}, r_{n-4}, \dots, r, b, a$ . In this case  $r_{n-1} = d$  is the greatest common divisor of  $a$  and  $b$  and as seen in Art. 15 two integers  $k$  and  $l$  may be found such that

$$ka + lb = d.$$

The greatest common divisor  $d$  of two integers  $a$  and  $b$  may be written  $(a, b) = d$ , and in particular, if  $a$  and  $b$  are relatively prime,  $(a, b) = 1$ .

**COROLLARY.** If  $(a, b) = 1$  and if  $c$  is any third integer, then every common divisor of  $ca$  and  $b$  is a common divisor of  $c$  and  $b$ .

This is evident if the equations above are each multiplied by  $c$ , thus giving

$$\begin{aligned} ac &= bcq + rc, \\ bc &= rcq_1 + r_1c, \\ rc &= r_1cq_2 + r_2c, \\ &\dots\dots\dots \\ &\dots\dots\dots \\ r_{n-2}c &= r_{n-1}cq_n + r_nc, \end{aligned}$$

where

$$r_n = 1.$$

It is evident that any divisor of  $ac$  and  $b$  in the first of the above equations also divides  $rc$ , and is also a divisor of  $r_1c$  in the second equation, as it is of  $r_2c, \dots, r_{n-1}c, r_nc = c$ . This is also seen from the fact that since  $(a, b) = 1$  we may write  $ma + nb = 1$  or  $mac + nbc = c$ . Hence, every divisor of  $ac$  and  $b$  on the left hand side is a divisor of  $c$  on the right hand side.

It follows that if  $(a, c) = 1$  and  $(b, c) = 1$ , then  $(ab, c) = 1$ ; and if  $(ab, p) = p$ , then either  $(a, p) = p$ , or  $(b, p) = p$ . From this it follows that: *A positive integer  $a$  may be decomposed into its positive prime factors in only one way.* And this is the *fundamental theorem*.

For, if

$$a = p_1^{h_1} p_2^{h_2} p_3^{h_3} \cdots = q_1^{k_1} q_2^{k_2} q_3^{k_3} \cdots,$$

where the  $p$ 's and  $q$ 's are prime integers, the  $h$ 's and  $k$ 's being positive integers, then from the theorem just proved, one of the  $p$ 's on one side must equal to one of the  $q$ 's on the other side, and vice versa.

ART. 25. *If  $a_1, a_2, \dots, a_n$  are  $n$  positive integers and if  $a_{ij}$  is the greatest common divisor of  $a_i$  and  $a_j$ , and if further  $d_\nu$  is the greatest common divisor of all products of every  $\nu$  of these numbers ( $\nu = 1, 2, \dots, n-1$ ), then is*

$$(1) \quad \prod_{i,j} a_{ij} = d_1 d_2 \cdots d_{n-1} \left( \begin{matrix} i=1, 2, \dots, n \\ j=2, 3, \dots, n \\ j > i \end{matrix} \right).$$

For let  $p$  be a prime number that enters  $a_i$  to the  $k_i$  power and arrange the numbers  $a_1, a_2, \dots, a_n$  so that  $k_1 \leq k_2 \leq k_3 \leq \dots \leq k_n$ ; then  $p$  appears in  $a_{i,j}$  to the  $k_i$  power and consequently in the product  $\prod a_{i,j}$  to the power  $(n-1)k_1 + (n-2)k_2 + \dots + 1 \cdot k_{n-1}$ . On the other hand  $p$  appears in  $d_1$  to the  $k_1$  power, in  $d_2$  to the  $(k_1 + k_2)$  power, in  $d_3$  to the  $(k_1 + k_2 + k_3)$  power, in  $d_{n-1}$  to the  $(k_1 + k_2 + \dots + k_{n-1})$  power. It follows that  $p$  appears to the same power on either side of the formula (1) with which the correctness of the theorem is established. It is seen in Art. 127 that the analogous theorem is true for moduls.

ART. 26. **A Fundamental Theorem in Linear Forms.** A homogeneous linear form in  $n$  variables is an expression

$$f = a_1 x_1 + a_2 x_2 + \dots + a_n x_n,$$

in which the  $a$ 's are constant coefficients and the  $x$ 's are variables.

If there are  $n$  such linear forms

$$f_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \quad (i=1, 2, \dots, n),$$

the determinant of the  $n^2$  coefficients of these forms

$$\Delta = (a_{11}, a_{22}, \dots, a_{nn})$$

is called the *determinant* of the  $n$  forms.

**THE MINKOWSKI<sup>1</sup> THEOREM.** *If  $f_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n$  ( $i=1, 2, \dots, n$ ) are  $n$  homogeneous linear forms with real coefficients and with determinant  $+1$ , it is always possible to determine  $n$  rational integers for  $x_1$  to  $x_n$  in such a way that*

$$|f_1| \leq 1, |f_2| \leq 1, \dots, |f_n| \leq 1.$$

The following proof due to Hilbert (1890–1891) is given for the case  $n=3$ , and then it is not difficult to pass to the general proof.

The proof is presented in three parts:

1°. Let the *normal* form of three forms  $f_1, f_2, f_3$  be defined by

$$f_1 = \frac{x_1}{h_1}, f_2 = \frac{x_2}{h_2}, f_3 = c_1x_1 + c_2x_2 + h_1h_2x_3,$$

where  $h_1$  and  $h_2$  are rational integers and  $c_1, c_2$  are arbitrary real quantities. Note that  $\Delta=1$ . The integers  $h_1, h_2$  may be taken positive, as the integers  $x_1$  and  $x_2$  are susceptible of either positive or negative integral rational values. Now write for  $x_1$  any one of the integers

$0, \pm 1, \pm 2, \dots, \pm \frac{h_1}{2}$  when  $h_1$  is an even integer, and

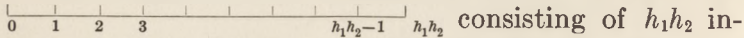
$0, \pm 1, \pm 2, \dots, \pm \frac{h_1-1}{2}, \pm \frac{h_1+1}{2}$ , when  $h_1$  is odd; similarly write for  $x_2$  any of the integers  $0, \pm 1, \dots, \pm \frac{h_2}{2}$

<sup>1</sup> *Geometrie der Zahlen*, p. 104.

when  $h_2$  is even, and  $0, \pm 1, \dots, \pm \frac{h_2-1}{2}, + \frac{h_2+1}{2}$  when  $h_2$  is odd. We thus have  $(h_1+1)(h_2+1)$  combinations of values of  $x_1$  and  $x_2$  for which  $f_1 \leq \frac{1}{2}$  or  $\leq \frac{1}{2} + \frac{1}{2h_1}$  and at the same time  $f_2 \leq \frac{1}{2}$  or  $\leq \frac{1}{2} + \frac{1}{2h_2}$ . Corresponding to each of these  $N = (h_1+1)(h_2+1)$  combinations of values of  $x_1, x_2$ , we may so choose  $x_3$  as a rational integer that

$$f_3 = h_1 h_2 \left[ \frac{c_1 x_1 + c_2 x_2}{h_1 h_2} + x_3 \right]$$

has a value situated between 0 and  $h_1 h_2$ ; for we have only to give  $x_3$  an integral value such that  $\frac{c_1 x_1 + c_2 x_2}{h_1 h_2} + x_3$  is situated between 0 and 1.

The integer  $h_1 h_2$  may be marked off on a straight line  consisting of  $h_1 h_2$  intervals of unit length. As there are  $N = (h_1+1)(h_2+1)$  combinations of values of  $x_1, x_2$ , it is seen that for these combinations there is more than one value of  $f_3$  that must fall within at least one of the intervals. Suppose then that  $x_1 = a_1, x_2 = a_2, x_3 = a_3$ , and  $x_1 = b_1, x_2 = b_2, x_3 = b_3$  are two of the above combinations of values of  $x_1, x_2$  that cause  $f_3$  to fall within one and the same interval and denote the corresponding values of  $f_3$  by  $f_3'$  and  $f_3''$  so that  $f_3' = c_1 a_1 + c_2 a_2 + h_1 h_2 a_3$  and  $f_3'' = c_1 b_1 + c_2 b_2 + h_1 h_2 b_3$ . Since  $f_3'$  and  $f_3''$  fall within a unit interval, it is seen that

$$|f_3' - f_3''| \leq 1,$$

and that is

$$|c_1(a_1 - b_1) + c_2(a_2 - b_2) + h_1 h_2(a_3 - b_3)| \leq 1,$$

where  $a_3 - b_3$  is an integer, while  $a_1 - b_1, a_2 - b_2$  are integral values of  $x_1, x_2$  that are found among the  $N$  combinations of values initially allotted to  $x_1, x_2$  so that  $|a_1 - b_1| \leq h_1,$



$|a_2 - b_2| \leq h_2$ . And these values make  $|f_1| \leq 1$  and  $|f_2| \leq 1$ .

2°. Next let

$$(1) \quad f_i = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 \quad (i=1, 2, 3)$$

be three linear forms with arbitrary *real* coefficients and determinant  $\Delta = 1$ . The transformation

$$(T) \quad x_i = l_{i1}y_1 + l_{i2}y_2 + l_{i3}y_3$$

in which the  $l$ 's are integers may be used to transform the  $f$ 's into the normal form above. The determinant of this transformation, namely  $(a_{11}, a_{22}, a_{33})(l_{11}, l_{22}, l_{33})$  must be unity; and that is  $(l_{11}, l_{22}, l_{33})$  must be unity.

From equation (T) it is seen that the  $y$ 's have integral values, if the  $x$ 's are integral, and *vice versa*.

In order that the unit transformation (T) cause  $f_1$  to become  $\frac{y_1}{h_1}$  where  $h_1$  is a rational integer, it is necessary that

$$(l_{11}, l_{22}, l_{33}) = 1, \quad (i)$$

$$a_{11}l_{11} + a_{12}l_{21} + a_{13}l_{31} = \frac{1}{h_1}, \quad (ii)$$

$$a_{11}l_{12} + a_{12}l_{22} + a_{13}l_{32} = 0, \quad (iii)$$

$$a_{11}l_{13} + a_{12}l_{23} + a_{13}l_{33} = 0. \quad (iv)$$

It is evident that (ii) cannot be satisfied if  $a_{11}, a_{12}, a_{13}$  have a greatest common divisor which is *not* of the form  $\frac{1}{h_1}$ . However, we may show as follows that the condi-

tions (i), (ii), (iii), and (iv) are satisfied by other forms which differ from the form (1) by quantities arbitrarily small. Note that the minor of at least one of the quantities  $a_{13}, a_{23}, a_{33}$  in the determinant

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

must be different from zero. Let this be  $a_{11}a_{22} - a_{21}a_{12}$ , the minor of  $a_{33}$ ; and let  $\delta$  be a positive quantity that is arbitrarily small. Then it is always possible to find a quantity  $\epsilon < \delta$ , such that when the coefficients  $a_{11}, a_{12}, \dots, a_{32}$  are varied by quantities  $\epsilon_{11}, \epsilon_{12}, \dots, \epsilon_{32}$  which are all less than  $\epsilon$ , the coefficient  $a_{33}$  need also be varied by a quantity  $\epsilon_{33}$  which is less than  $\delta$ , in order that the determinant of the corresponding forms be  $= 1$ ; that is

$$\begin{vmatrix} a_{11} - \epsilon_{11}, & a_{12} - \epsilon_{12}, & a_{13} - \epsilon_{13} \\ a_{21} - \epsilon_{21}, & a_{22} - \epsilon_{22}, & a_{23} - \epsilon_{23} \\ a_{31} - \epsilon_{31}, & a_{32} - \epsilon_{32}, & a_{33} - \epsilon_{33} \end{vmatrix} = 1.$$

Noting that the determinant  $(a_{11}, a_{22}, a_{33}) = 1$ , if we put each of the quantities  $\epsilon_{11}, \epsilon_{12}, \dots, \epsilon_{32}$ , equal to  $\epsilon$ , excepting  $\epsilon_{33}$  and expand the determinant, it is seen that

$$\epsilon_{33}[A_1 + \epsilon A_2] + \epsilon B_1 + \epsilon^2 B_2 = 0,$$

where  $A_1, A_2, B_1, B_2$  are functions of the coefficients  $a_{11}, \dots, a_{33}$ , and  $A_1 \neq 0$ .

It follows that

$$|\epsilon_{33}| = \left| \frac{\epsilon(B_1 + \epsilon B_2)}{A_1 + \epsilon A_2} \right|.$$

By choosing  $\epsilon$  sufficiently small, it is evident that  $\left| \frac{\epsilon(B_1 + \epsilon B_2)}{A_1 + \epsilon A_2} \right|$  may be made  $< \delta$ .

Suppose next that the coefficients of the function

$$f_1 = a_{11}x_2 + a_{12}x_2 + a_{23}x_3$$

which were hitherto *real* be varied by quantities less than  $\epsilon$  and at the same time are made rational numbers of the form

$$\frac{h_{11}}{h}, \quad \frac{h_{12}}{h}, \quad \frac{h_{13}}{h}.$$

Multiply the numerators and denominators of these quantities by a sufficiently high power of  $H = h_{11}h_{12}h_{13}$

and replace  $a_{11}, a_{12}, a_{13}$  in the form  $f_1$  by

$$\frac{H_{11}}{h_1} = \frac{h_{11}H^n + 1}{hH^n}, \quad \frac{H_{12}}{h_1} = \frac{h_{12}H^n}{hH^n}, \quad \frac{H_{13}}{h_1} = \frac{h_{13}H^n}{hH^n},$$

where these expressions differ from  $a_{11}, a_{12}, a_{13}$  by quantities less than  $\epsilon$ .

Since  $H_{11}, H_{12}, H_{13}$  can have no divisor other than unity, we may apply the transformation ( $T$ ) to the form

$$\varphi_1 = \frac{H_{11}}{h_1}x_1 + \frac{H_{12}}{h_1}x_2 + \frac{H_{13}}{h_1}x_3$$

and determine the coefficients  $l$  of the transformation so that

$$H_{11}l_{11} + H_{12}l_{21} + H_{13}l_{31} = 1, \quad (iia)$$

$$H_{11}l_{12} + H_{12}l_{22} + H_{13}l_{32} = 0, \quad (iia)$$

$$H_{11}l_{13} + H_{12}l_{23} + H_{13}l_{33} = 0. \quad (iva)$$

For, from (iia) and (iva) it is seen that

$$\left. \begin{aligned} H_{11} &= t(l_{22}l_{33} - l_{23}l_{32}), \\ H_{12} &= t(l_{32}l_{13} - l_{12}l_{33}), \\ H_{13} &= t(l_{12}l_{23} - l_{13}l_{22}), \end{aligned} \right\} \quad (v)$$

$t$  being the factor of proportionality.

It follows that

$$t = \frac{H_{11}}{l_{22}l_{33} - l_{23}l_{32}} = \frac{H_{12}}{l_{32}l_{13} - l_{12}l_{33}} = \frac{H_{13}}{l_{12}l_{23} - l_{13}l_{22}}.$$

Since 1 is the greatest common divisor of  $H_{11}, H_{12}$  and  $H_{13}$ , integers  $m, n$  and  $k$  may be found such that  $mH_{11} + nH_{12} + kH_{13} = 1$ , giving  $t = \frac{1}{g}$ , where  $g$  is a rational

integer. Writing this value of  $t$  in (v), it is seen that the differences  $l_{22}l_{33} - l_{23}l_{32}, \dots$ , must each be divisible by  $g$ . After this division the resulting integers must be relatively prime since this is true of  $H_{11}, H_{12}, H_{13}$ . Had the differences  $l_{22}l_{33} - l_{23}l_{32}, \dots$ , been chosen relatively prime initially, it is seen that  $t = 1$ . Suppose that this has

been done and determine values  $l_{11}, l_{21}, l_{31}$ , which satisfy (iia). If in the resulting form the values of  $H_{11}, H_{12}, H_{13}$  from (v) are written, it is seen that  $(l_{11}, l_{22}, l_{33}) = 1$ .

The transformation ( $T$ ) has thus offered the three new forms

$$(2) \quad \begin{cases} f'_1 = \frac{y_1}{h_1}, \\ f'_2 = b_{21}y_1 + b_{22}y_2 + b_{23}y_3, \\ f'_3 = b_{31}y_1 + b_{32}y_2 + b_{33}y_3, \end{cases}$$

where the  $b$ 's are real quantities.

Next determine a positive quantity  $\epsilon_1$  such that by a variation of  $b_{21}, b_{22}, b_{23}$  by quantities less than  $\epsilon_1$ , the corresponding variations of the original coefficients  $a_{21}, a_{22}, a_{23}$  shall be  $\leq \epsilon$ .

Then vary the quantities  $b_{21}, b_{22}, b_{23}$  by quantities less than  $\epsilon_1$  so that  $f'_2$  takes the form

$$\varphi'_2 = \frac{H_{21}}{h_2}y_1 + \frac{H_{22}}{h_2}y_2 + \frac{H_{23}}{h_2}y_3,$$

where the integers  $H_{22}, H_{23}$  have no common divisor save unity and where  $h_2$  and  $H_{21}$  are rational integers.

To the forms  $f'_1, \varphi'_2, f'_3$  apply a new transformation:

$$(T'') \quad \begin{cases} y_1 = z_1 \\ y_2 = m_{21}z_1 + m_{22}z_2 + m_{23}z_3 \\ y_3 = m_{31}z_1 + m_{32}z_2 + m_{33}z_3 \end{cases}$$

with determinant  $m_{22}m_{33} - m_{32}m_{23} = +1$ , where the integers  $m$  satisfy the conditions

$$H_{21} + H_{22}m_{21} + H_{23}m_{31} = 0, \quad (ib)$$

$$H_{22}m_{22} + H_{23}m_{32} = 1, \quad (iib)$$

$$H_{22}m_{23} + H_{23}m_{33} = 0. \quad (iiib)$$

Since the integers  $H_{22}$  and  $H_{23}$  are relatively prime, equation (iib) may be satisfied by integral values of  $m_{22}$  and  $m_{32}$ ; and by writing  $m_{33} = H_{22}$  and  $m_{23} = -H_{23}$  it is

seen that (iib) is satisfied as is also the determinant of the substitution. The transformation ( $T'$ ) offers the three new forms

$$f_1'' = \frac{z_1}{h_1},$$

$$f_2'' = \frac{z_2}{h_2},$$

$$\varphi_3'' = c_{31}z_1 + c_{32}z_2 + c_{33}z_3.$$

Since the determinant of these three forms is  $+1$ , it is seen that  $c_{33} = h_1 h_2$ . We thus have the normal form in which the Minkowski Theorem was proved to be true; that is, there are integral values of  $z_1, z_2, z_3$  which cause each of the forms just written to be less than unity. And by expressing the  $x$ 's in terms of the values of the  $z$ 's it is seen that the same is true of the three linear forms (1), where in these linear forms the coefficients have been varied by quantities less than  $\epsilon$ .

3°. We have finally only to prove that if the theorem is true for the forms

$$(1^1) \quad \varphi_i = (a_{i1} - \epsilon_{i1})x_1 + (a_{i2} - \epsilon_{i2})x_2 + (a_{i3} - \epsilon_{i3})x_3 \quad (i=1, 2, 3),$$

it is also true of the forms

$$(1) \quad f_i = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 \quad (i=1, 2, 3).$$

This may be done as follows:

Solve the equations

$$\varphi_i = w_i \quad (i=1, 2, 3)$$

for values of  $w_i$  which lie between  $-1$  and  $+1$ , with respect to  $x_i$  ( $i=1, 2, 3$ ). The values of  $x_i$  thus derived are all in absolute value less than a finite quantity  $G$ , say. Since, however, there are only a finite number of integral rational numbers whose absolute values are less than  $G$ , there are only a *finite* number of systems of integral values of  $x_1, x_2, x_3$ , for which  $|\varphi_1| < 1, |\varphi_2| < 1, |\varphi_3| < 1$ .



Suppose that for none of these systems the inequalities  $|f_i| \leq 1$  ( $i = 1, 2, 3$ ) exists, but that, for one of the forms  $f_i$ , say,  $|f_k| = 1 + \lambda$ , where  $\lambda$  is a *positive* quantity for all such systems of values.

Now so choose our  $\delta$  as defined above that

$$\delta < \frac{\lambda}{3G}.$$

It was seen that a system of integral values of  $x$ , say  $\xi_1, \xi_2, \xi_3$ , whose absolute values are less than  $G$ , cause  $|\varphi_k|$  to be less than unity, that is

$$(a_{k_1} - \epsilon_{k_1})\xi_1 + (a_{k_2} - \epsilon_{k_2})\xi_2 + (a_{k_3} - \epsilon_{k_3})\xi_3 \leq 1,$$

while

$$a_{k_1}\xi_1 + a_{k_2}\xi_2 + a_{k_3}\xi_3 = 1 + \lambda.$$

It follows that

$$\lambda - (\epsilon_{k_1}\xi_1 + \epsilon_{k_2}\xi_2 + \epsilon_{k_3}\xi_3) \leq 0,$$

or

$$\epsilon_{k_1}\xi_1 + \epsilon_{k_2}\xi_2 + \epsilon_{k_3}\xi_3 \geq \lambda,$$

and therefore also  $3GM \geq \lambda$ , where  $M$  is the largest absolute value of any  $\epsilon$ . But since  $M < \delta$ , this contradicts the value assumed for  $\delta$  above, as well as the assumption that  $\lambda$  is positive for all the system of integral values of  $x_1, x_2, x_3$ .

THEOREM II. *If*

$$f_i = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 \quad (i = 1, 2, 3)$$

*are three linear forms with real coefficients and with the positive determinant  $\Delta$ ; and if further  $w_1, w_2, w_3$  are three positive quantities whose product  $w_1 \cdot w_2 \cdot w_3 = \Delta$ , but which otherwise are quite arbitrary, then it is possible to determine three rational integers  $x_1, x_2, x_3$  for which the three inequalities*

$$|f_1| \leq w_1, \quad |f_2| \leq w_2, \quad |f_3| \leq w_3,$$

*simultaneously exist.*

The correctness of this theorem follows directly from the first theorem. We need only write

$$f_1 = w_1 \varphi_1, \quad f_2 = w_2 \varphi_2, \quad f_3 = w_3 \varphi_3,$$

from which it follows that  $\varphi_1, \varphi_2, \varphi_3$  are three real forms with determinant  $= +1$ .

It follows from the first theorem that integral values may be given to  $x_1, x_2, x_3$  such that

$$|\varphi_1| \leq 1, \quad |\varphi_2| \leq 1, \quad |\varphi_3| \leq 1$$

and consequently also

$$|f_1| \leq w_1, \quad |f_2| \leq w_2, \quad |f_3| \leq w_3.$$

Further, if the three equations  $f_i = c_i$  [ $i = 1, 2, 3$ ] be solved for  $x_1, x_2, x_3$ , we have the theorem:

**THEOREM III.** *If the three linear forms*

$$x_i = A_{i1}c_1 + A_{i2}c_2 + A_{i3}c_3 \quad (i = 1, 2, 3)$$

*have real coefficients with determinant  $+1$ , we may always give to  $c_1, c_2, c_3$  real values which are situated between  $+1$  and  $-1$ , in such a way that  $x_1, x_2, x_3$  are rational integers.*

Note in this connection that if  $\Delta$  is a determinant of the  $n$ th order, its reciprocal determinant  $\Delta' = \Delta^{n-1}$ , so that if  $\Delta = +1$ , then also  $\Delta' = +1$ . The proof given above is a variation of the one found in Sommer, *Vorlesungen über Zahlentheorie*, p. 64, where a reference is made to Hilbert.

**ART. 27.** The following is an ingenious proof of the Minkowski Theorem due to Hurwitz, *Gött. Nachrichten Math. Phys. Kl.*, 1897. See also note by Humbert in the Appendix of the Translation of Hilbert's *Die Theorie der algebraischen Zahlkörper*, by A. Levy and Th. Got.

As the process of the proof is the same for any number of variables, this number will be limited to three as in the preceding articles.

Let the three linear forms be

$$f_i(x) = a_i x + b_i y + c_i z \quad (i=1, 2, 3)$$

with determinant  $\Delta$ , which as above may be taken positive.

If the coefficients  $a_i, b_i, c_i$  ( $i=1, 2, 3$ ) are each divided by  $\sqrt[3]{\Delta}$ , the determinant becomes  $+1$ . Thus in all cases there are three forms, say  $\bar{f}_i(x)$  [ $i=1, 2, 3$ ] with determinant  $= +1$ . To say, then, that for  $x, y, z$  integral values different from zero may be determined such that

$$|\bar{f}_i| \equiv 1 \quad (i=1, 2, 3)$$

is the same as to say that for these values

$$|f_i| \equiv \sqrt[3]{\Delta}$$

( $\sqrt[n]{\Delta}$  in the case of  $n$  forms in  $n$  variables). The proof by Hurwitz is divided into four parts.

*First Part.* Suppose that the coefficients of the  $f_i$  are all integers.

If in the form

$$f_1 = a_1 x + b_1 y + c_1 z$$

the coefficient  $c_1$ , say, is in absolute value as small or smaller than  $a_1$  and  $b_1$ , we may make the substitution

$$x \parallel x, \quad y \parallel y, \quad z \parallel z + \lambda x,$$

a substitution whose determinant is  $+1$ .

This substitution is denoted briefly by  $(z; z + \lambda x)$ . Observe, however, that the variables on the right hand side are not the same as those on the left, although for convenience in notation they are written alike.

By this substitution the coefficient of  $x$  becomes  $a_1 + \lambda c_1$ , and by a proper choice of  $\lambda$ , this coefficient,  $a'_1$  say, may be made to be  $> 0$  and  $\equiv |c_1|$ , while the coefficients of  $y$  and of  $z$  remain unchanged.

Next make the substitution  $(x; x + \nu z)$ , and choose  $\nu$  so as to render the coefficient  $c'_1$ , say, of  $z$  positive and  $\equiv |a'_1|$ . By continuing this process the coefficient of  $z$

may be caused to vanish. Then by a series of similar substitutions ( $y; y + \mu y$ ) we may cause the coefficient of  $y$  to vanish. Due to these substitutions  $f_1(x)$  has become, say,  $F_1(x) = Ax$ , where  $A$  is positive.

The above substitutions have caused the form  $f_2(x)$  to become, say,  $b'x + b_2y + \bar{c}_2z$ . Leaving  $x$  unchanged we may operate with successive substitutions upon  $y$  and  $z$ , and cause the coefficient of  $z$  to vanish, the form  $f_2(x)$  becoming  $b'x + By$  where  $B > 0$ .

Finally making the substitution ( $y; y + \mu x$ ), we may make the resulting coefficient  $b$  of  $x$  positive and  $< B$ , the form thereby becoming

$$F_2(x) = bx + By.$$

Due to these substitutions the form  $f_3(x)$  is, say,

$$\bar{f}_3(x) = c'x + c''y + Cz.$$

Since all the substitutions made have had  $+1$  as determinant, the determinant of the three forms  $F_1(x)$ ,  $F_2(x)$ ,  $\bar{f}_3(x)$ , and that is  $ABC$ , is equal to  $\Delta$ . Hence  $C$  is positive.

Further, in the form  $\bar{f}_3(x)$ , make the substitutions ( $z; z + \lambda x$ ) and ( $z; z + \mu y$ ) and thereby render the coefficients, say  $c_1$  and  $c_2$  of  $x$  and  $y$ , respectively, *positive* and less than  $C$ , the form  $\bar{f}_3(x)$  now being  $F_3(x) = c_1x + c_2y + Cz$ .

Observe finally that the original system of forms  $f_i(x)$  ( $i = 1, 2, 3$ ) have become

$$F_1(x) = Ax \quad A > 0,$$

$$F_2(x) = bx + By \quad B > 0, \quad 0 \leq b < B,$$

$$F_3(x) = c_1x + c_2y + Cz \quad C > 0, \quad 0 \leq c_1 < C, \quad 0 \leq c_2 < C;$$

and note that, since all substitutions have had as determinant  $+1$ , the new variables are integers if the old were, and *vice versa*.

*Second Part.* Two linear homogeneous functions  $\Phi_1(x, y, z)$  and  $\Phi_2(x, y, z)$  with integral coefficients are

said to be *congruent* with respect to  $F_1(x)$ ,  $F_2(x)$ , and  $F_3(x)$  as moduli, if

$$\Phi_1(x, y, z) - \Phi_2(x, y, z) = \lambda_1 F_1 + \lambda_2 F_2 + \lambda_3 F_3,$$

where  $\lambda_1, \lambda_2, \lambda_3$  are any rational integers. The function  $\Phi$  being a fixed linear form with integral coefficients, all functions  $\Phi + \lambda_1 F_1 + \lambda_2 F_2 + \lambda_3 F_3$ , the  $\lambda$ 's being variable integers, are congruent (modd.  $F_1, F_2, F_3$ ).

Consider the function

$$\Psi \equiv \Phi + \lambda_1 F_1 + \lambda_2 F_2 + \lambda_3 F_3,$$

where

$$\Phi = A_1 x + B_1 y + C_1 z,$$

the integers  $A_1, B_1, C_1$  being fixed. In this  $\Psi$ -function choose  $\lambda_3$  so that  $C_1 + \lambda_3 C$  be positive and  $< C$ ; and similarly by suitable selections of  $\lambda_1$  and  $\lambda_2$  cause the coefficients of  $x$  and  $y$  to be *positive* and respectively less than  $A$  and  $B$ .

Such a function  $\Psi$  is said to be *reduced* (modd.  $F_1, F_2, F_3$ ).

Since the coefficient of  $x$  in such a function lies between 0 (inclusive) and  $A$  (exclusive), while that of  $y$  is between 0 (inclusive) and  $B$  (exclusive), and that of  $z$  is between 0 (inclusive) and  $C$  (exclusive), it is evident that there are  $ABC (= \Delta)$  such reduced forms, say  $\Psi_1, \Psi_2, \dots, \Psi_\Delta$ . And every linear form with integral coefficients is congruent (modd.  $F_1, F_2, F_3$ ) to one of these forms.

Thus it is seen that there are  $\Delta$  forms and only  $\Delta$  forms that are incongruent (modd.  $F_1, F_2, F_3$ ), and among them is the form in which all three coefficients are zero. It is clear that there are the same number of incongruent forms (modd.  $f_1, f_2, f_3$ ); for two incongruent forms (modd.  $f_1, f_2, f_3$ ) remain incongruent when they are operated upon by substitutions of determinant  $\pm 1$ .

Next let  $r$  be a positive integer such that  $r^3 \leq \Delta < (r+1)^3$  and consider the forms  $g(x) = l_1 x + l_2 y + l_3 z$ , where  $l_1, l_2, l_3$



may take any of the values 0, 1, 2,  $\dots$ ,  $r$ . It is evident that there are  $(r+1)^3$  such forms. It is also clear that at least two of these functions, say  $g_1(x)$  and  $g_2(x)$  must be congruent (modd.  $f_1, f_2, f_3$ ). And that is,

$$\lambda_1(a_1x + b_1y + c_1z) + \lambda_2(a_2x + b_2y + c_2z) + \lambda_3(a_3x + b_3y + c_3z) \\ = g_1(x) - g_2(x) = t'_1x + t'_2y + t'_3z.$$

Further note that  $t'_1, t'_2,$  and  $t'_3$  are not *all* zero, since  $g_1(x)$  and  $g_2(x)$  are two distinct functions.

It follows that

$$a_1\lambda_1 + a_2\lambda_2 + a_3\lambda_3 = t'_1, \\ b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3 = t'_2, \\ c_1\lambda_1 + c_2\lambda_2 + c_3\lambda_3 = t'_3,$$

where

$$|t'_i| \leq r \quad (i=1, 2, 3).$$

Since  $r \leq \Delta^{\frac{1}{3}}$ , the Theorem of Minkowski is proved for the forms  $f_i(x)$  [ $i=1, 2, 3$ ], whose coefficients are rational integers.

*Third Part.* The theorem is also true if the coefficients of  $f_i(x)$  [ $i=1, 2, 3$ ] are any fractions. For if  $S$  is the least common denominator of all these fractions, we may write

$$f_i(x) = \frac{g_i(x)}{S},$$

where all the coefficients of  $g_i(x)$  are integers.

Observe that the determinant of  $g_i(x)$  [ $i=1, 2, 3$ ] is  $\Delta S^3$ . The theorem being true of forms with integral coefficients, it is possible to find for  $x, y, z$  rational integral values that are not all zero, such that  $|g_i(x)| \leq S\Delta^{\frac{1}{3}}$ ; and for these values of  $x, y, z$  it is also true that  $|f_i(x)| \leq \Delta^{\frac{1}{3}}$ .

*Fourth Part.* Suppose finally that the coefficients  $a_i, b_i, c_i$  of the forms

$$f_i(x) = a_i x + b_i y + c_i z \quad (i=1, 2, 3)$$

are real quantities. As in Art. 26 it is seen that by varying all of these coefficients by quantities less than  $\delta$ ,

where  $\delta$  is an arbitrarily small positive quantity, the functions  $f_i(x)$  become the forms  $\varphi_i(x)$  with determinant  $\Delta$  where

$$\varphi_i(x) = A_i x + B_i y + C_i z \quad (i=1, 2, 3),$$

$A_i, B_i, C_i$  being rational numbers.

From the *third part* above integral values may be assigned to  $x, y, z$  such that  $|\varphi_i(x)| \leq \Delta^{\frac{1}{3}}$  ( $x=1, 2, 3$ ).

For such a system of values it follows also (Art. 26) that

$$|f_i(x)| \leq \Delta^{\frac{1}{3}} \quad (i=1, 2, 3).$$

Minkowski's proof of the theorem for forms in  $n$  variables is found in Vol. II, Chapter 8 of the present treatise.

## CHAPTER II

### THE GENERAL NOTION OF REALMS OF RATIONALITY

ART. 28. In Art. 2 it was seen that all integers constituted a *realm*. These integers may be called *elements* of the realm and the realm may be called a *realm of integrity*.<sup>1</sup> It is evident that the operations of addition, subtraction and multiplication performed with integers upon integers give integers belonging to the realm in question. Hilbert<sup>2</sup> calls such a realm of integrity a *Zahlring* or Ring.

There exists a realm which is constituted solely of the number "zero." This realm we shall once for all exclude.

Take a quantity  $a$  which is different from zero. It is seen that all quantities that are had through rational operations upon  $a$  constitute a *realm* (see Abel, Vol. II, p. 220). Such a realm was called a *realm of rationality* by Kronecker. In the word "realm" we must avoid any notion of space (Kronecker, Vol. II, p. 249). This realm of rationality, or realm as we shall usually denote it for brevity, was called a *body of numbers* (*Körper von Zahlen*, or *Zahlkörper* by Dedekind; see p. 435 of Dirichlet's *Zahlentheorie*, 4<sup>th</sup> Edition). Denote the realm formed by rational operations upon  $a$  by  $\mathfrak{R}(a)$ . It is sometimes denoted by  $\mathfrak{R}(a)$ . It is evident that the quantity  $\frac{a}{a} = 1$  appears in this realm and consequently

<sup>1</sup> See Kronecker, *Grundzüge*, etc., p. 14. We shall denote this paper by the word Kronecker.

<sup>2</sup> Hilbert, *Jahresbericht der deutschen math. Vereinigung*, Vol. IV, p. 237. We shall refer to it as Hilbert, *Bericht*.

also all integral or fractional numbers are found in the realm  $\mathfrak{R}(a)$ . The realm  $\mathfrak{R}(a)$  consisting only of rational functions of  $a$  is closed in itself.

The collectivity or totality of all rational numbers form for themselves a realm. This realm Kronecker (*Grundzüge*, p. 8) called the *absolute realm* of rationality. We denote it by  $\mathfrak{R}(1)$ , or simply by Roman R.

To get by means of an example an insight into what will follow, consider the plane of the complex variable  $z = x + iy$ . This plane is the realm  $\mathfrak{R}(i)$ , where  $i$  is a root of the equation  $x^2 + 1 = 0$ . If  $a$  and  $b$  are two rational numbers, or if, as we shall say,  $a$  and  $b$  are two numbers belonging to the realm  $\mathfrak{R}(1)$ , that is, to the realm of rational numbers, then  $a + ib$  is a number of the realm  $\mathfrak{R}(i)$  and is denoted by a point on the complex plane. If  $c + id$  is any other number of the realm  $\mathfrak{R}(i)$ , any rational combination of  $a + ib$  and  $c + id$  is a quantity of the form  $U + iV$ , where  $U$  and  $V$  are numbers belonging to  $\mathfrak{R}(1)$ . Further  $U + iV$  is represented by some point on the complex plane or is a quantity of the realm  $\mathfrak{R}(i)$ . Observe that all real numbers lie upon the real axis on the plane of the complex variable.

If all the numbers of the realm  $\mathfrak{A}$ , say, also belong to the realm  $\mathfrak{B}$ , we say (Kronecker, p. 9) that  $\mathfrak{A}$  is a *divisor* of  $\mathfrak{B}$  or that  $\mathfrak{B}$  is divisible by  $\mathfrak{A}$ . Every arbitrary realm is consequently divisible by the realm  $\mathfrak{R}(1)$ , that is, by the realm of rational numbers. A realm more general than the absolute realm must contain other quantities besides all rational numbers. If, for example, the realm contains an indeterminate quantity  $u$ , it contains also  $u^2$ ,  $u^3$ ,  $\dots$ , and all integral powers of  $u$ . If  $\phi(u)$  and  $\psi(u)$  are two such functions of  $u$ , the realm contains  $\frac{\phi(u)}{\psi(u)}$  and in short all rational functions of  $u$ .

Such a realm we denote by  $\mathfrak{R}(u)$ . If the realm contains two indeterminate quantities  $u$  and  $v$ , it contains also all rational functions of these quantities with rational coefficients. This realm we denote by  $\mathfrak{R}(u, v)$ , etc.

By  $\mathfrak{I}(1)$  we denote the *realm of integrity* which contains all integers; by  $\mathfrak{I}(u)$  we denote the realm of integrity which contains all integral functions of  $u$  with rational coefficients and by  $\mathfrak{I}(1, u)$  we denote the realm of integrity which contains all integral functions of  $u$  with integral coefficients.

It is evident that  $\mathfrak{R}(u)$  is divisible by  $\mathfrak{I}(u)$  and that  $\mathfrak{I}(u)$  is divisible by  $\mathfrak{I}(1, u)$ .

By  $\mathfrak{I}(u, v)$  we denote the realm of integrity that contains all integral functions of  $u$  and  $v$  with rational coefficients and in the realm  $\mathfrak{I}(1, u, v)$  the coefficients are also integers.

If of two realms  $\mathfrak{R}(u, v, \dots)$  and  $\mathfrak{R}(u', v', \dots)$  the elements  $u, v, \dots$  are rationally expressible through the elements  $u', v', \dots$ , then  $\mathfrak{R}(u, v, \dots)$  is a divisor of  $\mathfrak{R}(u', v', \dots)$ ; if further the elements  $u', v', \dots$  are also rationally expressible through  $u, v, \dots$ , the two realms are *identical*.

We consider any fixed realm as the basis of our investigation. Such a realm may be called the *stock-realm* (*Stammbereich*; see Kronecker, p. 7). It is the realm from which all other realms (and quantities) are produced during the investigation in question. When emphasis is put upon certain quantities  $u, v, \dots$  of this realm it is denoted by  $\mathfrak{R}(u, v, \dots)$ , otherwise simply by  $\mathfrak{R}$ . All quantities that belong to this realm are regarded as *rational*.

Let  $x$  be a variable that is not contained in the realm  $\mathfrak{R}$  and consider two integral functions of  $x$  whose coefficients belong to the fixed realm  $\mathfrak{R}$ . If we multiply two such



functions, it is evident that the coefficients of the product also belong to  $\mathfrak{R}$ . Reciprocally, if a function whose coefficients belong to  $\mathfrak{R}$  is resolvable into two other functions whose coefficients all belong to  $\mathfrak{R}$ , we say that the function is *reducible*, otherwise *irreducible* (cf. Abel, *Works*, Vol. I, p. 479) in the realm  $\mathfrak{R}$ . For example  $x^2 - 4x + 9$  is irreducible in  $\mathfrak{R}(1)$ ; but

$$x^2 - 4x + 9 = (x - (2 + \sqrt{-5}))(x - (2 - \sqrt{-5}))$$

is reducible in  $\mathfrak{R}(\sqrt{-5})$ .

$$x^4 + x^3 + x^2 + x + 1$$

$$= \left(x^2 + \frac{1 + \sqrt{-5}}{2}x + 1\right) \left(x^2 + \frac{1 - \sqrt{-5}}{2}x + 1\right)$$

is irreducible in  $\mathfrak{R}(1)$ , reducible in  $\mathfrak{R}(\sqrt{-5})$ .

#### EXAMPLES

1. Show that  $x^6 - 1$  may be decomposed into linear factors in  $R(\sqrt{-3})$ .

2. It was proved that  $\frac{x^n - 1}{x - 1}$  is irreducible in  $\mathfrak{R}(1)$ , if  $n$  is a prime integer (Art. 12). Show that this function is reducible in  $\mathfrak{R}\left(\cos \frac{2\pi}{n}\right)$ . It may also be observed that if  $\alpha$  is a root, other than unity of  $x^p - 1 = 0$ , then other roots are  $\alpha, \alpha^2, \dots, \alpha^{p-1}, \alpha^p = 1$ , so that  $\frac{x^p - 1}{x - 1} = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{p-1})$ ; or writing  $x = 1$ ,

$$p = 1(1 - \alpha)(1 - \alpha^2) \cdots (1 - \alpha^{p-1}).$$

It is seen from Ex. 2 that  $p$ , an irreducible prime in  $R$ , may be decomposed into  $p$  factors in  $\mathfrak{R}(\alpha)$ . We shall see later (Art. 105) that these factors are *algebraic* integers in  $\mathfrak{R}(\alpha)$ .

ART. 29. To fix the ideas let us consider some of the theorems of Chap. I in more extended realms of rationality, the proofs here being practically the same as there.

Take first a function  $P = P(u)$  integral in  $u$  whose coefficients are rational numbers, that is, let  $P(u)$  belong to the realm  $\mathfrak{Z}(u)$ . If  $P(u)$  is irreducible in the realm  $\mathfrak{R}(1)$ , we say it is a *prime* function in this realm although it may contain as a factor a *constant*. The quantity  $u$  may be looked upon as having definite values in the function  $P(u)$  and is introduced as an element in the realm of rationality  $\mathfrak{Z}(u)$ . Such a quantity  $u$  may be called an *indeterminate* to distinguish it from a variable  $x$  which never enters as such as an element in a realm of rationality.

Let  $g(u)$  and  $h(u)$  be two other functions of the indeterminate  $u$  which belong to the realm  $\mathfrak{Z}(u)$ . Denote them by  $A$  and  $B$  respectively.

**THEOREM:** *If the product  $A \cdot B$  is divisible by the prime function  $P$ , one of the factors  $A$  or  $B$  is divisible by  $P$ .* For suppose that  $A$  is *not* divisible by  $P$ . Then  $A$  and  $P$  are *relatively prime*; that is, they have no common divisor which is a function of  $u$ . For suppose they had a greatest common divisor, say  $\phi(u)$ . Denote this divisor by  $D$ , where  $D$  is an integral function in  $u$  whose coefficients are rational numbers. It would follow that  $P$  is divisible by  $D$ . But since  $P$  in the realm of all rational numbers is irreducible, it follows *either* that  $P = D$  or that  $D$  is a constant. But since  $A$  is supposed *not* to be divisible by  $P$ , the case  $P = D$  must be excluded. If then  $A \cdot B$  is divisible by  $P$ , the factor  $B$  must be divisible by  $P$ . Suppose further that  $P(u)$  is also a *primitive* function in  $\mathfrak{Z}(1, u)$ , that is, a function with integral coefficients whose greatest common divisor is unity. We also assume as above that  $P(u)$  is irreducible in the realm  $\mathfrak{R}(1)$ , and is called a *prime* function. If then  $A \cdot B$  is divisible by  $P$  and if  $A$  is not divisible by  $P$ , then  $B/P$  is an integral function with integral coefficients provided the coefficients of  $B$  are integral.

ART. 30. Consider next an integral function in  $x$  and  $u$ , say

$$f(x, u) = A_0 + A_1x + A_2x^2 + \dots,$$

where  $A_0, A_1, \dots$ , are integral functions in  $u$  with rational coefficients. The  $A$ 's therefore belong to the realm  $\mathfrak{F}(u)$ . Suppose as above that  $P(u)$  is irreducible in  $\mathfrak{R}(1)$  and further that  $f(x, u)$  is divisible by  $P$ ; in other words, let  $f(x, u)/P = g(x, u)$  where  $g(x, u)$  is an integral function in  $x$ , whose coefficients belong to  $\mathfrak{F}(u)$ . We may then write

$$f(x, u)/P = A_0/P + A_1/Px + A_2/Px^2 + \dots,$$

and from the preceding article it follows that  $A_0/P, A_1/P, \dots$  are integral functions in  $u$  with rational coefficients. We may state this in the following theorem: *If a function  $f(x, u)$  integral in  $x$  and  $u$  with rational coefficients is divisible by a prime function  $P(u)$ , then all the coefficients of this function arranged according to powers of  $x$  are divisible by  $P(u)$ .*

Further since any integral function in  $u$ , say  $Q(u)$ , may be resolved into a product of prime functions, and as the theorem is true for all of these prime functions it is also true if in the place of  $P(u)$  in the statement of the theorem we write  $Q(u)$ .

If we have two functions  $f(x, u)$  and  $g(x, u)$  integral in  $x$ , whose coefficients belong to the realm  $\mathfrak{F}(u)$ , then we may write as in Art. 3

$$f(x, u) \equiv g(x, u) [\text{mod. } P(u)],$$

if  $f(x, u) - g(x, u)$  is divisible by  $P(u)$ .

ART. 31. **Generalization of the Gaussian Lemma.**  
**THEOREM.** *Suppose that  $f(x, u)$  and  $g(x, u)$  are two given integral functions in  $x$  and  $u$ . If the product  $f(x, u)g(x, u)$  is divisible by  $P(u)$ , then one of the factors is divisible by*

$P(u)$ . The proof of this theorem is similar to the one given in Art. 4.

Let

$$f(x, u) = A_0 + A_1x + A_2x^2 + \dots,$$

$$g(x, u) = B_0 + B_1x + B_2x^2 + \dots,$$

where  $A_0, A_1, \dots, B_0, B_1, \dots$  belong to the realm  $\mathfrak{F}(u)$ . We assume, of course, as in the two preceding articles, that  $P(u)$  is irreducible in the realm  $\mathfrak{R}(1)$ .

The theorem may be indirectly proved by showing that if neither of the factors is divisible by  $P(u)$ , then their quotient is *not* divisible by  $P(u)$ . In  $f(x, u)$  suppose that the coefficients  $A_0, A_1, \dots, A_{r-1}$  are divisible by  $P(u)$ , but that  $A_r$  is *not* divisible by  $P(u)$ ; and further suppose that the coefficients  $B_0, B_1, \dots, B_{s-1}$  are divisible by  $P(u)$ , but that  $B_s$  is *not* divisible by  $P(u)$ . The coefficient of  $x^{r+s}$  in the quotient is  $A_0B_{s+r} + A_1B_{s+r-1} + \dots + A_rB_s + A_{r+1}B_{s-1} + \dots + A_{r+s}B_0$ . In this sum all the summands are divisible by  $P(u)$  except  $A_rB_s$ . It follows then that the product of the two factors of  $f(x, u)$  and  $g(x, u)$  is *not* divisible by  $P(u)$ .

ART. 32. We may next introduce the notion of *divisor* for such functions. Again write

$$f(x, u) = A_0 + A_1x + A_2x^2 + \dots,$$

where it is supposed that the coefficients  $A_0, A_1, \dots$  are integral or rational functions of  $u$ . Then as in Art. 7 a function  $t=t(u)$  may always be determined such that

$$F(x, u) = \frac{f(x, u)}{t(u)} = C_0 + C_1x + C_2x^2 + \dots,$$

where the  $C$ 's are *integral* functions in  $u$  and have no common divisor other than possibly a constant. The function  $F(x, u)$  is said to be *primitive* with respect to the realm  $\mathfrak{F}(u)$  and  $t$  is called the *divisor* of  $f(x, u)$ . It is also possible so to choose the *divisor* that the  $C$ 's are integral

functions in  $u$  with integral coefficients which have no common divisor other than unity. The corresponding function  $F(x, u)$  is then *primitive* with respect to the realm  $\mathfrak{S}(1, u)$ . In most cases the nature of the coefficients is disregarded, and we shall therefore (cf. Kronecker, *Grundzüge*, p. 4) employ the first definition as that of a *primitive* function. We have already (Art. 29) disregarded the constant factor in the definition of a prime function.

We have the theorem: *The product of two primitive functions of  $x$  and  $u$  is a primitive function; and the divisor of the product of two primitive functions is the product of the divisors of these functions.* These theorems are true for both the realms  $\mathfrak{S}(u)$  and  $\mathfrak{S}(1, u)$ . The following theorems may also be proved: *If  $f(x, u)$  and  $g(x, u)$  are integral functions in  $x$  and  $u$  whose coefficients are rational numbers, if further  $g(x, u)$  is a primitive function in  $\mathfrak{S}(u)$  and if  $\frac{f(x, u)}{g(x, u)}$  is an integral function in  $x$ , it is also an integral function in  $u$  (cf. Art. 7).*

From this we have further: *If an integral function in  $x$  and  $u$  is resolvable into two factors integral in  $x$  and rational in  $u$ , it is also resolvable into two factors that are integral in both  $x$  and  $u$ .* In other words: *If an integral function in  $x$  whose coefficients belong to the realm  $\mathfrak{S}(u)$  is resolvable into factors whose coefficients belong to the realm  $\mathfrak{R}(u)$ , the function may be resolved into factors whose coefficients belong to the realm  $\mathfrak{S}(u)$ ; and further if an integral function in  $x$  whose coefficients belong to the realm  $\mathfrak{S}(1, u)$  is resolvable into factors whose coefficients belong to the realm  $\mathfrak{R}(u)$ , it is also resolvable into factors whose coefficients belong to the realm  $\mathfrak{S}(1, u)$ .*

Let  $f(x, u)$  be an integral function in both  $x$  and  $u$  in which the coefficient of the highest power of  $x$  is unity and



let  $g(x, u)$  be an integral function in  $x$  in which the coefficient of the highest power of  $x$  is unity while the remaining coefficients are rational functions of  $u$  and finally suppose that  $\frac{f(x, u)}{g(x, u)}$  is an integral function of  $x$ , then also in  $g(x, u)$  the coefficients of  $x$  must all be integral functions of  $u$  (see Art. 9). Similarly, if  $f(x, u)$  is an integral function in  $x$  whose coefficients belong to  $\mathfrak{Z}(1, u)$  and the coefficient of the highest power of  $x$  is unity; if further in  $g(x, u)$  the coefficient of the highest power of  $x$  is unity and the other coefficients belong to  $\mathfrak{R}(u)$  and if  $\frac{f(x, u)}{g(x, u)}$  is an integral function of  $x$ , then also in  $g(x, u)$  the coefficients of  $x$  belong to  $\mathfrak{Z}(1, u)$ .

ART. 33. The above theory may be extended to the case where there are present two indeterminates  $u$  and  $v$ . Let  $P$  be an integral function in  $u$  and  $v$  whose coefficients are rational numbers. We further assume that  $P$  cannot be resolved into two integral functions of  $u$  and  $v$  with rational coefficients. In other words  $P(u, v)$  belongs to the realm  $\mathfrak{Z}(u, v)$  and considered as a function of  $u$  is irreducible in the realm  $\mathfrak{R}(v)$  and therefore also in  $\mathfrak{Z}(v)$  (Art. 32). The function  $P(u, v)$  is then said to be a *prime* function in the realm  $\mathfrak{R}(u, v)$ . It may have as a factor a constant term, which is independent of both  $u$  and  $v$ . Let  $g(u, v)$  be a second function which may be denoted by  $A$ . If  $A$  is *not* divisible by  $P$ , then considered as functions of  $u$  alone  $A$  and  $P$  must be *relatively prime*. For if considered as functions of  $u$  the functions  $A$  and  $P$  had a greatest common divisor  $D$ , then we must have  $P = D \cdot E$  where  $D$  and  $E$  are integral functions of  $u$  with coefficients that are rational in  $v$ . But  $P$  in the realm  $\mathfrak{R}(v)$  is irreducible. It follows that either  $D = P$  or that  $D$  is a constant. But  $P$  cannot equal  $D$ , for in that case

$A$  would be divisible by  $P$  which is contrary to our hypothesis.

ART. 34. Suppose that  $A$  and  $B$  as above are functions that belong to the realm  $\mathfrak{F}(u, v)$  and let  $P = P(u, v)$  be a prime function. If the product  $A \cdot B$  is divisible by  $P$  and if considered as functions of  $u$ ,  $A$  and  $P$  are relative prime, it follows that  $B$  must be divisible by  $P$  or  $\frac{B}{P}$  is an integral function in  $u$ . Further if  $P$  considered as a function of  $u$  is a primitive function with respect to the realm  $\mathfrak{R}(v)$  (Art. 32), it is seen that  $\frac{B}{P}$  is an integral function in both  $u$  and  $v$ . Suppose that  $\Phi(u, v) = t(v)\Psi(u, v)$ , where  $t(v)$  is the divisor of  $\Phi(u, v)$ . It follows that  $\Psi(u, v)$  belongs to  $\mathfrak{F}(u, v)$ . Then, since  $t(v) = \frac{g(v)}{g_1(v)}$ , where  $g(v)$  and  $g_1(v)$  are integral in  $v$  without a common divisor, it is seen, if  $\frac{A \cdot B}{\Phi(u, v)} = H(u, v)$ , where  $H(u, v)$  belongs to  $\mathfrak{F}(u, v)$ , that

$$\frac{A \cdot B g_1(v)}{g(v) \Psi(u, v)} = H(u, v).$$

Since  $g(v)$  is the product of prime functions, say  $p_1(v)$ ,  $p_2(v)$ ,  $\dots$ , while  $\Psi(u, v)$  is the product of prime functions  $P_1(u, v)$ ,  $P_2(u, v)$ ,  $\dots$ , then (see Art. 4)  $A$  must be divisible by all, some or none of the prime functions  $p(v)$  while  $B$  is divisible by the rest of them. If further  $\frac{A \cdot B}{g(v)} = C \cdot D$ , then  $C$  must be divisible by all, some or none of the prime functions  $P(u, v)$  while  $D$  is divisible by the rest of them.

ART. 35. Consider next integral functions of  $x$  whose coefficients belong to  $\mathfrak{F}(u, v)$ . The following theorem is

found also to be true here: *If the product of two functions  $f(x, u, v)$  and  $g(x, u, v)$  whose coefficients belong to  $\mathfrak{F}(u, v)$  is divisible by the prime function  $P(u, v)$  which belongs to  $\mathfrak{F}(u, v)$  and is irreducible in  $\mathfrak{R}(v)$ , then one of the functions is divisible by  $P(u, v)$ .*

To introduce the conception of the divisor for such functions, write

$$f(x, u, v) = A_0 + A_1x + A_2x^2 + \dots,$$

where the coefficients belong to the realm  $\mathfrak{R}(u, v)$ . Then as in Art. 32 we may always determine a divisor  $t = t(u, v)$  such that

$$F(x, u, v) = \frac{f(x, u, v)}{t(u, v)} = B_0 + B_1x + B_2x^2 + \dots,$$

where the  $B$ 's belong to  $\mathfrak{F}(u, v)$  and have no divisor other than a possible constant. The function  $F(x, u, v)$  is *primitive* with respect to the realm  $\mathfrak{R}(u, v)$ . If  $t$  has been so chosen that the  $B$ 's belong to the realm  $\mathfrak{F}(1, u, v)$  and the integral coefficients  $B_0, B_1, B_2, \dots$  have no common divisor other than unity, then  $F(x, u, v)$  is a *primitive* function with respect to the realm  $\mathfrak{F}(1, u, v)$ .

Let  $f$  be an integral function in  $x$  whose coefficients belong to  $\mathfrak{F}(u, v)$  and suppose that the coefficient of the highest power of  $x$  is unity. Further let  $g$  be an integral function in  $x$  whose highest coefficient is unity while the other coefficients belong to  $\mathfrak{R}(u, v)$ . If finally  $f/g$  is an integral function in  $x$  whose coefficients belong to  $\mathfrak{F}(u, v)$ , then the coefficients of  $g$  belong also to  $\mathfrak{F}(u, v)$ . The same is also true if for the realm  $\mathfrak{F}(u, v)$  in the statement of the theorem we substitute  $\mathfrak{F}(1, u, v)$ .

It may also be shown that if an integral function in  $x$  whose coefficients belong to  $\mathfrak{F}(1, u, v)$  may be resolved into factors whose coefficients belong to  $\mathfrak{R}(u, v)$ , it may also be resolved into factors whose coefficients belong to  $\mathfrak{F}(1, u, v)$ .



ART. 36. Continuing it is seen in general that if  $P = P(u, v, \dots, s)$  belongs to the realm  $\mathfrak{F} = \mathfrak{F}(u, v, \dots, s)$ , and considered as a function of  $u$  is irreducible in the realm  $\mathfrak{R}(v, \dots, s)$ , it is also irreducible in the realm  $\mathfrak{F}(v, \dots, s)$  and is a *prime* function belonging to the realm  $\mathfrak{R}(u, v, \dots, s) = \mathfrak{R}$ , say. The constant coefficients may have a common divisor other than unity. If  $A$  is any other function that belongs to  $\mathfrak{F}$  and if  $A$  considered as a function of  $u$  is not divisible by  $P$ , then  $A$  and  $P$  are *relatively prime*. If further  $A$  and  $B$  are two functions belonging to  $\mathfrak{F}$  and if  $A \cdot B \div P$  is a function belonging to  $\mathfrak{F}$ , then either  $A$  or  $B$  is divisible by  $P$ .

If the product of two integral functions in  $x$ , say  $f(x)$  and  $g(x)$  whose coefficients belong to  $\mathfrak{F}$  is divisible by  $P$ , then either  $f(x)$  or  $g(x)$  is divisible by  $P$ ; if  $f(x)$ , say, is divisible by  $P$ , all the coefficients of  $x$  in  $f(x)$  are divisible by  $P$ .

It is always possible to find in the realm  $\mathfrak{R}$  a divisor  $t$  which will render any integral function in  $x$  whose coefficients belong to  $\mathfrak{R}$  a primitive function. The product of two primitive functions of  $x$  whose coefficients belong to  $\mathfrak{F}$  is a primitive function whose coefficients belong to  $\mathfrak{F}$ . If further  $f$  is an integral function of  $x$  whose coefficients belong to  $\mathfrak{F}$  and if  $g$  is a primitive function of  $x$  with respect to the realm  $\mathfrak{R}$  and if  $f/g$  is an integral function of  $x$  whose coefficients belong to  $\mathfrak{R}$ , the coefficients of this quotient also belong to  $\mathfrak{F}$ .

It may be further shown that if an integral function in  $x$  whose coefficients belong to  $\mathfrak{F}$  is resolvable into two factors whose coefficients belong to  $\mathfrak{R}$ , it is also resolvable into two factors whose coefficients belong to  $\mathfrak{F}$ . The same is true for the realm  $\mathfrak{F}(1, u, v, \dots, s)$ .

If  $f$  is an integral function of  $x$  whose coefficients belong to  $\mathfrak{F}$ , the coefficient of the highest power of  $x$  being unity,





where in the *first* row unity and  $F(x_0)$  are to be included among the divisors, in the *second* row unity and  $F(x_1)$ , etc.

Further write

$$f(x_i) = d_{i1} (i = 0, 1, 2, \dots, n)$$

and put

$$\phi(x) = (x - x_0)(x - x_1) \cdots (x - x_n).$$

By Lagrange's interpolation formula (Art. 18) we form the function  $f(x)$  which for the  $n+1$  values  $x_0, x_1, \dots, x_n$  takes the  $n+1$  values  $d_{01}, d_{11}, \dots, d_{n1}$ , viz.

$$f(x) = \sum_{i=0}^{i=n} d_{i1} \frac{\phi(x)}{(x - x_i)\phi'(x_i)}.$$

If  $f(x)$  is a divisor of  $F(x)$ , it is evident that  $f(x_i)$  is a divisor of  $F(x_i)$ .

The number of functions of the  $n$ th degree which like  $f(x)$  may be formed by the interpolation formula by taking *one* of the  $d$ 's out of every row of the scheme (1) are in number  $k_0 \cdot k_1 \cdots k_n$ . The divisors, if any, of the  $n$ th degree in  $x$  of the function  $F(x)$  are contained among these functions and are to be found by trial. In the same way the divisors of the  $(n-1)$ st degree may be found, etc.

Take next the problem of finding the divisors of the function  $F(x, u)$ , which is an integral function of the  $2n$  or  $2n+1$  degree in  $x$  and whose coefficients belong to  $\mathfrak{F}(1, u)$ . We give to  $x$  respectively integral values  $x_0, x_1, \dots, x_n$  which are to be so chosen that the function is *not* zero for any of them. Let  $d_{j1}(u), d_{j2}(u), \dots, d_{j_l}(u)$  be the divisors of  $F(x_j)$  ( $j = 0, 1, 2, \dots, n$ ). We may then as above by means of Lagrange's interpolation formula determine  $l_0 \cdot l_1 \cdots l_n$  functions of the  $n$ th degree in  $x$  whose coefficients belong to  $\mathfrak{F}(1, u)$  from which the divisors of the  $n$ th degree in  $x$ , if any, of  $F(x, u)$  are to be

found by trial. The same process must be continued for the divisors, if any, of the  $(n-1)$ st degree in  $x$  of  $F(x, u)$ , etc.

In this manner it is evident that we may determine the irreducible factors of a polynomial  $F(x, u, v, \dots, s)$  integral in  $x$  whose coefficients belong to the realm  $\mathfrak{S}(1, u, v, \dots, s)$ .

To resolve an integral function of  $x$ , say  $\phi(x, u, v, \dots, s)$  into its irreducible factors, when the coefficients are not integral but belong to the realm  $\mathfrak{R}(u, v, \dots, s)$ , we note, if  $t(u, v, \dots, s)$  is the divisor (Art. 32) of  $\phi(x, u, v, \dots, s)$ , that

$$\frac{\phi(x, u, v, \dots, s)}{t(u, v, \dots, s)} = \Phi(x, u, v, \dots, s),$$

where  $\Phi(x, u, v, \dots, s)$  is integral in all its variables, with integral coefficients. We may further write

$$t(u, v, \dots, s) = \frac{g(u, v, \dots, s)}{g_1(u, v, \dots, s)},$$

where  $g$  and  $g_1$  are integral in the variables with integral coefficients. Writing

$$\phi(x, u, v, \dots, s) = \frac{g(u, v, \dots, s)}{g_1(u, v, \dots, s)} \Phi(x, u, v, \dots, s),$$

it is seen that the divisors of  $g$ ,  $g_1$  and  $\Phi$  may be derived as above and consequently also the divisors of  $\phi(x, u, v, \dots, s)$ .

The above method of decomposing an integral function into its irreducible factors is due to Kronecker (*Grundzüge*, p. 4). It is of interest in particular from a theoretical standpoint in that the *existence* of the roots is *not* presupposed.

In practice the process of finding the factors has been simplified.<sup>1</sup>

<sup>1</sup> See for example for the case of one variable papers by Runge, *Crelle's Journal*, Vol. 99, p. 89; Mandl, *Crelle's Journal*, Vol. 113, p. 252; and for the case of several variables, see Meyer, *Math. Ann.*, Vol. 30, p. 30; Hancock, *Ann. de l'École Norm. Sup.*, 3<sup>e</sup> Série, T. XVII, p. 89.

ART. 39. Let  $f(x)$  be an irreducible integral function of  $x$ , whose coefficients belong to a fixed realm of rationality  $\mathfrak{R}$  and let  $g(x)$  be an integral function whose coefficients belong to the same realm. We have the following theorem: *If the equation  $g(x)=0$  has a root in common with the irreducible equation  $f(x)=0$ , it is divisible by  $f(x)$ .* (See Abel, *Works*, Vol. I, p. 480).

To prove this theorem, let  $\phi(x)$  be the greatest common divisor of  $g(x)$  and  $f(x)$ . It is *not* possible for the irreducible function  $f(x)$  to be divisible by  $\phi(x)$  unless either  $\phi(x)=f(x)$  or  $\phi(x)=a$  constant. If  $\phi(x)=f(x)$ , then  $g(x)$  is divisible by  $f(x)$  and the coefficients of the quotient  $\frac{g(x)}{f(x)}=h(x)$  belong to the realm  $\mathfrak{R}$ . We then have

$$g(x) = f(x)h(x),$$

where  $h(x)$  is a function integral in  $x$ . It follows that every root of  $f(x)=0$  satisfies the equation  $g(x)=0$ . If  $\phi$  is a *constant*, then  $f$  and  $g$  are prime to each other with respect to the realm  $\mathfrak{R}$ . In this case it is always possible (cf. Art. 17) to determine two integral functions  $p(x)$  and  $q(x)$  whose coefficients belong to  $\mathfrak{R}$  such that

$$p(x)f(x) + q(x)g(x) = 1.$$

It is evident from this that  $f(x)$  and  $g(x)$  have here no root in common. Hence the irreducible equation  $f(x)=0$  either has all its roots in common with  $g(x)=0$  or none. (Abel, Vol. II, p. 230. See also Serret, *Cours d'algèbre supérieure*, No. 100).

ART. 40. If  $f(x)$  and  $g(x)$  are two integral functions of  $x$ , whose coefficients belong to the realm  $\mathfrak{R}$ , and if  $f(x)$  is irreducible in this realm, then if every root of  $g(x)=0$  satisfies the equation  $f(x)=0$ , it is seen that  $g(x)$  must to a constant factor be a power of  $f(x)$ . For if  $f(x)$  and

$g(x)$  have a root in common, it follows from the preceding article that  $g(x)$  is divisible by  $f(x)$  so that

$$g(x) = f(x)g_1(x),$$

where  $g_1(x)$  is a function integral in  $x$  whose coefficients belong to  $\mathfrak{R}$ . Since the roots of  $g_1(x) = 0$  also satisfy  $g(x) = 0$ , they must satisfy  $f(x) = 0$ . It follows that  $g_1(x)$  is divisible by  $f(x)$  or

$$g(x) = f(x)^2g_2(x),$$

where  $g_2(x)$  is integral in  $x$  with coefficients that belong to  $\mathfrak{R}$ . Continuing in this manner we must finally have  $g(x)$  equal to a power of  $f(x)$  multiplied by a constant.

ART. 41. The following theorems follow at once:

1. An irreducible equation can have no root in common with an equation of lower degree.

2. An irreducible equation  $f(x) = 0$  cannot have a multiple root; for this root would also be a root of  $f'(x) = 0$  and  $f'(x)$  is of lower degree than  $f(x)$ .

We shall regard two irreducible functions as different, when they differ otherwise than by a multiplicative constant.

3. Two different irreducible equations can have no common root.

4. When a product of two integral functions is divisible by an irreducible function, one of the factors is divisible by this function.

5. A reducible function may be distributed into irreducible factors in only one way, where all the coefficients belong to a fixed realm  $\mathfrak{R}$ .

For let  $A$  be a reducible function of  $x$  which by a continued reduction into factors has the form

$$A = P \cdot P' \cdot P'' \dots,$$

where the  $P$ 's are irreducible functions, not necessarily

different. If there is possible another reduction, say

$$A = Q \cdot Q' \cdot Q'' \dots,$$

we must have

$$P \cdot P' \cdot P'' \dots = Q \cdot Q' \cdot Q'' \dots.$$

It follows that  $P \cdot P' \cdot P'' \dots$  must be divisible by  $Q$ , and also by  $Q'$ ,  $Q''$ ,  $\dots$ . Hence one of the factors  $P$ ,  $P'$ ,  $P''$ ,  $\dots$ , say  $P$  is divisible by  $Q$ . But since  $P$  and  $Q$  are both irreducible, it follows that  $P = Q$  and similarly for all the other factors. It is thus seen that the sequence of the irreducible factors of a function may be different while the factors themselves must be the same.

#### EXAMPLES

1. Using the method of Mandl (*Crelle*, Vol. 113, p. 252) show that  $x^6 + 2x^5 + 3x^4 + 3x^3 + 3x^2 + 2x + 1$  is factorable in  $\mathfrak{Z}(1, x)$ .

2. Using the same method show that

$$\frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

is irreducible in  $\mathfrak{Z}(1, x)$ . The six roots of this last function are given by Poisson, *Réflexions sur la théorie des nombres*, p. 125.

See also Gauss, *Disq. Arithm.*, Art. 73.

For such equations as  $\frac{x^p - 1}{x - 1} = 0$ , see the method given in Weber's

*Algebra*, Vol. I, § 179, and the original source as found in Legendre, *Théorie des nombres*, Vol. II, pp. 191 et seq.



## CHAPTER III

### ALGEBRAIC REALMS OF RATIONALITY

ART. 42. Take a fixed realm of rationality  $R$ , as the *stock realm*. Let  $f$  denote an integral algebraic function whose coefficients belong to the realm  $R$ . If  $x$  is a quantity which does not belong to this realm and which causes such a function as  $f$  to vanish, we say that  $x$  is an *algebraic* quantity. If, however, there is no algebraic equation which  $x$  satisfies, then  $x$  is a *transcendental* quantity. That there exist such quantities was first shown by Liouville in a paper "Sur des classes très-étendus des quantités dont la valeur n'est ni algébrique ni même réductible à des irrationnelles algébriques" (*Liouville's Journal*, Vol. 16, p. 133, Série I, 1851).

In particular Hermite (1873) in a paper "Sur la fonction exponentielle" (*Comp. Rend.*, Vol. LXXVII) has shown that  $e$  is *not* an algebraic quantity. Later Lindemann<sup>1</sup> proved that the same is true of  $\pi$ . In the same connection see a paper by G. Cantor "Ueber eine Eigenschaft des Inbegriffs aller algebraischen Zahlen," *Crelle*, Bd. 77, p. 258 (1874).

ART. 43. If the stock realm  $\mathfrak{R}$  is formed of all rational functions of  $u, v, w, \dots, z$ , then  $x$  is an *algebraic* function of  $u, v, w, \dots, z$ , if there exists an algebraic equation whose coefficients belong to this realm and which  $x$

<sup>1</sup> Lindemann, "Ueber die Zahl  $\pi$ " (*Math. Ann.*, Bd. XX, p. 213). See also Weierstrass, "Zu Lindemann's Abhandlung, ueber die Ludolp'sche Zahl," *Sitz. der Ber. Akad.* (Dec. 1885). Papers by Hilbert, Hurwitz, and Gordan on the same subject are found in the 43<sup>rd</sup> Volume of the *Mathematische Annalen*. See other references in the *Encyclopædie der math. Wiss.*, Bd. I, p. 669; also in Hancock's "Systèmes modulaires de Kronecker," *Ann. de l'École Normale*, Paris, 1900; and *Report on Algebraic Numbers*, p. 76.

satisfies, provided  $x$  does not belong to this same realm. We say that  $x$  is an algebraic quantity which is *derived* from the realm  $\mathfrak{R}$  (any stock realm), if  $x$  satisfies an algebraic equation whose coefficients belong to this realm.

All the algebraic quantities which are derived from a fixed stock realm clearly form another realm.

If  $x$  is an algebraic quantity that is derived from the realm  $\mathfrak{R}$ , there is an algebraic function which vanishes for this value of the variable. It may happen that the function is reducible. In this case, as we saw above, it may be uniquely resolved into its irreducible factors, one of which must be satisfied by  $x$ . Hence associated with every algebraic quantity  $x$  there is a definite irreducible equation which  $x$  satisfies. If this equation,  $f(x) = 0$  say, is of the  $n$ th degree, then the remaining  $n - 1$  roots  $x', x'', \dots, x^{(n-1)}$  are called the algebraic quantities *conjugate* to  $x$ . This conception is *relative*, since it refers to the realm  $\mathfrak{R}$ .

ART. 44. If we adjoin (cf. Galois, *Oeuvres*, p. 34; Galois, *Liouville's Journal*, Vol. 11, p. 418; see also Weber's *Algebra*, I, § 147 of the 2<sup>nd</sup> Edition) the algebraic quantity  $x$  to the stock realm  $\mathfrak{R}$ , we have a new realm  $\mathfrak{R}(x)$ , which in addition to containing the realm  $\mathfrak{R}$  consists of all rational functions of  $x$  whose coefficients belong to  $\mathfrak{R}$ . (See also Dedekind, p. 455 of Dirichlet's *Zahlentheorie*).

Consider next any *rational* function of  $x$ , say  $h(x)/g(x)$ , which has a definite value, so that therefore  $g(x) \neq 0$ . Suppose further that  $x$  satisfies the irreducible equation  $f(t) = 0$  of degree  $n$  and also that  $g(t)$  and  $f(t)$  have no roots in common. We may determine (Art. 39) two functions  $p(t)$  and  $q(t)$  such that

$$p(t)g(t) + q(t)f(t) = 1.$$

If in this expression we write  $t = x$ , we have

$$p(x)g(x) = 1 \quad \text{or} \quad h(x)/g(x) = h(x)p(x),$$

which is an integral function of  $x$ . It is therefore sufficient in the realm  $\mathfrak{R}(x)$  to consider only *integral* functions of the algebraic quantity  $x$ . Further suppose that  $g(t)$  is an integral function whose degree in  $x$  is greater than  $n$ , so that

$$g(t) = f(t)\phi(t) + h(t),$$

where  $h(t)$  is an integral function in  $t$  of degree less than  $n$ .

Writing  $t = x$ , we have  $g(x) = h(x)$ . From the above it is seen that *every rational function of  $x$  may by means of the equation  $f(x) = 0$  be transformed into an equation of degree less than  $n$ , and in such a way that we have the entire realm  $\mathfrak{R}(x)$ , if we form the expression*

$$c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$$

*and write for the  $c$ 's all possible quantities of the realm  $\mathfrak{R}$ ; and every quantity of this realm is thereby had only once.*

Otherwise by equating two such quantities, we would have an equation of degree less than  $n$  that was satisfied by  $x$ .

The realm  $\mathfrak{R}(x)$  is called *an algebraic realm* of the  $n$ th degree.

ART. 45. If  $x$  satisfies an irreducible equation of the  $n$ th degree, the  $n$  roots of this equation were defined above as being *conjugate* to one another. We saw above that by *adjoining*  $x$  to the stock-realm  $\mathfrak{R}$  a new realm  $\mathfrak{R}(x)$  was derived. Similarly to the quantity  $x'$  there corresponds the realm  $\mathfrak{R}(x')$ , to the quantity  $x''$  the realm  $\mathfrak{R}(x'')$ , etc. These  $n$  realms are called *conjugate* realms.

Two conjugate realms  $\mathfrak{R}(x)$  and  $\mathfrak{R}(x')$  will have a number of quantities in common, for example all the quantities of the stock realm  $\mathfrak{R}$ . They may also be wholly contained the one in the other. For if  $x'$  is a rational function of  $x$ , the realm  $\mathfrak{R}(x')$  is contained in the realm  $\mathfrak{R}(x)$ . If not only  $x'$  is a rational function of  $x$

but also  $x$  is a rational function of  $x'$ , the two realms  $\mathfrak{R}(x)$  and  $\mathfrak{R}(x')$  are identical.<sup>1</sup>

There are realms which are identical with all their conjugate realms. Such realms are called *Galois or normal realms of rationality*. They exist if all the roots of the equation  $f(t) = 0$  have the property that each one is a rational function of the other. Equations in which this property exist are called *Galois or normal equations*. (See Galois, *Oeuvres*. See also Abel, *Mémoire sur une classe particulière d'équations*, etc.; *Oeuvres* (Sylow and Lie), Vol. I, p. 478; Weber, *Algebra*, I, § 152 et seq.)

ART. 46. If we compare realms of rationality with one another we have two important conceptions to develop: viz., the *least common multiple* and the *greatest common divisor of realms of rationality*.

Let  $x$  be an algebraic quantity which is derived from the stock realm  $R$  and let  $y$  and  $z$  be two other algebraic quantities that are derived from  $R$ . Consider the realms  $\mathfrak{R}(x)$ ,  $\mathfrak{R}(y)$  and  $\mathfrak{R}(z)$ . We understand by the *least common multiple* of these realms, the *smallest realm which contains them all*; by the *greatest common divisor* we understand the realm which consists of all quantities *common* to these realms.

ART. 47. We shall first develop the notion of the *least common multiple*. The least common multiple of any number of realms is also called the *product* of these realms. Both conceptions are the same. For the realm  $\mathfrak{R}(x, y)$  contains the realms  $\mathfrak{R}(x)$  and  $\mathfrak{R}(y)$ ; or  $\mathfrak{R}(x)$  and  $\mathfrak{R}(y)$  are both divisors of  $\mathfrak{R}(x, y)$ . The latter realm is also the least common multiple of the two former. For any

<sup>1</sup> If  $\alpha$  is a quantity belonging to  $\mathfrak{R}(x)$ , then is

$$\alpha = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1},$$

where the  $c$ 's are rational numbers in  $\mathfrak{R}$ ; and when for  $x$  we write the conjugate roots  $x', x'', \dots, x^{(n-1)}$ , we have the quantities  $\alpha', \alpha'', \dots, \alpha^{(n-1)}$  which are conjugate to  $\alpha$ .

realm that contains  $\Re(x)$  and  $\Re(y)$  contains also  $\Re(x, y)$ . We may therefore write  $\Re(x)\Re(y) = \Re(x, y)$ . It is evident if the realm  $\Re(x)$  contains the realm  $\Re(y)$  that  $\Re(x) \cdot \Re(y) = \Re(x, y) = \Re(x)$ , since  $y$  must be a rational function of  $x$ . We always have  $\Re(1)\Re(x) = \Re(x)$ .

If further  $x, y, z, \dots$ , are algebraic quantities that are derived from  $\Re$ , then all rational functions of  $x, y, z, \dots$  form a realm  $\Re(x, y, z, \dots)$  which is the least common multiple of the realms  $\Re(x), \Re(y), \Re(z), \dots$ .

We shall show how such a realm is equivalent to a realm  $\Re(\sigma)$  where the algebraic quantity  $\sigma$  is a rational function of  $x, y, z, \dots$  and reciprocally the quantities  $x, y, z, \dots$  are rational functions of  $\sigma$ . This theorem was first given by Abel, *Précis d'une théorie des fonctions elliptiques*. The proof given here is somewhat different. See also Weber's *Algebra*, Vol. I, p. 459. Let  $x$  be a root of the irreducible equation  $f(x) = 0$  of degree  $m$  whose coefficients are quantities of the realm  $\Re$  and let  $y$  satisfy the irreducible equation  $g(x) = 0$  of degree  $n$  whose coefficients likewise belong to  $\Re$ . We wish to show that there is a quantity  $\tau$  say which belongs to the realm  $\Re(x, y)$  and is consequently a rational function of  $x, y$ ; and reciprocally that  $x$  and  $y$  are rational functions of  $\tau$ . When this has been proved it is evident that the realms  $\Re(x, y)$  and  $\Re(\tau)$  are identical.

Let  $x, x', x'', \dots, x^{(m-1)}$  be the roots of  $f(x) = 0$ , and let  $y, y', y'', \dots, y^{(n-1)}$  be those of  $g(x) = 0$ . It is always possible to determine a rational function  $\tau = \chi(x, y)$  in such a way that the  $m \cdot n$  values of  $\tau$  are all different when for  $x$  all the conjugate values  $x, x', x'', \dots, x^{(m-1)}$  are written and for  $y$  the values  $y, y', y'', \dots, y^{(n-1)}$ . The linear function  $x + qy$  has this property, if the constant  $q$  is chosen as follows: Note that the difference  $x + qy - (x' + qy')$  is not zero, if  $q \neq \frac{x - x'}{y - y'}$ ; and observe that there



are  $m \cdot n$  such values. If we give to  $q$  any other values and write  $\chi(x, y) = x + qy$ , it is clear that the  $m \cdot n$  values of  $\tau = \chi(x, y)$  are different, when  $x$  and  $y$  take the above values.

ART. 48. We may accordingly write

$$\tau = \chi(x, y), \quad \tau' = \chi(x', y), \quad \tau'' = \chi(x'', y), \quad \dots,$$

where the  $x$ 's go through the above conjugate values of  $x$ , as do the  $y$ 's of  $y$ . Let  $t$  be a variable quantity and form the product

$$(t - \tau)(t - \tau') \dots = \Phi(t),$$

where  $\Phi(t)$  is an integral function of the  $m \cdot n$  degree in  $t$  whose coefficients are the elementary symmetric functions of the  $\tau$ 's. These coefficients may in turn be replaced by rational expressions in the coefficients of  $f(x)$  and  $g(x)$  and consequently belong to the realm  $\mathfrak{R}$ . To each of the  $m \cdot n$  values of  $\chi(x, y)$  there corresponds a different value of  $\tau$  and to every  $\tau$  there corresponds a definite value of  $\chi(x, y)$ .

Let  $\rho = \vartheta(x, y)$  be any rational function of  $x, y$  and write

$$\rho = \vartheta(x, y), \quad \rho' = \vartheta(x', y), \quad \rho'' = \vartheta(x'', y), \quad \dots,$$

where the  $\rho$ 's are marked as the  $\tau$ 's above, when the  $x$ 's and  $y$ 's have corresponding values in the  $\rho$ 's as in the  $\tau$ 's. Next form the function

$$\left[ \frac{\rho}{t - \tau} + \frac{\rho'}{t - \tau'} + \frac{\rho''}{t - \tau''} + \dots \right] \Phi(t),$$

which is an integral function in  $t$ . If we write this function in the form

$$\left[ \frac{\vartheta(x, y)}{t - \chi(x, y)} + \frac{\vartheta(x', y)}{t - \chi(x', y)} + \dots \right] \Phi(t) = \Psi(t),$$

it is seen that  $\Psi(t)$  is an integral function in  $t$  whose coefficients are symmetric functions in the  $x$ 's and  $y$ 's and therefore belong to the realm  $\mathfrak{R}$ . Writing  $t = \tau$ , we

have

$$\rho\Phi'(\tau) = \Psi(\tau) \quad \text{or} \quad \rho = \frac{\Psi(\tau)}{\Phi'(\tau)},$$

which is a rational function of  $\tau$  whose coefficients belong to the realm  $\mathfrak{R}$ . But  $\rho = \vartheta(x, y)$  is any rational function of  $x, y$ . We may therefore write  $\rho = x$  with the result that  $x$  is a rational function of  $\tau$ . The same is true for  $y$ .

*If therefore the function  $\chi$  as written above gives  $m \cdot n$  different values, it is seen that the realms  $\mathfrak{R}(\tau)$  and  $\mathfrak{R}(x, y)$  are identical.*

This is a sufficient, but not a necessary condition; for it is sufficient that  $k$  of the  $m \cdot n$  values of  $\chi$  be different, where  $k$  is the degree of the irreducible factor  $h(t)$ , say, of  $\Phi(t)$ , which is satisfied by  $\tau$ .

ART. 49. Continuing the investigation we may take instead of the two quantities  $x$  and  $y$  any number of such quantities  $x, y, z, \dots$ , which are derived from the realm  $\mathfrak{R}$ . Let  $x$  be defined through the irreducible equation  $f(x) = 0$  of degree  $m$ , while  $y$  is defined through the irreducible equation  $g(y) = 0$  of degree  $n$ ,  $z$  through an irreducible equation of degree  $l$ , etc.

The smallest realm which contains all these quantities is the *least common multiple* of these realms, the realm  $\mathfrak{R}(x, y, z, \dots)$ . It may be shown that from this realm  $\mathfrak{R}(x, y, z, \dots)$  a new quantity  $\sigma$  may be derived which is a rational function of  $x, y, z, \dots$ , say  $\sigma = \phi(x, y, z, \dots)$  and at the same time  $x$  is a rational function of  $\sigma$  and also  $y$  is a rational function of  $\sigma$ , while  $z$  is a rational function of  $\sigma$ , etc.

It follows then that the realms  $\mathfrak{R}(x, y, z, \dots)$  and  $\mathfrak{R}(\sigma)$  are identical. It is sufficient for the proof of this theorem so to choose  $\sigma$  that the  $m \cdot n \cdot l \dots$  values of  $\sigma$  which are had when for  $x, y, z, \dots$  their conjugate values are written, are all different. Such a function can always

be determined.<sup>1</sup> For consider the linear expression

$$(1) \quad w = h_1\alpha_1 + h_2\alpha_2 + \cdots + h_k\alpha_k,$$

where the  $\alpha$ 's are all different as are the  $h$ 's. It is seen by permuting the  $\alpha$ 's that there are  $\lfloor n = N$  values of  $w$ . The difference of any two such  $w$ 's, say  $w_i$  and  $w_j$ , gives an expression of the form

$$(2) \quad w_i - w_j = h_1(\alpha_{1i} - \alpha_{1j}) + h_2(\alpha_{2i} - \alpha_{2j}) \\ + \cdots + h_k(\alpha_{ki} - \alpha_{kj}),$$

where  $\alpha_{1i} - \alpha_{1j}$ , etc., are differences among the  $\alpha$ 's including zero. There are  $\frac{N(N-1)}{1 \cdot 2}$  such differences among the  $w$ 's. If we put  $h_1 = 1$ ,  $h_2 = h$ ,  $h_3 = h^2$ ,  $\cdots$ ,  $h_k = h^{k-1}$ , then any of the differences of (2) may be equal for  $k-1$  values of  $h$ , that is, for any root of the equation (2), when we put  $w_i - w_j = 0$ , and consequently there are

$$\frac{N(N-1)}{1 \cdot 2}(k-1)$$

values of  $h$  for which any two values of  $w$  may be equal. Any other value of  $h$  will give values of  $w$  different from one another. Another proof is given in the next article.

ART. 50. We may with Weber (*Algebra*, Vol. I, § 43) let  $\Phi_1(x, y, z, \cdots)$ ,  $\Phi_2(x, y, z, \cdots)$ ,  $\Phi_3(x, y, z, \cdots)$ ,  $\cdots$  be integral functions of the variables  $x, y, z, \cdots$  with numerical coefficients, which do not all simultaneously vanish in any of the functions. It may be proved that values may be given to the variables in an infinite number of ways, so that none of the functions  $\Phi_1, \Phi_2, \Phi_3, \cdots$  vanishes. For, if the functions depend only upon one variable, there are only a finite number of values which cause the functions to vanish. Assuming that this is true for  $n$  variables, it may be proved to hold for  $n+1$

<sup>1</sup> See Camille Jordan, *Math. Ann.*, Vol. I, p. 143; *Traité des substitutions*, No. 351; Cantor, *Math. Ann.*, Vol. V, p. 133; Bachmann or Galois, *Math. Ann.*, Vol. 18, p. 460.

variables. To show this, arrange the terms with respect to the  $(n+1)^{\text{st}}$  variable  $t$ , say. Then by hypothesis, values may be given to the other  $n$  variables such that the coefficients of all the powers of  $t$  shall vanish in none of the functions. We thus have functions of the one variable  $t$  and can ascribe such values to it that none of the functions vanish. It is clear that we may use rational values of the variables in establishing the desired result.

**THEOREM.** *If none of the functions  $\Phi_1, \Phi_2, \Phi_3, \dots$  above have a common factor, values may be given the variables such that one of the functions vanishes while the others are different from zero.*

Let the variable  $t$  be present in say  $\Phi_1$  and observe (see Art. 17, end) that functions  $\Psi_i, \Omega_i$  may be determined such that

$$\Psi_i \Phi_i + \Omega_i \Phi_1 = \chi_i, \tag{a}$$

where  $\chi_i$  is independent of  $t$ . Determine such values of the other variables that the functions  $\chi_i$  are all different from zero while  $\Phi_1$  becomes a function of  $t$  alone. Then give to  $t$  such a value that  $\Phi_1$  becomes zero. It is seen from (a) that none of the other functions  $\Phi_i$  can vanish for this value of  $t$ .

**ART. 51.** If  $\sigma = \phi(x, y, z, \dots)$  is a rational function of  $x, y, z, \dots$ , and if the  $m \cdot n \cdot l \dots$  values of  $\phi$  are all different when the conjugate values are written for  $x, y, z, \dots$ , then reciprocally the quantities  $x, y, z, \dots$  may be expressed as rational functions of  $\sigma$ . The proof may be performed in the same way as the one above for the two quantities  $x$  and  $y$ . However, through a repetition of that process, it follows that if

$$\Re(x, y) = \Re(\tau),$$

then is

$$\begin{aligned} \Re(x, y, z) &= \Re(\tau, z) = \Re(\lambda), \\ \Re(x, y, z, t) &= \Re(\lambda, t) = \Re(\mu), \quad \text{etc.} \end{aligned}$$

As an example, let  $R$  be the realm of all rational numbers, that is, take  $R = \mathfrak{R}(1)$  and let

$$x = \sqrt{2} \quad \text{and} \quad y = \sqrt{3}$$

be two algebraic numbers that are derived from this realm. A quantity  $\tau$  may always be found which is a rational function of  $\sqrt{2}$  and  $\sqrt{3}$  and through which  $\sqrt{2}$  and  $\sqrt{3}$  may be rationally expressed. Such a function is for example

$$\tau = \sqrt{2} + \sqrt{3}.$$

It is seen that

$$\tau^3 = 11\sqrt{2} + 9\sqrt{3}.$$

It follows that

$$\tau^3 - 9\tau = 2\sqrt{2} \quad \text{or} \quad \sqrt{2} = \frac{\tau^3 - 9\tau}{2};$$

and similarly

$$\sqrt{3} = \frac{11\tau - \tau^3}{2}.$$

It is thus shown that

$$\mathfrak{R}(\sqrt{2})\mathfrak{R}(\sqrt{3}) = \mathfrak{R}(\sqrt{2}, \sqrt{3}) = \mathfrak{R}((\sqrt{2} + \sqrt{3})).$$

EXAMPLE. If  $\mathfrak{R}(\sqrt{5})\mathfrak{R}(\sqrt{-3}) = \mathfrak{R}(\tau)$ , find  $\tau$ .

ART. 52. **Another Proof.** Let  $\alpha$  and  $\beta$  be two algebraic numbers which satisfy the irreducible equations

$$\alpha^r = a_1\alpha^{r-1} + a_2\alpha^{r-2} + \dots + a_r,$$

$$\beta^s = b_1\beta^{s-1} + b_2\beta^{s-2} + \dots + b_s.$$

Further let  $u$  and  $v$  be two indeterminates. It may be shown first that

$$\gamma = \alpha u + \beta v$$

is an algebraic number. For represent the  $r \cdot s = n$  numbers  $\alpha^\rho \beta^\sigma$  ( $\rho = 0, 1, \dots, r-1$ ;  $\sigma = 0, 1, \dots, s-1$ ) in any sequence by  $w_\nu$  ( $\nu = 1, 2, \dots, n$ ). We assert that  $w_\nu \gamma$  may be expressed through the form

$$(1) \quad w_\nu \gamma = x_{\nu 1} w_1 + x_{\nu 2} w_2 + \dots + x_{\nu n} w_n,$$





If this equation is differentiated with regard to  $u$  and  $v$  respectively, we have

$$\frac{\partial f(\alpha u + \beta v, u, v)}{\partial(\alpha u + \beta v)} \alpha + \frac{\partial f(\alpha u + \beta v, u, v)}{\partial u} = 0,$$

$$\frac{\partial f(\alpha u + \beta v, u, v)}{\partial(\alpha u + \beta v)} \beta + \frac{\partial f(\alpha u + \beta v, u, v)}{\partial v} = 0.$$

Since the function  $\frac{\partial f(\alpha u + \beta v, u, v)}{\partial(\alpha u + \beta v)}$  is of a finite degree in  $\alpha u + \beta v$  whose coefficients are rational functions of  $u$  and  $v$ , we may always give a pair of values to  $u$  and  $v$  such that

$$\frac{\partial f(\alpha u + \beta v, u, v)}{\partial(\alpha u + \beta v)} \neq 0.$$

It is then seen that  $\alpha$  and  $\beta$  are rational functions of  $\gamma$ .

*It has thus been shown that if  $\alpha$  and  $\beta$  are two arbitrary algebraic numbers, we may always determine a number  $\gamma$  such that (1)  $\gamma$  is algebraic, (2)  $\gamma$  is a rational function of  $\alpha$  and  $\beta$  (this rational function may indeed be taken linear) and (3)  $\alpha$  and  $\beta$  are themselves rational functions of  $\gamma$  with rational coefficients. Similarly it may be proved that if  $\alpha_1, \alpha_2, \dots, \alpha_n$  are  $n$  algebraic numbers, we may always find a number  $w$ , such that (1)  $w$  is algebraic, (2)  $w$  is a rational function of  $\alpha_1, \alpha_2, \dots, \alpha_n$  (indeed  $w$  may be chosen a linear function of  $\alpha_1, \alpha_2, \dots, \alpha_n$  with rational coefficients) and (3) each of the quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$  is a rational function of  $w$  with rational coefficients.*

**ART. 53. Normal Realms.** The following is an important application of the theorem in Art. 49. Let  $\Re$  be the stock realm from which the algebraic quantity  $x$  is derived, and suppose that  $x$  satisfies the irreducible equation  $f(x) = 0$  which is of the  $n$ th degree in  $x$ . Further let  $x, x', x'', \dots, x^{(n-1)}$  be the  $n$  roots of this equation and form the realms  $\Re(x), \Re(x'), \dots, \Re(x^{(n-1)})$ .

The *norm* of the realm  $\Re(x)$  is defined as the product

of the realms <sup>1</sup>

$$\mathfrak{R}(x), \mathfrak{R}(x'), \dots, \mathfrak{R}(x^{(n-1)}).$$

As shown in Art. 49 we may determine a function

$$\sigma = \phi(x, x', \dots, x^{(n-1)}),$$

linear in the quantities  $x, x', \dots, x^{(n-1)}$ , which by the permutation of the  $x$ 's takes  $n!$  different values. These  $n!$  values are denoted by  $\sigma, \sigma', \sigma'', \dots$ . Take next a variable quantity  $t$  and form the product

$$\Phi(t) = (t - \sigma)(t - \sigma')(t - \sigma'') \dots,$$

a function of the  $n!$  degree in  $t$  whose coefficients remain unaltered when  $x, x', x'', \dots$  are interchanged. They are therefore symmetric functions and belong to the realm  $\mathfrak{R}$ . Next take  $n!$  arbitrary functions formed like the functions above. For example, such functions may be had by permuting the  $x$ 's as follows;

$$\begin{aligned} v &= \vartheta(x, x', x'', \dots, x^{(n-1)}), \\ v' &= \vartheta(x', x, x'', \dots, x^{(n-1)}), \\ v'' &= \vartheta(x'', x', x, \dots, x^{(n-1)}), \end{aligned}$$

etc. Form the function

$$\left( \frac{v}{t - \sigma} + \frac{v'}{t - \sigma'} + \dots \right) \Phi(t) = \Psi(t).$$

It is seen that  $\Psi(t)$  is an integral function in  $t$  whose coefficients remain unaltered when for  $v$  and  $\sigma$  their values in terms of the  $x$ 's are substituted and then the  $x$ 's permuted. They are consequently symmetric functions of the  $x$ 's and belong to the realm  $\mathfrak{R}$ . It follows at once that

$$v\Phi'(\sigma) = \Psi(\sigma),$$

or

$$v = \frac{\Psi(\sigma)}{\Phi'(\sigma)},$$

<sup>1</sup> See Abel, Vol. I, pp. 546, 547; Vol. II, pp. 231, 241, 242, 336, 337; Gauss, *Works*, Vol. I, p. 103 (1831); and Kummer, *Liouv. Journ.* 12, p. 187 (1844).

which is a rational function of  $\sigma$ . Since  $v$  is an arbitrary function of  $x, x', \dots, x^{(n-1)}$ , we may write each of these quantities in the place of  $v$  and then from the above equation it is seen that each of these  $x$ 's may be expressed as a rational function of  $\sigma$ . (See Example 6 at end of this chapter.)

Consequently the norm of the realm  $\mathfrak{R}(x)$ , that is  $\mathfrak{R}(x, x', x'', \dots, x^{(n-1)})$ , is identical with the realm  $\mathfrak{R}(\sigma)$ . The degree of the realm  $\mathfrak{R}(\sigma)$  is equal to the degree of the irreducible equation which  $\sigma$  satisfies. This degree is very important in the further discussion. It is called the *order* of the equation  $f(x) = 0$ .

It was seen above that  $\sigma, \sigma', \sigma'', \dots$  were rational functions of  $x, x', x'', \dots$ . Since  $x, x', x'', \dots$  are rational functions of  $\sigma$ , it follows also that  $\sigma, \sigma', \sigma'', \dots$  are rational functions of  $\sigma$ . Hence the realms  $\mathfrak{R}(\sigma'), \mathfrak{R}(\sigma''), \dots$ , are identical with the realm  $\mathfrak{R}(\sigma)$ . A realm having this property is called *normal*.

We have thus proved the theorem: *The norm of a realm is a normal realm.* (See Art. 45.)

ART. 54. We may next develop more fully the idea of an algebraic realm of the  $n$ th degree. In Art. 44, such a realm was defined through an irreducible algebraic equation of the  $n$ th degree. It was seen that every quantity of the realm  $\mathfrak{R}(x)$  could in only one way be represented in the form

$$b_1 + b_2x + b_3x^2 + \dots + b_nx^{n-1},$$

where the  $b$ 's take all possible values of a fixed (stock-) realm of rationality. The following definitions may be offered: If  $x_1, x_2, \dots, x_n$  are any  $n$  quantities of the realm  $\mathfrak{R}(x)$ , they are said to be *linearly independent*, if it is *not* possible to determine  $n$  quantities  $a_1, a_2, \dots, a_n$  of the stock-realm  $\mathfrak{R}$  such that

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = 0;$$

and when this is the case, the  $n$  quantities  $x_1, x_2, \dots, x_n$  form an *irreducible system* (with respect to the realm  $\mathfrak{R}(x)$ ; Dedekind, § 164 of the Dirichlet, *Zahlentheorie*).

If we take  $1, x, x^2, \dots, x^{n-1}$  as these  $n$  quantities, it is seen that they are linearly independent, since  $x$  satisfies an irreducible equation of degree not lower than the  $n$ th.

If  $x_0, x_1, x_2, \dots, x_n$  are  $n+1$  quantities of the realm  $\mathfrak{R}(x)$ , it follows that they may be expressed in the form

$$\begin{aligned} x_0 &= b_{01} + b_{02}x + b_{03}x^2 + \dots + b_{0n}x^{n-1}, \\ x_1 &= b_{11} + b_{12}x + b_{13}x^2 + \dots + b_{1n}x^{n-1}, \\ &\dots\dots\dots \\ x_n &= b_{n1} + b_{n2}x + b_{n3}x^2 + \dots + b_{nn}x^{n-1}, \end{aligned}$$

where the  $b$ 's belong to the realm  $\mathfrak{R}$ .

The  $n+1$  quantities  $x_0, x_1, \dots, x_n$  are *linearly dependent*, for it is always possible to determine  $n+1$  quantities  $a_0, a_1, \dots, a_n$  in such a way that

$$(1) \quad a_0x_0 + a_1x_1 + \dots + a_nx_n = 0.$$

To show this, substitute for  $x_0, x_1, \dots, x_n$  their values from above and equate the coefficients of the different powers of  $x$  to zero. It follows that

$$\begin{aligned} b_{01}a_0 + b_{11}a_1 + b_{21}a_2 + \dots + b_{n1}a_n &= 0, \\ b_{02}a_0 + b_{12}a_1 + b_{22}a_2 + \dots + b_{n2}a_n &= 0, \\ &\dots\dots\dots \\ b_{0n}a_0 + b_{1n}a_1 + b_{2n}a_2 + \dots + b_{nn}a_n &= 0. \end{aligned}$$

We thus have  $n$  equations in  $n+1$  unknown quantities, and from them we may always determine  $n+1$  values for  $a_0, a_1, \dots, a_n$  which are different from zero and which satisfy the relation (1). All these quantities belong to the fixed realm  $\mathfrak{R}$ , since they are determined through rational operations upon the  $b$ 's.

ART. 55. We seek the criterion by which it may be determined whether  $n$  quantities  $x_1, x_2, \dots, x_n$  are





sub-determinants of higher order are zero, the extreme case being the determinant  $D$  itself. Bordering the determinant  $D_1$  and developing the resulting determinant

$$D_2 = \begin{vmatrix} b_{11}, & b_{21}, & \dots, & b_{m1}, & u_1 \\ b_{12}, & b_{22}, & \dots, & b_{m2}, & u_2 \\ \dots & \dots & \dots & \dots & \dots \\ b_{1,m+1}, & b_{2,m+1}, & \dots, & b_{m,m+1}, & u_{m+1} \end{vmatrix}$$

with respect to  $u_1, u_2, \dots, u_{m+1}$ , it is seen that

$$D_2 = u_1 C_1 + u_2 C_2 + \dots + u_m C_m + u_{m+1} C_{m+1},$$

where

$$C_{m+1} = D_1 \neq 0.$$

Observe that two columns in  $D_2$  become equal for

$$u_1 = b_{i1}, u_2 = b_{i2}, \dots, u_{m+1} = b_{i,m+1} \quad (i=1, 2, \dots, m);$$

and when  $i = m+1, m+2, \dots, n$ , the determinant  $D_2$  being a sub-determinant of  $D_1$  and of order higher than  $m$ , is by hypothesis zero.

Accordingly, if we write

$$a_1 = C_1, a_2 = C_2, \dots, a_{m+1} = C_{m+1}, a_{m+2} = 0, \dots, a_n = 0,$$

it is seen that the equations (1) are satisfied. Next multiply the equations (1) respectively by  $1, x, x^2, \dots, x^{n-1}$  and adding, it follows that

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = 0.$$

With this it is seen that the  $x$ 's are linearly dependent if  $D_1 = 0$  and form a reducible system. Otherwise the  $a$ 's are all zero and consequently the  $x$ 's are linearly independent and form an irreducible system.

ART. 57. We may accordingly introduce the following definition of an *algebraic realm of rationality*. Having fixed a realm  $\mathfrak{R}$  as a stock-realm, we regard all quantities belonging to this realm as *rational*. Consider further a realm which contains besides the quantities that belong to the realm  $\mathfrak{R}$  still other quantities. This latter realm is said to be *algebraic*, if there is a number  $n$ , such that





terminant is

$$C_{ik} = \sum_{h=1}^{h=n} a_{hk} r_{hi} - x r_{ki}$$

and in the second case the general term is

$$C'_{ik} = \sum_{h=1}^{h=n} a'_{ih} r_{kh} - x r_{ki}.$$

To show that these terms are equal, note that if the values (1) are written in (2) we have

$$x \sum_{k=1}^{k=n} r_{ki} x_k = \sum_{k=1}^{k=n} (x_k \sum_{h=1}^{h=n} a'_{ih} r_{kh}),$$

while from the equations

$$x x_i = a_{i1} x_1 + a_{i2} x_2 + \dots + a_{in} x_n$$

it follows directly that

$$x \sum_{k=1}^{k=n} r_{ki} x_k = \sum_{k=1}^{k=h} (x_k \sum_{h=1}^{h=n} a_{hk} r_{hi}),$$

with which it is proved that  $C_{ik} = C'_{ik}$  and that  $\Phi_1(x) = \Phi_2(x)$ .

**ART. 59. Norm; Spur.** Expanding the determinant that defines  $\Phi_1(x)$ , it is seen that

$$\Phi_1(x) = x^n + A_1 x^{n-1} + A_2 x^{n-2} + \dots + A_{n-1} x + A_n = 0.$$

Denote the roots of this equation by  $x^{(1)}, x^{(2)}, \dots, x^{(n)}$ . If  $x$  is any one of these conjugate roots, by definition the *norm* of  $x$  is the product of the roots and written

$$N(x) = N(x^{(1)}) = N(x^{(2)}) = \dots = N(x^{(n)}) = x x^{(1)} \dots x^{(n-1)};$$

while the *spur* of  $x$ , is written

$$S(x) = x^{(1)} + x^{(2)} + \dots + x^{(n)}.$$

By writing  $x=0$  in the determinant that defines  $\Phi_1(x)$ , it is seen that

$$(1) \quad (-1)^n A_n = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = N(x),$$



while

$$S(x) = a_{11} + a_{22} + \dots + a_{nn} = -A_1.$$

From the equations (1) of Art. 57 it is seen that  $S(0) = 0$ ,  $S(1) = n$ . If  $a$  is any rational number,

$$S(ax) = aS(x).$$

If  $\alpha$  and  $\beta$  are two numbers of the realm  $\Omega$ , then is  $S(\alpha + \beta) = S(\alpha) + S(\beta)$ . Observe further that

$$N(0) = 0, \quad N(1) = 1.$$

It may be proved that  $x = 0$  is the only quantity of the realm  $\Omega$  whose norm is zero. For, under the assumption that the determinant (1) above is zero, quantities  $t_1, t_2, \dots, t_n$  may be found such that

$$t_1 a_{i1} + t_2 a_{i2} + \dots + t_n a_{in} = 0 \quad (i=1, 2, \dots, n).$$

Hence, multiplying the equations (1) of Art. 57 respectively by  $t_1, t_2, \dots, t_n$  and adding, it is seen that

$$x(t_1 x_1 + t_2 x_2 + \dots + t_n x_n) = 0.$$

Since the quantities  $x_1, x_2, \dots, x_n$  are linearly independent, it follows that  $x = 0$ .

If  $a$  is a rational number,  $N(a) = a^n$ . If  $y$  is any other number of  $\Omega$ , so that we have a second system of equations analogous to equations (1) of Art. 57 and (2) of Art. 58

$$y x_i = a'_{i1} x_1 + a'_{i2} x_2 + \dots + a'_{in} x_n \quad (i=1, 2, \dots, n),$$

it is seen that

$$x y x_i = C_{i1} x_1 + C_{i2} x_2 + \dots + C_{in} x_n \quad (i=1, 2, \dots, n),$$

where

$$C_{ik} = a'_{i1} a_{1k} + a'_{i2} a_{2k} + \dots + a'_{in} a_{nk}.$$

From the multiplication of determinants it is seen that

$$|C_{ik}| = |a_{ik}| \cdot |a'_{ik}| \quad \left( \begin{matrix} i=1, 2, \dots, n \\ k=1, 2, \dots, n \end{matrix} \right);$$

and that is

$$N(x \cdot y) = N(x)N(y).$$

Writing in this expression  $y = \frac{1}{x}$ , it follows that

$$N(x)N\left(\frac{1}{x}\right) = 1. \quad (i)$$

It is also seen that

$$N\left(\frac{x}{y}\right) = N(x)N\left(\frac{1}{y}\right);$$

or from (i)

$$N\left(\frac{x}{y}\right) = \frac{N(x)}{N(y)}.$$

ART. 60. Realms such as were defined like  $\Omega$  in Article 57 are *finite realms*. It was seen that a *finite* realm contains only algebraic quantities. It follows also that no transcendental quantity can belong to such a realm. Regarding infinite realms we can only make *negative* statements, just as the definition of an infinite realm may only be expressed *negatively*.

If we adjoin the root of an irreducible algebraic equation to the stock-realm  $\mathfrak{R}$ , the realm thereby produced is finite.

Reciprocally, we have all possible finite realms, if we adjoin to the realm  $\mathfrak{R}$  the roots of all possible algebraic equations.

To prove this we have only to show that in every finite realm  $\mathfrak{A}$ , say, there exists an algebraic quantity  $x$  of such a nature that the realm is completely determined through it.

Let  $n$  be the degree of  $\mathfrak{A}$ . If  $n = 1$ , then is  $\mathfrak{A} = \mathfrak{R}(1) = \mathfrak{R}$  and consequently  $x = 1$ . But if  $n > 1$ , there is an algebraic quantity in the realm  $\mathfrak{A}$ . Let this quantity be  $\alpha$  and let the degree of the irreducible equation which  $\alpha$  satisfies be  $a$ . If  $n = a$ , we have all the quantities of the realm  $\mathfrak{A}$  by multiplying respectively the quantities  $1, \alpha, \alpha^2, \dots, \alpha^{a-1}$  by all possible rational numbers and adding the products thus formed. In this case  $\mathfrak{A} = \mathfrak{R}(\alpha)$

and consequently  $x = \alpha$ . But if  $n > a$ , there must be in  $\mathfrak{R}$  more than  $a$  linearly independent quantities so that there must be at least another quantity  $\alpha'$  which is linearly independent of the  $a$  quantities  $1, \alpha, \alpha^2, \dots, \alpha^{a-1}$ . We may however (Art. 51) always determine a quantity  $\beta$  which is a rational function of the  $\alpha$ 's and  $\alpha'$  and through which the  $\alpha$ 's and  $\alpha'$  may be rationally expressed. Let the degree of the irreducible equation which  $\beta$  satisfies be  $b$  so that  $\mathfrak{R}(\beta)$  is of degree  $b$ . It is seen that the realm  $\mathfrak{R}(\beta)$  contains the  $a+1$  quantities  $1, \alpha, \alpha^2, \dots, \alpha^{a-1}$  and  $\alpha'$  and since these quantities are linearly independent  $b \geq a+1$ .

If  $b = n$ , then is  $\mathfrak{R} = \mathfrak{R}(\beta)$  and consequently  $x = \beta$ . But if  $b < n$ , we must continue this process until finally we come to a realm of degree  $n$  so that  $\mathfrak{R} = \mathfrak{R}(x)$  where  $x$  satisfied an irreducible equation of the  $n$ th degree.

We have thus shown that *in every finite realm there exists a quantity  $x$  which satisfies an irreducible equation whose coefficients are rational and whose degree is  $n$ ; and through this quantity  $x$  the realm is completely determined.*

**ART. 61. Primitive Quantities; Kronecker's Gattung.** By adjoining to the realm  $\mathfrak{R}$  the algebraic quantities  $\alpha, \beta, \dots$ , we saw that by a finite number of operations, we must come to a realm  $\mathfrak{R}(x)$  of the  $n$ th degree. There must exist several such quantities such as  $x$  which belong to the same realm. Let  $y$  be another quantity which also satisfies an irreducible equation of the  $n$ th degree. It is evident from the manner in which these quantities are derived (see also Art. 69) that both  $x$  and  $y$  may be rationally expressed the one in terms of the other. Such quantities are called *primitive quantities*. A *primitive* quantity determines its realm of rationality. The collectivity of primitive quantities constitute what Kronecker called a

“Gattung.” Thus, associated with every realm is its *Gattung*.

The following method may be employed to determine whether quantities are primitive or not. Suppose that  $x$  is a primitive quantity and that  $y = \phi(x)$  is another quantity belonging to the same realm  $\mathfrak{R}$ . Let  $t$  be a variable quantity and form the equation

$$[t - \phi(x)][t - \phi(x')][t - \phi(x'')] \cdots [t - \phi(x^{(n-1)})] = g(t),$$

which is an integral function of the  $n$ th degree in  $t$  whose coefficients belong to the realm  $\mathfrak{R}$ . Writing  $y = \phi(x)$ ,  $y' = \phi(x')$ ,  $y'' = \phi(x'')$ ,  $\dots$ ,  $y^{(n-1)} = \phi(x^{(n-1)})$ , the above equation becomes

$$(t - y)(t - y')(t - y'') \cdots (t - y^{(n-1)}) = g(t),$$

which is satisfied if  $y$  is written in the place of  $t$ . But if  $y$  is to be a *primitive* quantity, it must satisfy an irreducible equation of the  $n$ th degree. Hence the equation  $g(t) = 0$  must be irreducible and  $y'$ ,  $y''$ ,  $\dots$ ,  $y^{(n-1)}$  must be the conjugate values of  $y$ .

Accordingly, if the  $n$  quantities  $y = \phi(x)$ ,  $y' = \phi(x')$ ,  $y'' = \phi(x'')$ ,  $\dots$ ,  $y^{(n-1)} = \phi(x^{(n-1)})$  are all different, then  $y$  is a primitive quantity in the realm  $\mathfrak{R}$ ; and the realm is completely determined through  $y$ .

Observe that if a realm  $\mathfrak{A}$  is determined by a quantity  $x$ , so that  $\mathfrak{A} = \mathfrak{R}(x)$ , then  $x$  may be replaced by a rational function of  $x$ , say  $\Phi(x)$ , provided that the conjugate quantities  $y = \Phi(x)$ ,  $y' = \phi(x')$ ,  $\dots$ ,  $y^{(n-1)} = \phi(x^{(n-1)})$  are all different, the realms  $\mathfrak{R}(x)$  and  $\mathfrak{R}(y)$  being in this case identical.

We have here also a second proof of the theorem that if  $y$  belongs to the realm  $\mathfrak{R}(x)$ , it is an algebraic quantity. For it may be rationally expressed in terms of  $x$  and from what we have just seen satisfies an irreducible equation of degree at most  $= n$ .

**ART. 62. Basis.** In Art. 54 we were able to define the degree of a finite realm by means of the properties of the realm. We saw that a realm was of the  $n$ th degree when there were  $n$  linearly independent quantities in this realm, while any  $n+1$  quantities of this realm were linearly dependent, however these quantities be chosen.

In a realm of the  $n$ th degree any system of  $n$  linearly independent quantities is called a *basis* (cf. Dedekind, p. 468 of Dirichlet's *Zahlentheorie*) of the realm. If we multiply the  $n$  quantities that constitute the basis by all possible numbers that belong to the stock realm  $\mathfrak{R}$ , we have through addition all possible quantities of our new realm and each quantity only *once* (see *below*).

If  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis of a realm of the  $n$ th degree and if  $\eta$  is any arbitrary quantity of this realm, then (Art. 54) we may always determine  $n+1$  rational numbers  $x_0, x_1, x_2, \dots, x_n$  so that

$$x_0\eta + x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n = 0,$$

and in such a way that  $x_0, x_1, \dots, x_n$  are not all zero. In particular  $x_0$  is different from zero, for otherwise there would be a linear relation among the  $\alpha$ 's. It follows that

$$\eta = y_1\alpha_1 + y_2\alpha_2 + \dots + y_n\alpha_n,$$

where the  $y$ 's are rational numbers.

There is only one way of expressing  $\eta$  in this manner. For if

$$\eta = y'_1\alpha_1 + y'_2\alpha_2 + \dots + y'_n\alpha_n,$$

we would have

$$0 = (y_1 - y'_1)\alpha_1 + (y_2 - y'_2)\alpha_2 + \dots + (y_n - y'_n)\alpha_n;$$

and consequently since the  $\alpha$ 's are linearly independent, we must have

$$y_\nu = y'_\nu \quad (\nu = 1, 2, \dots, n).$$

The rational numbers  $y_1, y_2, \dots, y_n$  are called the *coördinates* of  $\eta$ . The coördinates of any number of a



realm are uniquely determined when once a definite basis has been established.

If  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_n$  are two systems of  $n$  numbers which belong to a fixed realm of the  $n$ th degree and if  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis of this realm, we must have

$$\beta_\nu = c_{\nu 1}\alpha_1 + c_{\nu 2}\alpha_2 + \dots + c_{\nu n}\alpha_n \quad (\nu=1, 2, \dots, n).$$

The  $\beta$ 's also form a basis of the fixed realm if

$$C = |c_{rs}| \neq 0 \quad \begin{matrix} (r=1, 2, \dots, n) \\ (s=1, 2, \dots, n) \end{matrix}.$$

They do *not* form a basis if  $C=0$ ; for in this case there exists a relation of the form (Art. 56)

$$t_1\beta_1 + t_2\beta_2 + \dots + t_n\beta_n = 0,$$

where the  $t$ 's are rational numbers.

The quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$  are called *basal elements* or elements (terms) of the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

**ART. 63. Discriminant.** We shall now give a *criterion* by which it may be determined whether a system of  $n$  numbers  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis of a realm or not.

Let the algebraic quantity through which the realm of the  $n$ th degree is determined be  $x$  and let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be expressed as integral functions of  $x$  (Art. 44). Then in the expressions of the  $\alpha$ 's in terms of  $x$ , let  $x$  be replaced by each of its conjugate values (including  $x$ )  $x^{(1)}, x^{(2)}, \dots, x^{(n)}$  and let the corresponding values of  $\alpha_\nu$  be

$$\alpha'_\nu, \alpha''_\nu, \dots, \alpha^{(n)}_\nu \quad (\nu=1, 2, \dots, n).$$

We then write

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \begin{vmatrix} \alpha'_1 & \alpha'_2 & \dots & \alpha'_n \\ \alpha''_1 & \alpha''_2 & \dots & \alpha''_n \\ \dots & \dots & \dots & \dots \\ \alpha^{(n)}_1 & \alpha^{(n)}_2 & \dots & \alpha^{(n)}_n \end{vmatrix}^2,$$

and call  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$  the *discriminant* of the  $n$  quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$ .



We therefore have

$$\Delta(1, x, x^2, \dots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{\nu=1}^{\nu=n} f'(x^{(\nu)}).$$

Since the equation  $f(t) = 0$ , through which the algebraic quantity  $x$  is determined, is irreducible, it has no multiple root (Art. 41) and consequently  $f'(x^{(\nu)}) \neq 0$  and therefore also  $\prod_{\nu=1}^{\nu=n} f'(x^{(\nu)}) \neq 0$ .

It follows that  $\Delta(1, x, x^2, \dots, x^{n-1}) \neq 0$ . The four theorems stated above are seen to be true for this special case, as we know that  $1, x, x^2, \dots, x^{n-1}$  form a basis.

ART. 64. Let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be any  $n$  quantities of a realm of the  $n$ th degree. They may therefore be expressed in the form

$$\alpha_\nu = a_{\nu 1} + a_{\nu 2}x + a_{\nu 3}x^2 + \dots + a_{\nu n}x^{n-1} \quad (\nu = 1, 2, \dots, n).$$

Let  $x^{(1)}, x^{(2)}, \dots, x^{(n)}$  be the quantities that are conjugate with  $x$  (including  $x$ ) and write

$$\alpha_\nu^{(\mu)} = a_{\nu 1} + a_{\nu 2}x^{(\mu)} + a_{\nu 3}x^{(\mu)2} + \dots + a_{\nu n}x^{(\mu)n-1} \quad (\mu, \nu = 1, 2, \dots, n).$$

By the theorem for the multiplication of determinants, we have

$$\begin{vmatrix} \alpha'_1 & \alpha''_1 & \dots & \alpha^{(n)}_1 \\ \alpha'_2 & \alpha''_2 & \dots & \alpha^{(n)}_2 \\ \dots & \dots & \dots & \dots \\ \alpha'_n & \alpha''_n & \dots & \alpha^{(n)}_n \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ x^{(1)} & x^{(2)} & \dots & x^{(n)} \\ \dots & \dots & \dots & \dots \\ x^{(1)n-1} & x^{(2)n-1} & \dots & x^{(n)n-1} \end{vmatrix},$$

or

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = |a_{rs}|^2 \Delta(1, x, x^2, \dots, x^{n-1}) \quad (r, s = 1, 2, \dots, n).$$

Since  $\Delta(1, x, x^2, \dots, x^{n-1}) \neq 0$  and since the quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis, when and only when  $|a_{rs}| \neq 0$ , it is seen that  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis when and only when the discriminant  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$ .

We also note the quadratic relation that exists between the two discriminants of any  $n$  quantities of a realm.

The conception of a discriminant of any  $n$  numbers of an algebraic realm of the  $n$ th degree is a very fortunate generalization of the discriminant of an algebraic equation (Art. 22).

**ART. 65. Divisors of Realms of Rationality.** So far we have considered only *multiples* of algebraic realms; we may next consider the *divisors* of such realms.

Let  $\mathfrak{R}$  be the stock-realm and let  $h(z) = 0$  be an irreducible equation of degree  $c$  in  $z$  whose coefficients belong to the realm  $\mathfrak{R}$ . Let the roots of the equation  $h(z) = 0$  be  $z, z', z'', \dots, z^{(c-1)}$ . We consider the realm  $\mathfrak{R}(z)$  and an arbitrary quantity  $x$  of this realm. This quantity  $x$  must (Art. 44) be an integral function of  $z$ , say  $x = \phi(z)$ , whose coefficients belong to the realm  $\mathfrak{R}$ .

Suppose that the quantities which are had when for  $z$  we write its conjugate values are

$$\begin{aligned}x &= \phi(z), \\x' &= \phi(z'), \\x'' &= \phi(z''), \text{ etc.}\end{aligned}$$

These quantities are the roots of the equation

$$F(t) = (t-x)(t-x') \dots (t-x^{(c-1)}) = 0,$$

or

$$F(t) = [t - \phi(z)][t - \phi(z')] \dots [t - \phi(z^{(c-1)})] = 0.$$

This is a symmetric function of the  $c$  roots  $z, z', \dots, z^{(c-1)}$  and consequently its coefficients may be expressed through those of  $h(z)$ ; but these coefficients belong to the realm  $\mathfrak{R}$ ; consequently the coefficients of  $F(t)$  belong also

to the realm  $\mathfrak{R}$ . We may prove the following theorem:  
*The function  $F(t)$  is either an irreducible function or the power of an irreducible function.*

If possible resolve  $F(t)$  into factors and let  $f(t)$  be one of the irreducible factors of degree  $a$ , which vanishes for  $t = \phi(z)$  say, so that

$$f[\phi(z)] = 0.$$

This equation has therefore with respect to the realm  $\mathfrak{R}$  a root in common with the irreducible equation  $h(z) = 0$ .

We consequently (Art. 39) must have  $f[\phi(z)] = 0$ ,  $f[\phi(z')] = 0$ ,  $f[\phi(z'')] = 0$ ,  $\dots$ ,  $f[\phi(z^{(c-1)})] = 0$ , or  $f(x) = 0$ ,  $f(x') = 0$ ,  $\dots$ ,  $f(x^{(c-1)}) = 0$ . It is thus seen that every root of  $F(t) = 0$  satisfies the irreducible equation  $f(t) = 0$ , so that therefore (the lower suffices denoting the degrees of their respective functions)

$$F_c(t) = [f_a(t)]^n,$$

where  $c = a \cdot n$  (cf. Lagrange, *Oeuvres*, III, p. 355) and where the coefficients of both  $F$  and  $f$  belong to  $\mathfrak{R}$ .

ART. 66. Consider the realm  $\mathfrak{R}(x)$  which is formed by adjoining the quantity  $x$  of the preceding article to the realm  $\mathfrak{R}$ . Since every quantity in the realm  $\mathfrak{R}(x)$  is a rational function of  $x$  and as  $x$  is a rational function of  $z$ , it follows that every quantity in  $\mathfrak{R}(x)$  is a rational function of  $z$  and therefore belongs to the realm  $\mathfrak{R}(z)$ . Hence the realm  $\mathfrak{R}(x)$  is a *divisor* of the realm  $\mathfrak{R}(z)$ . On the other hand every quantity in  $\mathfrak{R}(z)$  is *not* contained in  $\mathfrak{R}(x)$ .

If  $n = 1$  in the preceding article, then  $x$  satisfies an irreducible equation whose degree is  $c$ . Further the quantities  $1, x, x^2, \dots, x^{c-1}$  all belong to the realm  $\mathfrak{R}(z)$  and are linearly independent. But the realm  $\mathfrak{R}(z)$  does not contain more than this number of independent quantities. It follows that  $z$  may be expressed rationally in



terms of the powers of  $x$ , and it is seen that  $x$  and  $z$  are *primitive quantities* (Art. 61) in the realm  $\mathfrak{R}(z)$ . The realms  $\mathfrak{R}(x)$  and  $\mathfrak{R}(z)$  are then *identical*.

ART. 67. We take  $\mathfrak{R}$  as the stock-realm and consider a realm  $\mathfrak{C}$  of degree  $c$ . In this realm  $\mathfrak{C}$  there is a primitive quantity  $z$  which satisfies an irreducible equation  $h(z) = 0$  of degree  $c$ . The realm  $\mathfrak{C}$  is completely determined through this quantity so that

$$\mathfrak{C} = \mathfrak{R}(z).$$

Suppose next that the realm  $\mathfrak{A}$  is a divisor of the realm  $\mathfrak{C}$ , the realm  $\mathfrak{A}$  being of degree  $a$ . If  $x$  is a primitive quantity in  $\mathfrak{A}$  it satisfies an irreducible equation  $f(t) = 0$  of degree  $a$ . Since  $x$  also belongs to the realm  $\mathfrak{C}$ , it is seen that  $x$  is an integral function of  $z$ , say  $x = \phi(z)$ . It was shown in Art. 68 that  $c = a \cdot n$ , where  $n$  is an integer. From this it follows that if  $\mathfrak{A}$  is a divisor of  $\mathfrak{C}$ , then  $a$ , the degree of  $\mathfrak{A}$ , is a divisor of  $c$ , the degree of  $\mathfrak{C}$ . It is evident that there are realms which have no divisors save  $\mathfrak{R}$ . This is evidently true when  $c$  is a prime integer.

ART. 68. If  $\mathfrak{A}$  is a divisor of  $\mathfrak{C}$ , then the  $c$  quantities  $\phi(z), \phi(z'), \dots, \phi(z^{(c-1)})$ , as shown above, may be distributed into  $a$  groups, there being  $n$  equal quantities in each group, namely (writing these same quantities in a somewhat different notation)

$$\begin{aligned} x &= \phi(z) = \phi(z_1) = \phi(z_2) = \dots = \phi(z_{n-1}), \\ x' &= \phi(z') = \phi(z'_1) = \phi(z'_2) = \dots = \phi(z'_{n-1}), \\ &\dots\dots\dots \\ x^{(a-1)} &= \phi(z^{(a-1)}) = \phi(z_1^{(a-1)}) = \dots = \phi(z_{n-1}^{(a-1)}). \end{aligned}$$

Observe that the function  $\phi(t) - x$  vanishes for the  $n$  values of  $t = z, z_1, \dots, z_{n-1}$ . It is seen that the functions

$$g(t, x) = (t - z)(t - z_1) \dots (t - z_{n-1})$$

and  $h(t)$  have the common root  $t = z$ . And from this it follows that  $t = z$  satisfies the irreducible equation  $h(t) = 0$

of degree  $c$  in the realm  $\mathfrak{R}$ , while in the realm  $\mathfrak{R}(x)$  it satisfies an equation of degree  $n = \frac{c}{a}$ .

It may be shown as follows that every symmetric function of  $z, z_1, \dots, z_{n-1}$  is a rational function of  $x$ . For, let  $S(t, t_1, \dots, t_{n-1})$  be any symmetric function in  $t, t_1, \dots, t_{n-1}$ , and write

$$\begin{aligned}\tau &= S(z, z_1, \dots, z_{n-1}), \\ \tau' &= S(z', z'_1, \dots, z'_{n-1}), \\ &\dots\dots\dots \\ \tau^{(a-1)} &= S(z^{(a-1)}, z_1^{(a-1)}, \dots, z_{n-1}^{(a-1)}).\end{aligned}$$

Observe that  $f(t) = (t-x)(t-x') \dots (t-x^{(a-1)})$  is an irreducible function in  $\mathfrak{R}$  and form the expression

$$f(t) \left[ \frac{\tau}{t-x} + \frac{\tau'}{t-x'} + \dots + \frac{\tau^{(a-1)}}{t-x^{(a-1)}} \right] = \Psi(t).$$

It is clear that the coefficients of  $\Psi(t)$  belong to  $\mathfrak{R}$ , while  $\tau = \frac{\Psi(x)}{f'(x)}$ , is a rational function in  $x$ .

**THEOREM.** *With respect to the realm  $\mathfrak{A}$  the function  $g(t, x)$  above, is irreducible.* For suppose that  $g(t, x)$  were resolvable into factors and let the irreducible factor that contains the root  $z$  be  $G(t, x)$ . Then, since  $x = \phi(z)$ , it follows that  $G[z, \phi(z)] = 0$ . The coefficients of  $G[z, \phi(z)]$  belong to the realm  $\mathfrak{R}$ . Hence this function vanishes for the other roots of the irreducible equation  $h(z) = 0$  (Art. 41). It follows that

$$G[z, \phi(z)] = 0, \quad G[z_1, \phi(z_1)] = 0, \quad \dots, \quad G[z_{n-1}, \phi(z_{n-1})] = 0$$

and consequently  $G(t, x)$  vanishes for the same values of  $t$  as  $g(t, x)$ ; and, since  $G(t, x)$  is by hypothesis a divisor of  $g(t, x)$ , it is seen that  $g(t, x)$  is irreducible in the realm  $\mathfrak{A}$ .

Hence also the degree of  $\mathfrak{C}$  with respect to  $A$  is  $c/a$ , if with respect to the realm  $\mathfrak{R}$  it is  $c$ .

ART. 69. Let  $y$  be a second quantity belonging to the realm  $\mathfrak{C}$ , and form the realm  $\mathfrak{B} = \mathfrak{R}(y)$ . Corresponding to this divisor of the realm  $\mathfrak{C}$  suppose that there is a second distribution of the  $c$  quantities into  $a$  systems of  $n$  quantities.

$$\begin{aligned} y &= \psi(z) = \psi(z_1) = \dots = \psi(z_{n-1}), \\ y' &= \psi(z') = \psi(z'_1) = \dots = \psi(z'_{n-1}), \\ &\dots\dots\dots \\ y^{(a-1)} &= \psi(z^{(a-1)}) = \psi(z_1^{(a-1)}) = \dots = \psi(z_{n-1}^{(a-1)}). \end{aligned}$$

It may be shown that  $y$  is a rational function of  $x$ ; for let  $t$  be any variable. Form the function

$$\left[ \frac{y}{t-x} + \frac{y'}{t-x'} + \dots + \frac{y^{(a-1)}}{t-x^{(a-1)}} \right] f(t).$$

This expression is the same as

$$\frac{f(t)}{n} \times \left\{ \begin{aligned} &\frac{\psi(z)}{t-\phi(z)} + \frac{\psi(z_1)}{t-\phi(z_1)} + \dots + \frac{\psi(z_{n-1})}{t-\phi(z_{n-1})} \\ &+ \frac{\psi(z')}{t-\phi(z')} + \frac{\psi(z'_1)}{t-\phi(z'_1)} + \dots + \frac{\psi(z'_{n-1})}{t-\phi(z'_{n-1})} \\ &\dots\dots\dots \\ &+ \frac{\psi(z^{(a-1)})}{t-\phi(z^{(a-1)})} + \frac{\psi(z_1^{(a-1)})}{t-\phi(z_1^{(a-1)})} + \dots + \frac{\psi(z_{n-1}^{(a-1)})}{t-\phi(z_{n-1}^{(a-1)})}, \end{aligned} \right.$$

which is an integral function in  $t$  whose coefficients belong to the realm  $\mathfrak{R}$ . Denote it by  $S(t)$ .

If in the above equation we put  $t = x$ , we have

$$yf'(x) = S(x) \quad \text{or} \quad y = \frac{S(x)}{f'(x)},$$

and consequently  $y$  belongs to the realm  $\mathfrak{R}(x)$ . It follows that the realm  $\mathfrak{R}(y)$  is a divisor of the realm  $\mathfrak{R}(x)$ .

In the above discussion it is not necessary that the quantities  $y, y', y'', \dots, y^{(a-1)}$  be all different; but if they are, the two realms  $\mathfrak{A} = \mathfrak{R}(x)$  and  $\mathfrak{B} = \mathfrak{R}(y)$  are identical, the quantities  $x$  and  $y$  being primitive quantities in them.

ART. 70. We have seen that if the degree  $a$  of a divisor-realm  $\mathfrak{R}$  is less than  $c$  the degree of the realm  $\mathfrak{C}$ , then to this divisor there corresponds a distribution of the  $c$  quantities into  $n$  equal groups of  $a$  different quantities or into  $a$  different systems of  $n$  equal quantities. Such a distribution corresponds to each divisor. There is, however, only a finite number of distributions of  $c$  quantities into  $a$  systems of  $n$  quantities. Possibly to many of these distributions there will correspond no divisors; to each divisor, however, there will correspond one and only one distribution. From this we conclude that *an algebraic realm has only a finite number of divisors.*

Reciprocally, it may be shown that *if a realm contains only a finite number of divisors, it is an algebraic realm.* For consider any realm  $\mathfrak{C}$  taken with respect to a stock-realm  $\mathfrak{R}$ . Let  $z$  be a quantity of the realm  $\mathfrak{C}$ , and form the realm  $\mathfrak{R}(z)$  which consists of all rational functions of  $z$ . Besides  $z$  the realm  $\mathfrak{C}$  contains also  $z^2$ . Hence also the realm  $\mathfrak{R}(z^2)$  is a divisor of  $\mathfrak{C}$ . In the same way  $\mathfrak{C}$  contains also the realms  $\mathfrak{R}(z^3)$ ,  $\mathfrak{R}(z^4)$ ,  $\dots$ . It is thus seen that  $\mathfrak{C}$  contains an infinite number of divisors. But in virtue of our hypothesis, there can be only a finite number of such divisors. Hence some of the realms  $\mathfrak{R}(z^k)$  must be equal, say

$$(1) \quad \mathfrak{R}(z^p) = \mathfrak{R}(z^q), \quad \text{where } p < q.$$

The realm  $\mathfrak{R}(z^q)$  consists of all rational function of  $z^q$  of the form

$$\frac{a_0 + a_1 z^q + a_2 z^{2q} + \dots + a_r z^{r^q}}{b_0 + b_1 z^q + b_2 z^{2q} + \dots + b_s z^{s^q}},$$

where the  $a$ 's and  $b$ 's belong to the realm  $\mathfrak{R}$ . Since  $z^p$  belongs in virtue of (1) to the realm  $\mathfrak{R}(z^q)$  it is seen that  $z^p$  must be expressible in the above form, so that

$$b_0 z^p + b_1 z^{p+q} + b_2 z^{p+2q} + \dots + b_s z^{p+s^q} = a_0 + a_1 z^q + \dots + a_r z^{r^q}.$$

This being an algebraic equation in  $z$ , which is not identically satisfied, since none of the exponents on either side of the equation are equal, it follows that  $z$  is an *algebraic quantity*.

If then  $\lambda$  is any quantity that belongs to the realm  $\mathfrak{C}$ , then is  $\lambda$  an algebraic quantity, with which we may form the realm  $\mathfrak{R}(\lambda)$ . Let  $\lambda'$  be another algebraic quantity of  $\mathfrak{C}$  which is *not* contained in  $\mathfrak{R}(\lambda)$ . Since  $\mathfrak{C}$  contains the two realms  $\mathfrak{R}(\lambda)$  and  $\mathfrak{R}(\lambda')$ , it contains also their product, that is  $\mathfrak{R}(\lambda) \cdot \mathfrak{R}(\lambda') = \mathfrak{R}(\lambda, \lambda') = \mathfrak{R}(\mu)$ , say. Continuing in this manner, if  $\mu'$  is an algebraic quantity different from  $\mu$  which is also found in  $\mathfrak{C}$  we form the realm  $\mathfrak{R}(\nu) = \mathfrak{R}(\mu)R(\mu')$  which is a divisor of the realm  $\mathfrak{C}$ . Since  $\mathfrak{C}$  contains only a finite number of divisors, by continuing this process, we must finally come to an algebraic quantity  $\vartheta$ , such that  $\mathfrak{C} = \mathfrak{R}(\vartheta)$ . From this it follows that  $\mathfrak{C}$  is a finite or algebraic realm.

ART. 71. Let  $\mathfrak{C}$  be a realm of degree  $c$  and let  $z$  be a primitive quantity of this realm so that  $\mathfrak{C} = \mathfrak{R}(z)$ . Further let  $\mathfrak{A}$  be a divisor-realm of degree  $a$  and let  $x$  be a primitive quantity in this realm so that  $\mathfrak{A} = \mathfrak{R}(x)$ . Since  $x$  belongs to  $\mathfrak{A}$  and as  $\mathfrak{A}$  is a divisor of  $\mathfrak{C}$ , it is seen that  $x$  is a quantity in  $\mathfrak{C}$  so that  $x = \phi(z)$ , where  $\phi$  denotes an integral function. The quantity  $z$  satisfies an irreducible equation of degree  $c$ . Let the other roots of this equation be  $z', z'', \dots, z^{(c-1)}$  so that the  $a$  quantities conjugate with (and including)  $x$  are to be found among  $\phi(z), \phi(z'), \dots, \phi(z^{(c-1)})$ , each repeated  $n$  times (Art. 65).

ART. 72. We shall now see again how a realm is reduced if we consider instead of the realm  $\mathfrak{R}$ , a more general realm  $\mathfrak{B} = \mathfrak{R}(y)$  as the realm of rationality. Let the irreducible equation in  $\mathfrak{R}$  which  $x$  satisfies be  $F_a(u) = 0$  of degree  $a$ . Next consider the realm  $\mathfrak{B} = \mathfrak{R}(y)$  of degree



$b$  and let the least common multiple of  $\mathfrak{A}$  and  $\mathfrak{B}$  be  $\mathfrak{C} = \mathfrak{R}(z)$  of degree  $c$ ; that is  $\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{C}$ . Since  $\mathfrak{B}$  is a divisor of  $\mathfrak{C}$  we have  $y = \psi(z)$ , where  $\psi$  denotes a rational function whose coefficients belong to  $\mathfrak{R}$ . We may also express  $\mathfrak{C}$  in the form  $\mathfrak{C} = \mathfrak{R}(x, y)$  (Art. 47). It follows that all quantities in  $\mathfrak{C}$  are rational functions of  $x$  and  $y$ , so that  $z = \chi(x, y)$ , where  $\chi$  denotes a rational function.

With respect to the realm  $\mathfrak{B} = \mathfrak{R}(y)$ ,  $z$  satisfies an irreducible equation of degree  $\frac{c}{b}$  and  $\mathfrak{C}$  with respect to this realm is of degree  $\frac{c}{b}$  (see Art. 68).

Due to the equations  $x = \phi(z)$  and  $z = \chi(x, y)$ , it is seen that  $x$  is a rational function of  $z$  and that  $z$  is a rational function of  $x$  (taken with respect to the realm  $\mathfrak{B}$ ). Let the irreducible equation which  $x$  satisfies with respect to the realm  $\mathfrak{B}$  be (see Art. 68, end),

$$G_{\frac{c}{b}}(u, y) = 0.$$

Note in this connection also that  $\mathfrak{A} = \frac{\mathfrak{C}}{\mathfrak{B}}$ . If then  $\mathfrak{R}$  is taken as the realm of rationality, then  $\mathfrak{A}$  is of degree  $a$ , but if  $\mathfrak{B}$  is the realm of rationality, then  $\mathfrak{A}$  is of degree  $a' = \frac{c}{b}$  and we may represent all the quantities of  $\mathfrak{A}$  in the form

$$B_0 + B_1x + B_2x^2 + \cdots + B_{a'-1}x^{a'-1},$$

where the  $B$ 's are all quantities of the realm  $\mathfrak{B} = \mathfrak{R}(y)$ .

**ART. 73. LEMMA.** Let  $\mathfrak{B}$  be a finite realm and  $y$  a primitive quantity in it, and let  $y'$  be a quantity conjugate with  $y$ . Further let  $F(u, y)$  and  $G(u, y)$  be two functions whose coefficients belong to  $\mathfrak{B}$ .

**THEOREM:** *If  $F(u, y)$  is divisible by  $G(u, y)$ , then is  $F(u, y')$  divisible by  $G(u, y')$ .* For if  $F(u, y)$  is divisible

by  $G(u, y)$ , we must have  $F(u, y) = G(u, y)H(u, y)$ , where the coefficients of  $H(u, y)$  also belong to the realm  $\mathfrak{B}$ . In the equation

$$F(u, y) - G(u, y)H(u, y) \equiv 0,$$

the coefficient of any power of  $u$  in this difference is a function of  $y$ , say  $\Phi(y)$ , and since these coefficients are identically zero, it is seen that  $\Phi(t)$  becomes zero for  $t = y$ . Hence also  $\Phi(t)$  becomes zero for the conjugate values of  $y$  (Art. 41; cf. Abel, Vol. II, p. 231).

It follows at once that

$$F(u, y') \equiv G(u, y')H(u, y').$$

Further if  $F(u, y)$  is irreducible in the realm  $\mathfrak{R}(y)$ , then also  $F(u, y')$  is irreducible. For if

$$F(u, y') = G(u, y')H(u, y'),$$

then we must have

$$F(u, y) = G(u, y)H(u, y).$$

We saw that in the realm  $\mathfrak{A} = \frac{\mathfrak{C}}{\mathfrak{B}}$ , that is, when  $\mathfrak{B}$  is taken as the realm of rationality,<sup>1</sup> the quantity  $x$  satisfied an equation of degree  $\frac{c}{b}$ , say  $G(u, y) = 0$ ; and in the realm  $\mathfrak{R}$ , the quantity  $x$  satisfied an irreducible equation  $F_a(u) = 0$  of degree  $a$ . Since both equations are satisfied by  $x$  and since  $G_c(u, y) = 0$  is irreducible in the more extended realm, it follows that  $F_a(u)$  is divisible by  $G_c(u, y)$ .

From the lemma just proved it follows that  $F_a(u)$  is also divisible by  $G_c(u, y')$ , since  $F_a(u)$  remains unchanged when in it we interchange  $y$  and  $y'$ . Similarly it is seen that  $F(u)$  is divisible by  $G(u, y'')$ ,  $\dots$ ,  $G(u, y^{(b-1)})$ . Each of these functions contains therefore at least one

<sup>1</sup> See Camille Jordan, *Traité des substitutions*, p. 269; Hölder, *Math. Ann.*, Bd. 34, p. 47.

of the roots of  $F_a(u) = 0$ . But the coefficients of the product of the  $G$ 's belong to the realm  $\mathfrak{R}$ . It follows then that the product of the  $G$ 's is a power of  $F_a(u)$  and indeed the  $\frac{c}{a}$  power.

ART. 74. Let  $\mathfrak{A}$  and  $\mathfrak{B}$  be two finite realms of degrees  $a$  and  $b$ , with respect to  $\mathfrak{R}$ , and let  $\mathfrak{C}$  be the product of these realms of degree  $c$ . If  $\mathfrak{A}$  is taken as the realm of rationality then  $\mathfrak{B}$  is of degree  $b' = \frac{c}{a}$ , while if  $\mathfrak{B}$  is taken as the realm of rationality, then  $\mathfrak{A}$  is of degree  $\frac{c}{b} = a'$ . Hence  $c = ab' = ba'$  or

$$(1) \quad \frac{a}{a'} = \frac{b}{b'}$$

This result may be expressed in the following manner: *Take  $\mathfrak{R}$  as the stock-realm of rationality and let  $x$  and  $y$  be two quantities that belong to the realm  $\mathfrak{C} = \mathfrak{R}(z)$ ,  $x$  satisfying an irreducible equation of degree  $a$  in  $\mathfrak{R}$  and  $y$  satisfying an irreducible equation of degree  $b$  in  $\mathfrak{R}$ . Then there are also in  $\mathfrak{R}(z)$  equations in which  $x$  appears with coefficients that are functions of  $y$  and vice versa. Let the one in which  $x$  appears to the lowest degree be of degree  $a'$  in  $x$  while the one in which  $y$  appears to the lowest degree be of degree  $b'$  in  $y$ ; then among the numbers  $a, a', b, b'$  we have the relation (1).*

*A special case is when  $x$  and  $y$  are rationally expressed the one in terms of the other; in this case we have*

$$a' = 1 = b'.$$

ART. 75. **The Greatest Common Divisor.** If  $\mathfrak{A}$  and  $\mathfrak{B}$  are two arbitrary realms of degrees  $a$  and  $b$  they will in general have certain quantities in common. All these quantities that are common to the two realms form

another realm  $\mathfrak{D}$ , the greatest common divisor of the realms  $\mathfrak{A}$  and  $\mathfrak{B}$ . If  $t$  is a primitive quantity in  $\mathfrak{D}$  so that  $\mathfrak{D} = \mathfrak{R}(t)$ , it is evident that  $t$  is a rational function of  $x$  and of  $y$ , say

$$t = \phi(x) \quad \text{and} \quad t = \psi(y).$$

Further since  $\mathfrak{R}(t)$  is the greatest common divisor of the realms  $\mathfrak{A}$  and  $\mathfrak{B}$ , any quantity  $t'$  common to these realms is a rational function of  $t$ .

We start then with two realms  $\mathfrak{A} = \mathfrak{R}(x)$  and  $\mathfrak{B} = \mathfrak{R}(y)$  of degrees  $a$  and  $b$  with respect to  $\mathfrak{R}$ . We form their product  $\mathfrak{C} = \mathfrak{R}(x, y) = \mathfrak{R}(z)$  of degree  $c$  and we let their greatest common divisor be  $\mathfrak{D} = \mathfrak{R}(t)$  of degree  $d$ . The quantity  $x$  satisfies an irreducible equation  $F_a(u) = 0$  of degree  $a$  taken with respect to the realm  $\mathfrak{R}$  while it satisfies the irreducible equation  $G_{\frac{c}{b}}(u, y) = 0$  taken with regard to the realm  $\mathfrak{B}$ .

If next we take the realm  $\mathfrak{D}$  as the realm of rationality it is seen that  $x$  satisfies an irreducible equation  $H_{\frac{a}{d}}(u, t) = 0$  of degree  $a/d$  (Art. 68). The coefficients of this equation belong to  $\mathfrak{D}$  and since  $\mathfrak{D}$  is a divisor of  $\mathfrak{B}$ , they also belong to the realm  $\mathfrak{B}$ . Consequently with respect to the realm  $\mathfrak{B}$  the quantity  $x$  satisfies the equation  $H_{\frac{a}{d}}(u) = 0$ . But we just saw that with respect to the realm  $\mathfrak{B}$  the quantity  $x$  satisfies the irreducible equation  $G_{\frac{c}{b}}(u) = 0$ . Hence  $G_{\frac{c}{b}}(u)$  considered as a function of  $u$ , must be a divisor of  $H_{\frac{a}{d}}(u) = 0$ . It follows that  $\frac{a}{d} \geq \frac{c}{b}$  or  $cd \leq ab$ .

ART. 76. Under certain conditions  $cd = ab$  and consequently  $H(u) = G(u)$ . This is always the case if  $\mathfrak{A}$  or  $\mathfrak{B}$  is a Galois or *normal realm*. If for example  $\mathfrak{A}$  is a normal

realm, then the conjugate quantities with  $x$ , that is,  $x'$ ,  $x''$ ,  $\dots$ ,  $x^{(a-1)}$ , which are the roots of  $F_a(u)=0$ , are rationally expressible in terms of  $x$ . Since  $G(u)$  is a divisor of  $F(u)$ , it contains a certain number of the  $a$  factors of  $F(u)$ , say

$$G(u) = (u-x)(u-x') \cdots (u-x^{(k)}), \quad \text{where } k \leq a-1.$$

The coefficients of  $G(u)$  belong to the realm  $\mathfrak{B}$ , but since they are rational functions of  $x$ , they also belong to the realm  $\mathfrak{A}$ . Hence also they belong to the realm  $\mathfrak{D}$  which is the greatest common divisor of  $\mathfrak{A}$  and  $\mathfrak{B}$ . But in  $\mathfrak{D}$  the quantity  $x$  satisfies the irreducible equation  $H(u)=0$ . It follows (Art. 39) that  $G$  is divisible by  $H$ . But since  $H$  is divisible by  $G$ , it follows that

$$G=H \quad \text{and} \quad ab=cd.$$

It may be proved as follows that instead of assuming  $\mathfrak{A}$  to be a Galois realm in the above statement, it is sufficient to assume that  $\frac{\mathfrak{A}}{\mathfrak{D}}$  is a Galois realm.

In  $\mathfrak{A}$  the quantity  $x$  satisfies the irreducible equation

$$F_a(u) = (u-x)(u-x') \cdots (u-x^{(a-1)})$$

and in  $\mathfrak{D}$  it satisfies the irreducible equation

$$H(u, t) = (u-x)(u-x') \cdots (u-x^{\binom{a}{d}-1}).$$

If  $\frac{\mathfrak{A}}{\mathfrak{D}}$  is a Galois realm, the roots of  $H(u)$  are all rationally expressible in terms of  $x$ . Further since  $G(u)$  is a divisor of  $H(u)$ , it follows that the coefficients of  $G(u)$  are rational functions of  $x$  and therefore belong to the realm  $\mathfrak{A}$ . But in the equation  $G(u)=0$  the coefficients are quantities in the realm  $\mathfrak{B}$ ; consequently they belong to the realm  $\mathfrak{D}$ . In  $\mathfrak{D}$ , however, the function  $H(u)$  is irreducible and since  $x$  satisfies  $G(u)=0$  and also  $H(u)=0$  (the coefficients of both equations being rational in the realm  $\mathfrak{D}$ ), it follows



that  $G(u)$  is divisible by  $H(u)$  and consequently as above

$$H(u) = G(u) \quad \text{or} \quad ab = cd.$$

**ART. 77. The Relative Equality of Two Realms.** As an example of what has been given above we may introduce as a new conception that of the *relative equality* of two realms. Let  $\mathfrak{R}$  be a fixed stock-realm and with respect to this realm consider the realm  $\mathfrak{A}$  in which the quantity  $x$  is a primitive quantity satisfying an irreducible equation  $F_a(u) = 0$  of degree  $a$  so that  $\mathfrak{A} = \mathfrak{R}(x)$ . Hence every quantity of the realm  $\mathfrak{A}$  is expressible in the form (Art. 44)

$$g_0 + g_1x + g_2x^2 + \cdots + g_{a-1}x^{a-1},$$

where the  $g$ 's are rational quantities of the realm  $\mathfrak{R}$ .

If  $\mathfrak{A}'$  is another realm taken with respect to a new stock-realm  $\mathfrak{R}'$  and if  $x$  is a primitive quantity of  $\mathfrak{A}'$  so that  $\mathfrak{A}' = \mathfrak{R}'(x)$  and if the quantity  $x$  satisfies the *same* irreducible equation  $F_a(u) = 0$  with respect to  $\mathfrak{R}'$  as it did with respect to  $\mathfrak{R}$ , then we may say that the two realms  $\frac{\mathfrak{A}}{\mathfrak{R}}$  and  $\frac{\mathfrak{A}'}{\mathfrak{R}'}$  are *relatively equal*. The coefficients of the equation  $F_a(u) = 0$  belong to both realms  $\mathfrak{R}$  and  $\mathfrak{R}'$  and consequently to the greatest common divisor of these two realms. Every quantity in  $\mathfrak{A}$  and  $\mathfrak{A}'$  may be expressed in the form

$$g'_0 + g'_1x + g'_2x^2 + \cdots + g'_{a-1}x^{a-1},$$

where the coefficients belong to the greatest common divisor of the realms  $\mathfrak{R}$  and  $\mathfrak{R}'$ .

It is seen that if  $cd = ab$ , the realms  $\frac{\mathfrak{C}}{\mathfrak{B}}$  and  $\frac{\mathfrak{A}}{\mathfrak{D}}$  are relatively equal; for in  $\frac{\mathfrak{A}}{\mathfrak{D}}$  the quantity  $x$  is a primitive quantity which satisfies the irreducible equation  $H_{\frac{a}{d}}(u) = 0$

and in  $\frac{\mathfrak{C}}{\mathfrak{B}}$  the quantity  $x$  is likewise a primitive quantity which satisfies the irreducible equation  $G_{\frac{c}{b}}(u, y) = 0$ .

And from above  $G(u) = H(u)$ .

ART. 78. Consider again (Art. 68) the four realms  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$ ,  $\mathfrak{D}$ . We saw that if  $\mathfrak{B} = \mathfrak{R}(y)$  is taken as the realm of rationality, the quantity  $x$  satisfies the irreducible equation  $G_{\frac{c}{b}}(u, y) = 0$ . The realm  $\mathfrak{D}$  being a divisor of  $\mathfrak{B}$ , it is evident (Art. 68), if  $t = \psi(y)$ , that we have the following system

$$\begin{aligned} t &= \psi(y) = \psi(y_1) = \dots = \psi(y_{m-1}), \\ t' &= \psi(y') = \psi(y'_1) = \dots = \psi(y'_{m-1}), \\ &\dots\dots\dots \\ t^{(d-1)} &= \psi(y^{(d-1)}) = \psi(y_1^{(d-1)}) = \dots = \psi(y_{m-1}^{(d-1)}), \end{aligned}$$

where

$$b = m \cdot d.$$

Since  $\mathfrak{D}$  is a divisor of  $\mathfrak{A}$ , it follows also that (see Art. 73)

$$F_a(u) = H_{\frac{a}{a}}(u, y) H_{\frac{a}{a}}(u, y') \dots H_{\frac{a}{a}}(u, y^{(d-1)}).$$

If further  $ab = cd$ , then from Art. 76 we have

$$H(u, t) = G(u, y),$$

and consequently also

$$F_a(u) = G(u, y) G(u, y') \dots G(u, y^{(d-1)}).$$

Hence if we suppose that  $\mathfrak{B}$  is a normal realm, then since  $G(u, y)$  is irreducible in the realm  $\mathfrak{R}(y)$ , as are also  $G(u, y')$ ,  $G(u, y'')$ ,  $\dots$ ,  $G(u, y^{(d-1)})$  (Art. 73), it is seen that the function  $F(u)$  irreducible in  $\mathfrak{R}$  has the above factors *irreducible* in  $\mathfrak{R}(y)$ .

ART. 79. We may next consider the *norm* of several realms. If  $x$  is the root of an irreducible equation, and if  $x'$ ,  $x''$ ,  $\dots$  are the quantities conjugate to  $x$ , we define the product  $x \cdot x' \cdot x'' \cdot \dots$  as the *norm* of any one of the

quantities  $x, x', x'', \dots, x^{(a-1)}$  and write this product  $=N(x)=N(x')=\dots$ . From  $x$  is derived the realm  $\Re(x)$ ; from  $x'$  the realm  $\Re(x')$ ; etc. These realms we called conjugate realms (Art. 45) and their product we called the norm (Art. 53) of the realm  $\Re(x)$  so that

$$\begin{aligned}\Re(x)\Re(x')\dots\Re(x^{(a-1)}) &= \Re(x, x', \dots, x^{(a-1)}) = N[\Re(x)] \\ &= N[\Re(x')] = \dots = N[\Re(x^{(a-1)})].\end{aligned}$$

**THEOREM I.** *The norm of the product of several realms is equal to the product of their norms.* Suppose we have given the two realms  $\Re(x)$  and  $\Re(y)$ . The product of these realms, that is  $\Re(x)\Re(y)=\Re(x, y)$  forms a new realm, say,  $\Re(z)$ , where  $z$  satisfies an irreducible equation of degree  $c$ . We wish to prove that

$$\begin{aligned}\Re(z, z', z'', \dots, z^{(c-1)}) \\ = \Re(x, x', x'', \dots, x^{(a-1)}, y, y', y'', \dots, y^{(b-1)}).\end{aligned}$$

This equality may be proved by showing that each of the realms is divisible by the other.

From the equality of the realms

$$\Re(z) = \Re(x, y),$$

we have

$$z = \chi(x, y), \quad x = \phi(z), \quad y = \psi(z),$$

where all the functions are rational in their arguments, the coefficients belonging to the stock-realm  $\Re$ . It is evident since  $x=\phi(z)$ , that  $\Re(x)$  is a divisor of  $\Re(z)$ ; and, if we form

$$\phi(z'), \quad \phi(z''), \quad \dots, \quad \phi(z^{(c-1)}),$$

these quantities are conjugate to  $x$ , each one being repeated  $c/a$  times. In the same way the quantities

$$\psi(z'), \quad \psi(z''), \quad \dots, \quad \psi(z^{(c-1)})$$

are the quantities conjugate to  $y$ , each one being repeated

<sup>1</sup> Gauss, *Werke*, I, p. 103 (1831); Kummer, *Journ. d. Math.*, Vol. 12, p. 187.

$c/b$  times. We have at once

$$\mathfrak{R}(x, x', \dots, x^{(a-1)}, y, y', \dots, y^{(b-1)}) \\ = \mathfrak{R}[\phi(z), \phi(z'), \dots, \phi(z^{(c-1)}), \psi(z), \dots, \psi(z^{(c-1)})],$$

from which it is seen that every rational function of the realm  $\mathfrak{R}(x, x', \dots, x^{(a-1)}, y, y', \dots, y^{(b-1)})$  is a rational function of the realm  $\mathfrak{R}(z, z', \dots, z^{(c-1)})$  and consequently the first realm is a divisor of the second; or as it may be expressed symbolically

$$(1) \quad \mathfrak{R}(x, x', \dots, y, y' \dots) < \mathfrak{R}(z, z', \dots, z^{(c-1)}).$$

On the other hand, since

$$z = \chi(x, y), \text{ we have} \\ z = \chi[\phi(z), \psi(z)],$$

where in the latter expression the coefficients belong to the realm  $\mathfrak{R}$ . It follows that

$$z' = \chi[\phi(z'), \psi(z')],$$

and consequently

$$z' = \chi(x', y').$$

It is thus shown that  $z'$  is a rational function of  $x'$  and  $y'$  and similarly  $z''$  is a rational function of  $x''$  and  $y''$ , etc. It follows that  $z, z', z'', \dots, z^{(c-1)}$  belong to the realm  $\mathfrak{R}(x, x', \dots, x^{(a-1)}, y, y', \dots, y^{(b-1)})$  and consequently

$$(2) \quad \mathfrak{R}(z, z', \dots, z^{(c-1)}) < \mathfrak{R}(x, x', \dots, y, y', \dots).$$

From the inequalities (1) and (2) results the equality

$$\mathfrak{R}(x, x', \dots, y, y', \dots) = \mathfrak{R}(z, z', \dots, z^{(c-1)}).$$

**THEOREM II.** *The norm of the divisor of a realm is a divisor of its norm.* Let  $\mathfrak{C} = \mathfrak{R}(z)$  be a realm of degree  $c$  and let  $z', z'', \dots, z^{(c-1)}$  be the quantities that are conjugate to  $z$ , so that

$$\mathfrak{N}(z, z', \dots, z^{(c-1)}) \text{ is the norm of } \mathfrak{C}.$$

Further suppose that  $\mathfrak{A} = \mathfrak{R}(x)$  is a divisor of  $\mathfrak{C}$  where the degree of  $\mathfrak{A}$  is  $a$  and denote by  $x, x', \dots, x^{(a-1)}$  the

quantities that are conjugate to  $x$  so that  $\Re(x', x'', \dots, x^{(a-1)})$  is the norm of  $\Re(x)$ . Since  $\mathfrak{A}$  is a divisor of  $\mathfrak{C}$ , every quantity in  $\mathfrak{A}$  is also contained in  $\mathfrak{C}$ , and consequently  $x = \phi(z)$  where  $\phi$  denotes a rational function. The conjugate quantities are  $x' = \phi(z')$ ,  $x'' = \phi(z'')$ ,  $\dots$ ; and these quantities  $x', x'', \dots$  are quantities of  $\Re(x', x'', \dots)$  which is the norm of  $\Re(x) = \mathfrak{A}$ , while  $z', z'', \dots$  belong to the norm of  $\Re(z) = \mathfrak{C}$ . Hence every quantity belonging to the norm of  $x$  is also to be found in the norm of  $z$ , so that the norm of  $\mathfrak{A}$  is a divisor of the norm of  $\mathfrak{C}$ .

ART. 80. We defined the realm  $\mathfrak{A} = \Re(x)$  as a *normal* or Galois realm (Art. 45), if  $\Re(x) = \Re(x') = \dots = \Re(x^{(a-1)})$ ; that is, if the realm  $\Re(x)$  is equal to its norm.

THEOREM III. *The least common multiple and the greatest common divisor of two normal realms are normal realms.* Let  $\mathfrak{A} = \Re(x)$  and  $\mathfrak{B} = \Re(y)$  be two normal realms, where  $x', x'', \dots, x^{(a-1)}$  are the quantities conjugate to  $x$  and the quantities  $y', y'', \dots, y^{(b-1)}$  are the quantities conjugate to  $y$ . Further suppose that  $\mathfrak{C} = \Re(x, y) = \Re(z)$  is the least common multiple of  $\mathfrak{A}$  and  $\mathfrak{B}$  so that

$$x = \phi(z), \quad y = \psi(z) \quad \text{and} \quad z = \chi(x, y),$$

$\phi$ ,  $\psi$  and  $\chi$  denoting rational functions. The quantities  $\phi(z), \phi(z'), \dots, \phi(z^{(c-1)})$  are conjugate to  $x$ , each repeated  $c/a$  times; while  $\psi(z), \psi(z'), \dots, \psi(z^{(c-1)})$  are conjugate to  $y$ , each repeated  $c/b$  times. Since  $z = \chi(x, y)$ , it follows (see preceding article) that  $z' = \chi(x', y')$ , so that  $z'$  is a rational function of  $x'$  and  $y'$ . But since  $x'$  is a rational function of  $x$  while  $y'$  is a rational function of  $y$ , and as  $x$  and  $y$  are both rational functions of  $z$ , it is seen that  $z'$  is a rational function of  $z$ . Similarly it is seen that  $z''$  is a rational function of  $z$ , etc. It follows that  $\mathfrak{C}$  is a normal realm.

Next let the greatest common divisor of two normal realms  $\mathfrak{A}$  and  $\mathfrak{B}$  be  $\mathfrak{D} = \Re(t)$ , so that  $t = \phi(x)$  and  $t = \psi(y)$ ,



where  $\phi$  and  $\psi$  denote rational functions. Further every quantity that may be rationally expressed in terms of  $x$  and also in terms of  $y$  is found in the realm  $\mathfrak{D}$  and consequently is a rational function of  $t$ .

Let the quantities that are conjugate to  $t$  be  $t' = \phi(x')$ ,  $t'' = \phi(x'')$ ,  $\dots$ ; and correspondingly let

$$t' = \psi(y'), \quad t'' = \psi(y''), \quad \dots$$

It is seen that  $t'$  is a rational function of  $x'$ , and consequently also of  $x$ , since  $x'$  is a rational function of  $x$ ; similarly  $t'$  is a rational function of  $y$ ; and being a rational function of both  $x$  and  $y$ , it follows that  $t'$  is a rational function of  $t$ . Similarly it may be shown that  $t''$ ,  $t'''$ ,  $\dots$  are rational functions of  $t$ , and consequently  $\mathfrak{D}$  is a *normal* realm.

ART. 81. Let  $\mathfrak{C}$  be a normal realm and consider all divisors of this realm; of these divisors select those which are also normal realms. Let  $\mathfrak{C}'$  and  $\mathfrak{C}''$  be two such realms. Suppose further that it is possible to find a divisor  $\mathfrak{A}$  of  $\mathfrak{C}$  which is contained in  $\mathfrak{C}'$  and in which  $\mathfrak{C}''$  is contained. If  $\mathfrak{A}$ ,  $\mathfrak{C}'$  and  $\mathfrak{C}''$  are different from one another  $\mathfrak{A}$  is said to *lie between*  $\mathfrak{C}'$  and  $\mathfrak{C}''$  or

$$\mathfrak{C}' > \mathfrak{A} > \mathfrak{C}''.$$

And this *means* that  $\mathfrak{C}'$  is *divisible* by  $\mathfrak{A}$  and  $\mathfrak{A}$  by  $\mathfrak{C}''$ . Realms which have besides themselves and  $\mathfrak{A}$  no other normal divisors are called *simple realms*.<sup>1</sup>

Suppose that  $\mathfrak{C}$  is *not* a simple realm and that it has the normal divisor  $\mathfrak{C}_3$ . Suppose also that there is a normal divisor between  $\mathfrak{C}$  and  $\mathfrak{C}_3$  and denote this divisor by  $\mathfrak{C}_1$ . We next see whether between  $\mathfrak{C}$  and  $\mathfrak{C}_1$  there lies a normal divisor. Suppose that this is *not* the case, but suppose that between  $\mathfrak{C}_1$  and  $\mathfrak{C}_3$  there lies the normal divisor  $\mathfrak{C}_2$ . We further assume that between  $\mathfrak{C}_1$  and  $\mathfrak{C}_2$ ;

<sup>1</sup> Camille Jordan, *Math. Ann.*, Vol. I, p. 142, and *Traité des substitutions*, p. 41.

$\mathfrak{C}_2$  and  $\mathfrak{C}_3$ ;  $\mathfrak{C}_3$  and  $\mathfrak{R}$  there lie no other common divisors. We say that the realms

$$\mathfrak{C}, \mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{R}$$

form a *connected chain of normal divisors*.

In order then that the above realms form a connected chain of normal divisors, it is necessary that

$$\mathfrak{C} > \mathfrak{C}_1 > \mathfrak{C}_2 > \mathfrak{C}_3 > \mathfrak{R},$$

and that between two successive divisors no other normal divisor appears.

ART. 82. It may next be shown that such a representation of a connected chain of normal divisors is unique and completely determined if the sequence of the divisors is not considered. Suppose that we have found in any manner the connected chain of normal divisors

$$\mathfrak{C}, \mathfrak{C}_1, \mathfrak{C}_2, \dots, \mathfrak{C}_k, \mathfrak{R}$$

and suppose that the degrees of

$$\frac{\mathfrak{C}}{\mathfrak{C}_1}, \frac{\mathfrak{C}_1}{\mathfrak{C}_2}, \frac{\mathfrak{C}_2}{\mathfrak{C}_3}, \dots, \frac{\mathfrak{C}_k}{\mathfrak{R}}$$

are

$$\frac{c}{c_1}, \frac{c_1}{c_2}, \frac{c_2}{c_3}, \dots, \frac{c_k}{1}$$

Suppose further that we have found in another manner the connected chain of normal divisors  $\mathfrak{C}, \mathfrak{C}'_1, \mathfrak{C}'_2, \dots, \mathfrak{C}'_k, \mathfrak{R}$  and suppose that the degrees of

$$\frac{\mathfrak{C}}{\mathfrak{C}'_1}, \frac{\mathfrak{C}'_1}{\mathfrak{C}'_2}, \frac{\mathfrak{C}'_2}{\mathfrak{C}'_3}, \dots, \frac{\mathfrak{C}'_k}{\mathfrak{R}}$$

are

$$\frac{c}{c'_1}, \frac{c'_1}{c'_2}, \frac{c'_2}{c'_3}, \dots, \frac{c'_k}{1}$$

We shall show that the numbers  $c, c_1, c_2, \dots, c_k$  are identical with the numbers  $c, c'_1, c'_2, \dots, c'_k$ , if the sequence is neglected. By assuming the truth of the theorem for

the divisors of  $\mathfrak{C}$  which are of lower degree than  $\mathfrak{C}$ , we may show it to be true also for the series including  $\mathfrak{C}$ .

Take the two connected chains of normal divisors

$$\begin{array}{c} \mathfrak{C}, \mathfrak{A}, \mathfrak{A}_1, \dots, \mathfrak{K} \\ \mathfrak{C}, \mathfrak{B}, \mathfrak{B}_1, \dots, \mathfrak{N}, \end{array}$$

in which the  $\mathfrak{A}$ 's and  $\mathfrak{B}$ 's are different. We shall show that the realms of both series are relatively equal (Art. 77) to one another.

Let  $\mathfrak{D}$  be the greatest common divisor of  $\mathfrak{A}$  and  $\mathfrak{B}$ . Let  $d, a, b$  be the degrees of these respective realms. It was seen in Art. 80, end, that  $\mathfrak{D}$  is a normal realm. As there is no divisor between  $\mathfrak{C}$  and  $\mathfrak{A}$  and none between  $\mathfrak{C}$  and  $\mathfrak{B}$ , it is evident that  $\mathfrak{C}$  is the least common multiple of  $\mathfrak{A}$  and  $\mathfrak{B}$  (Art. 47) so that  $\mathfrak{C} = \mathfrak{A} \cdot \mathfrak{B}$ . We may show that  $\mathfrak{C}, \mathfrak{A}, \mathfrak{D}$  and  $\mathfrak{C}, \mathfrak{B}, \mathfrak{D}$  form connected chains. To prove this we need only show that if there were a normal divisor between  $\mathfrak{A}$  and  $\mathfrak{D}$ , then there would be also one between  $\mathfrak{C}$  and  $\mathfrak{B}$ ; and if there were one between  $\mathfrak{B}$  and  $\mathfrak{D}$  there would be one between  $\mathfrak{C}$  and  $\mathfrak{A}$ . Suppose that  $\mathfrak{A}'$  is a normal divisor between  $\mathfrak{A}$  and  $\mathfrak{D}$  and let  $\mathfrak{C}'$  be the least common multiple of  $\mathfrak{A}'$  and  $\mathfrak{B}$ . We assert  $\mathfrak{C}'$  lies between  $\mathfrak{C}$  and  $\mathfrak{B}$ . For it is clear that  $\mathfrak{C}'$  is a normal realm that is a divisor of  $\mathfrak{C}$  and a multiple of  $\mathfrak{B}$ . We have then only to show that  $\mathfrak{C}'$  is equal to neither  $\mathfrak{C}$  nor to  $\mathfrak{B}$ . The greatest common divisor of  $\mathfrak{A}'$  and  $\mathfrak{B}$  is  $\mathfrak{D}$ , for  $\mathfrak{D}$  is the greatest common divisor of  $\mathfrak{A}$  and  $\mathfrak{B}$  and further  $\mathfrak{A}'$  is a divisor of  $\mathfrak{A}$  while  $\mathfrak{D}$  is a divisor of  $\mathfrak{A}'$  and  $\mathfrak{B}$ .

If  $c'$  is the degree of  $\mathfrak{C}'$  and  $a'$  that of  $\mathfrak{A}'$ , it follows since the realms are normal realms (Art. 76), that

$$c'd = a'b \quad \text{and} \quad cd = ab.$$

We thus have

$$\frac{c}{c'} = \frac{a}{a'}.$$

Since  $a > a'$ , it follows that  $c > c'$  and therefore  $\mathfrak{C} > \mathfrak{C}'$ . Further  $\mathfrak{A}'$  is different  $\mathfrak{D}$ , it being  $> \mathfrak{D}$ . It follows that  $\mathfrak{A}'$  is not a divisor of  $\mathfrak{B}$ ; and since  $\mathfrak{A}'$  is a divisor of  $\mathfrak{C}'$ , it follows that  $\mathfrak{C}'$  is different from  $\mathfrak{B}$ . Hence if between  $\mathfrak{A}$  and  $\mathfrak{D}$  there were to lie a normal realm, there would also be one between  $\mathfrak{C}$  and  $\mathfrak{B}$  and *vice versa*. Hence  $\mathfrak{C}, \mathfrak{A}, \mathfrak{D}$  is a connected chain as is also  $\mathfrak{C}, \mathfrak{B}, \mathfrak{D}$ .

ART. 83. Consider next the following four chains of normal divisors:

- (1)  $\mathfrak{C}, \mathfrak{A}, \mathfrak{D}, \mathfrak{D}', \dots, \mathfrak{R}$
- (2)  $\mathfrak{C}, \mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{R}$
- (3)  $\mathfrak{C}, \mathfrak{B}, \mathfrak{B}_1, \mathfrak{B}_2, \dots, \mathfrak{R}$
- (4)  $\mathfrak{C}, \mathfrak{B}, \mathfrak{D}, \mathfrak{D}', \dots, \mathfrak{R}$ .

Since  $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$  we have  $ab = cd$  and hence also

$$\frac{\mathfrak{C}}{\mathfrak{B}} = \frac{\mathfrak{A}}{\mathfrak{D}}$$

and

$$\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{\mathfrak{B}}{\mathfrak{D}}$$

(Arts. 75 and 76). Hence if we take the series (1) and (4)

$$\frac{\mathfrak{C}}{\mathfrak{A}'} \frac{\mathfrak{A}}{\mathfrak{D}'} \frac{\mathfrak{D}}{\mathfrak{D}''} \dots,$$

$$\frac{\mathfrak{C}}{\mathfrak{B}'} \frac{\mathfrak{B}}{\mathfrak{D}'} \frac{\mathfrak{D}}{\mathfrak{D}''} \dots,$$

it is seen that these series are identical, only the first two terms are interchanged. It is also seen that (1) and (2) are identical by hypothesis, since they have the terms  $\mathfrak{C}, \mathfrak{A}$  in common and the theorem is supposed to be true from  $\mathfrak{A}$  to  $\mathfrak{R}$ . Similarly (3) and (4) are identical, and consequently also (2) and (3) are equal, since the quotients in both series are neglecting the sequence relatively equal.

ART. 84. With the material which has been formulated, we are now able to state the following theorem. We know that the root of an algebraic equation is expressed through its coefficients and involves the extraction of roots.

THEOREM. *Suppose that we have an irrational quantity which has been found through the extraction of roots: let rational functions be formed of this quantity, the coefficients belonging to a fixed realm. Then form another quantity by extraction of roots of these functions. Further form rational functions of this new quantity, etc. The root expression so formed satisfies an algebraic equation. Form the norm  $\mathfrak{C}$  of this equation. The numbers  $\frac{c}{c_1}, \frac{c_1}{c_2}, \dots$ , that are therewith determined, are powers of prime numbers, if  $\mathfrak{C}$  is the norm of a solvable realm. Reciprocally, if  $\frac{c}{c_1}, \frac{c_1}{c_2}, \dots$ , are powers of prime numbers, then  $\mathfrak{C}$  is the norm of a solvable realm.<sup>1</sup> For the truth of the theorem it is not necessary that the chain of normal divisors be a continuous one. The necessary and sufficient condition that the quantities of a realm be expressible through the extraction of roots is that the integers  $\frac{c}{c_1}, \frac{c_1}{c_2}, \dots$  be the powers of prime numbers. Galois stated the theorem for prime numbers (but not for powers of these numbers), viz., that such an equation could be solved through the extraction of roots and that the roots could be expressed rationally in terms of one another.<sup>2</sup> Jordan observed that the numbers  $\frac{c}{c_1}, \frac{c_1}{c_2}, \dots$ , are invariant. It may also be observed that the associated realms themselves are invariant.*

<sup>1</sup> See for example Frobenius, *Crelle*, Vol. 100. Sylow, *Math. Ann.*, Vol. V, p. 589. Hölder, *Math. Ann.*, Vol. 34, p. 47.

<sup>2</sup> Camille Jordan, *Journ. de Math.* (2) T. 12, p. 111. Camille Jordan, *Journal de l'École Poly.*, Vol. 38, p. 190 (1861). Abel, *Oeuvres*, II, p. 222 and pp. 233, 256, 260, 262, 266, 270, 279.



ART. 85. **Realms of Rationality That Are Associated with the Cubic Equation.** Write the general cubic in the form

$$x^3 - p_1x^2 + p_2x - p_3 = 0,$$

and denote its roots by  $x_0, x_1, x_2$ . Let the quantities  $p_1, p_2, p_3, \omega$ , where  $\omega$  is a cube root of unity constitute a stock-realm  $\mathfrak{R}$ . To this realm adjoin the quantity  $x_0$  and denote the realm  $\mathfrak{R}(x_0)$  by  $\mathfrak{A}$ , which is evidently of the third degree. The conjugate realms are  $\mathfrak{R}(x_1)$  and  $\mathfrak{R}(x_2)$ . Form the normal realm (Art. 53)

$$\mathfrak{R}(x_0)\mathfrak{R}(x_1)\mathfrak{R}(x_2) = \mathfrak{R}(x_0, x_1, x_2) = \mathfrak{R}(x_0, x_1) = \mathfrak{C},$$

say. Consider next the linear expression

$$z = x_0 + \omega x_1 + \omega^2 x_2,$$

and note that the six values that this function may take when  $x_0, x_1, x_2$  are permuted, are

$$(1) \quad \begin{cases} z = x_0 + \omega x_1 + \omega^2 x_2, & \omega^2 z = x_1 + \omega x_2 + \omega^2 x_0, \\ & \omega z = x_2 + \omega x_0 + \omega^2 x_1, \\ z' = x_0 + \omega^2 x_1 + \omega x_2, & \omega^2 z' = x_2 + \omega x_1 + \omega^2 x_0, \\ & \omega z' = x_1 + \omega x_0 + \omega^2 x_2. \end{cases}$$

Since  $zz' = p_1^2 - 3p_2$ , it is seen that the  $z'$  may be expressed rationally in terms of  $z$ , since  $\omega$  is an element of the stock-realm. The same is true of all six of the above values. It follows<sup>1</sup> that  $z$  is a primitive quantity of the realm  $\mathfrak{C}$ , so that  $\mathfrak{C} = \mathfrak{R}(z)$ .

Consider next the third powers of the six quantities in (1). It is seen that only  $z^3$  and  $z'^3$  are different. These quantities  $z^3$  and  $z'^3$  belong therefore to a quadratic realm. Further note that the square root of the discriminant is a two-valued function of the third degree in

<sup>1</sup> Lagrange, III, 403 writes: "Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire; tout se réduit, comme on voit, à une espèce de calcul des combinaisons, par lequel on trouve a priori les résultats auxquels on doit s'attendre."

$z$ , the two values being  $\sqrt{D}$  and  $-\sqrt{D}$ , where

$$(2) \quad \begin{cases} D = (x_0 - x_1)^2(x_1 - x_2)^2(x_2 - x_0)^2. & \text{For it is seen that} \\ \sqrt{D} = +(x_0 - x_1)(x_1 - x_2)(x_2 - x_0), \\ z^3 = \frac{1}{2}(2p_1^3 - qp_1p_2 + 27p_3) + 3/2\sqrt{-3}\sqrt{D}; \end{cases}$$

and the interchange of  $x_1$  and  $x_2$  in (1) and (2) changes  $z$  to  $z'$  and  $\sqrt{D}$  to  $-\sqrt{D}$ . And it is evident that one of these quantities may be expressed rationally in terms of the other. It follows that the realm of the sixth degree contains the realm, say  $\mathfrak{B} = \mathfrak{K}(\sqrt{D})$ , which is a normal realm of the second degree. It further contains the realm  $\mathfrak{A} = \mathfrak{K}(x_0)$ , which is not a normal realm. Hence the realm  $\mathfrak{C}$  is the least common multiple of the realms  $\mathfrak{A}$  and  $\mathfrak{B}$ . Let  $\mathfrak{D}$  be the greatest common divisor of these two realms. From Art. 76 it is evident that the relation  $cd = ab$  exists among the degrees of the four realms  $\mathfrak{A}$ ,  $\mathfrak{B}$ ,  $\mathfrak{C}$ ,  $\mathfrak{D}$ , so that

$$\frac{\mathfrak{C}}{\mathfrak{B}} = \frac{\mathfrak{A}}{\mathfrak{D}} = \frac{\mathfrak{A}}{\mathfrak{K}}.$$

If the realm  $\mathfrak{C}$  is considered with respect to the realm  $\mathfrak{B}$ , it is seen that  $\mathfrak{C}$  is of the third degree and may be written  $\mathfrak{C} \equiv \mathfrak{K}(x_0, x_1) = \mathfrak{K}(x_0, \sqrt{D})$ . Further since  $\mathfrak{C}$  is a normal realm, the quantities  $x_1, x_2$  may be expressed rationally through  $x_0$  and  $\sqrt{D}$ .

To verify this, observe that

$$\begin{aligned} \sqrt{D} &= (x_1 - x_0)(x_2 - x_0)(x_2 - x_1), \\ F(x) &= (x - x_0)(x - x_1)(x - x_2), \\ F'(x_0) &= (x_0 - x_1)(x_0 - x_2). \end{aligned}$$

It is seen that

$$x_2 - x_1 = \frac{\sqrt{D}}{F'(x_0)};$$

and since  $x_2 + x_1 = p_1 - x_0$ , it results that

$$2x_2 = p_1 - x_0 + \frac{\sqrt{D}}{F'(x_0)}$$

and

$$2x_1 = p_1 - x_0 - \frac{\sqrt{D}}{F'(x_0)}.$$

In the same way it may be shown that

$$2x_2 = p_1 - x_1 - \frac{\sqrt{D}}{F'(x_1)}, \quad 2x_0 = p_1 - x_1 + \frac{\sqrt{D}}{F'(x_1)};$$

$$2x_0 = p_1 - x_2 - \frac{\sqrt{D}}{F'(x_2)}, \quad 2x_1 = p_1 - x_2 + \frac{\sqrt{D}}{F'(x_2)}.$$

In Art. 81 a connected chain of normal divisors was defined. Such a case is present here, namely,  $\mathfrak{C}$  of the sixth degree,  $\mathfrak{B}$  of the second degree,  $\mathfrak{A}$  of the third degree and  $\mathfrak{R}$  of the first degree. Their quotients offer the prime integers 3 and 2; and to this is due the fact that the cubic may be solved through the extraction of roots. Thus it is seen that if the radical  $\sqrt{D}$  be considered among the quantities regarded as known, it is possible in the realm of  $\mathfrak{R}(\sqrt{D})$  to express any root of a cubic as a rational function of any other root and known quantities. (See Serret, *Algèbre supérieure*, Vol. II, p. 406). Similar results were derived by the author for the roots of the biquadratic. See examples and references at the end of the chapter.

**ART. 86. Realms of Rationality Connected with the Biquadratic.** Write the biquadratic in the form

$$F(x) = ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0$$

and denote its roots by  $x_0, x_1, x_2, x_3$ . Next form the normal realm

$$\begin{aligned} \mathfrak{R}(x_0)\mathfrak{R}(x_1)\mathfrak{R}(x_2)\mathfrak{R}(x_3) &= \mathfrak{R}(x_0, x_1, x_2, x_3) \\ &= \mathfrak{R}(x_0, x_1, x_2) = \mathfrak{C}, \end{aligned}$$

say. This is a realm of the 24th degree, since the four roots may be permuted in 24 ways. In the Theory of Equations (see for example Burnside and Panton, Fourth

Edition, 1899, Art. 61), it is seen that

$$\begin{aligned} ax_0 + b &= \sqrt{p} - \sqrt{q} - \sqrt{r}, & ax_1 + b &= -\sqrt{p} + \sqrt{q} - \sqrt{r}, \\ ax_2 + b &= -\sqrt{p} - \sqrt{q} + \sqrt{r}, & ax_3 + b &= \sqrt{p} + \sqrt{q} + \sqrt{r}, \end{aligned}$$

where  $p, q, r$  are the roots of Euler's cubic

$$t^3 + 3Ht^2 + \left(3H^2 - \frac{a^2I}{4}\right)t - \frac{G^2}{4} = 0.$$

It is evident that  $x_0, x_1, x_2, x_3$  may be expressed rationally in terms of  $\sqrt{p}, \sqrt{q}, \sqrt{r}$ , and *vice versa*; and consequently it follows that

$$\mathfrak{C} = \Re(x_0, x_1, x_2) = \Re(\sqrt{p}, \sqrt{q}, \sqrt{r}).$$

From this it is also seen that  $\mathfrak{C}$  contains the realm of all rational quantities in  $p, q, r$ , and that is the realm  $\Re(p, q, r) = \mathfrak{B}$ , where  $\mathfrak{B}$  like  $\mathfrak{C}$  is a normal realm being equal to  $\Re(p)\Re(q)\Re(r)$ , the quantities  $p, q, r$  being the roots of a cubic. It was seen in the preceding article that  $\mathfrak{B}$  in its turn contained the normal realm of the second degree  $\Re(\sqrt{D}) = \mathfrak{A}$ , say; while  $\mathfrak{A}$  contains the stock-realm  $\Re$  of the first degree. The quotients of the degrees of these realms are  $\frac{24}{6} = 2^2, \frac{6}{2} = 3, \frac{2}{1} = 2$ , which are powers of prime integers.

It follows from Art. 84 that the associated equations are solvable. If further the realm  $\mathfrak{C}$  is considered with respect to the realm  $\mathfrak{B}$ , then  $\mathfrak{C}/\mathfrak{B}$  is of the fourth degree and  $x_0$  is a primitive quantity in it. It results that the other roots  $x_1, x_2, x_3$  may be rationally expressed in terms of  $x_0, p, q, r$ .

#### EXAMPLES

1. If

$$ax_0 + b = \sqrt{p} + \sqrt{q} + \sqrt{r} = \sigma \text{ and } ax_1 + b = \sqrt{p} - \sqrt{q} - \sqrt{r} = T,$$

show that the *rational* relations

$$\begin{aligned} T^4 + T^3\sigma + 3H(T^2 + T\sigma + 6p) + G(3\sigma + 5T) - 2p(T^2 + 2T\sigma - 6p) &= 0, \\ \sigma^4 + \sigma^3T + 3H(\sigma^2 + \sigma T + 6p) + G(3T + 5\sigma) - 2p(\sigma^2 + 2\sigma T - 6p) &= 0 \end{aligned}$$

exist, where  $p, q, r$  are the roots of the equation

$$t^3 + 3Ht^2 + \left(3H^2 - \frac{a^2I}{4}\right)t - \frac{G^2}{4} = 0;$$

and that is:  $\sigma$  may be expressed rationally in  $T$  and *vice versa*.

2. Show that the following *integral* relations exist:

$0 = T[8p^3 + 12Hp^2 + G^2] + 4p^2\sigma^3 + 2Gp\sigma^2 + (24Hp^2 + G^2)\sigma + 6Gp(2p + H)$   
with another equation having  $T$  and  $\sigma$  interchanged and five other similar pairs of relations.

3. Write 
$$\frac{a^6\Delta G^2}{8p^3 + 12Hp^2 + G^2} = A_0p^2 + A_1p + A_2,$$

where  $\Delta$  is the discriminant of the biquadratic, and show that  $A_0, A_1,$  and  $A_2$  are integral functions of  $H, G^2$  and  $I$ .

4. Write

$$G^2a^6\Delta T = C_0\sigma^3 + C_1\sigma^2 + C_2\sigma + C_3; \quad G^2a^6\Delta\sigma = C_0T^3 + C_1T^2 + C_2T + C_3$$

and show that  $C_0, C_1, C_2, C_3$  are integral functions of  $p$  with coefficients that are integral functions in  $H, G^2, I$ .

5. Show that if the equations  $8t^3 + 12Ht^2 + G^2 = 0$  and the Euler Cubic  $t^3 + 3Ht^2 + \left(3H^2 - \frac{a^2I}{4}\right)t - \frac{G^2}{4} = 0$  (where  $G \neq 0$ ) have a common root, the original biquadratic has a double root.

For solutions of Examples 1-5, see *Am. Math. Monthly*, Vol. XXVI, pp. 292-5, where they were given for the first time by the author.

6. In Art. 53 let  $x, x', x''$  be roots of  $x^3 + Ax + B = 0$ . Write  $\sigma = 2x + 3x' + x'', \sigma' = 2x' + 3x + x'', \sigma'' = 2x'' + 3x' + x, \sigma''' = 2x + 3x'' + x', \sigma^{(4)} = 2x' + 3x'' + x, \sigma^{(5)} = 2x'' + 3x + x'$ .

Further write  $\phi(t) = (t - \sigma)(t - \sigma') \cdots (t - \sigma^{(5)})$ . Calculate  $x$  from the formula 
$$\phi(t) \left[ \frac{x}{t - \sigma} + \frac{x'}{t - \sigma'} + \frac{x''}{t - \sigma''} + \frac{x'''}{t - \sigma'''} + \frac{x^{(4)}}{t - \sigma^{(4)}} + \frac{x^{(5)}}{t - \sigma^{(5)}} \right].$$

Similarly determine  $x'$  from  $\phi(t) \left[ \frac{x'}{t - \sigma} + \frac{x}{t - \sigma'} + \cdots \right]$ . Finally determine  $x''$  as a rational function of  $\sigma$ ; also determine  $\sigma'$  and  $\sigma''$  as rational functions of  $\sigma$ .



## CHAPTER IV

### ALGEBRAIC INTEGERS

ART. 87. A quantity  $x$  is by definition an *algebraic number* if it satisfies an *irreducible* algebraic equation

$$t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t + a_n = 0,$$

where  $a_1, a_2, \dots, a_n$  are integral or fractional numbers that belong to a fixed realm of rationality <sup>1</sup>  $\mathfrak{R}$ ; and  $x$  is by definition an *algebraic integer* if the quantities  $a_1, a_2, \dots, a_n$  are all integers in the fixed realm. This conception is true also for the case of rational integers, for here  $n = 1$  and the equation which  $x$  satisfies is  $t - a = 0$ .

If  $x$  is an algebraic integer, all the conjugate quantities to  $x$  are algebraic integers.

The *product* of these quantities was called (Art. 59) the *norm* of  $x$  [written  $N(x)$ ]. The sum of these quantities may be called the *spur*<sup>2</sup> of  $x$  [written  $S(x)$ ]. It is evident that the spur and norm of an algebraic integer are rational integers; for in the above equation

$$S(x) = -a_1 \quad \text{and} \quad N(x) = (-1)^n a_n.$$

*If an algebraic quantity satisfies a reducible or an irreducible algebraic equation, in which the coefficient of the highest power = 1, while the remaining coefficients are all integers belonging to a fixed realm, the algebraic quantity is integral.*

For, if the equation is reducible, it may always be

<sup>1</sup> Those who are reading this subject for the first time may consult with advantage a paper by L. J. Mordell; "An introductory account of the arithmetical theory of algebraic numbers, etc." *Bulletin of the Am. Math. Society*, Vol. 29, p. 445.

<sup>2</sup> Dedekind, § 167 of the Dirichlet *Zahlentheorie*; see also Dedekind-Weber, *Crelle*, Vol. 92, p. 188.

resolved into irreducible factors in which the coefficient of the highest power of the variable = 1, and the other coefficients are all integral (Art. 10). One of these irreducible factors must be satisfied by the algebraic quantity, which is consequently an algebraic integer.

This may also be shown as follows: If

$$h(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \dots + c_{n-1}x + c_n,$$

where the  $c$ 's are integers, and if  $h(x) = f(x) \cdot g(x)$  where

$$f(x) = x^r + \frac{a_1}{a_0}x^{r-1} + \frac{a_2}{a_0}x^{r-2} + \dots + \frac{a_{r-1}}{a_0}x + \frac{a_r}{a_0}$$

and

$$g(x) = x^s + \frac{b_1}{b_0}x^{s-1} + \frac{b_2}{b_0}x^{s-2} + \dots + \frac{b_{s-1}}{b_0}x + \frac{b_s}{b_0},$$

the integers  $a_0, a_1, \dots, a_r$  and the integers  $b_0, b_1, \dots, b_s$  having no common divisor, save unity, then is  $a_0 = 1 = b_0$ .

For

$$a_0 b_0 h(x) = (a_0 x^r + a_1 x^{r-1} + \dots + a_r)(b_0 x^s + b_1 x^{s-1} + \dots + b_s).$$

If  $p$  is a prime integer that divides  $a_0 b_0$ , then (Art. 4) it must divide one of the factors on the right hand side. But the coefficients of neither of these factors have a common divisor other than unity.

Making an application of this to the special case that  $x$  is a rational number, we have the theorem:

*Every rational root of an algebraic equation, in which the coefficient of the highest power of  $x = 1$  and the remaining coefficients integers, is integral.*

For if  $x = \frac{r}{s}$  (where  $r$  and  $s$  are relatively prime) is a root of the equation

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n = 0,$$

where the  $a$ 's are integers, then

$$r^n + a_1 s r^{n-1} + a_2 s^2 r^{n-2} + \dots + a_{n-1} s^{n-1} r + a_n s^n = 0.$$

It follows that  $s$  must be = 1; otherwise if  $p$  is a prime

integer that divides  $s$ , it must also divide  $r$ , contrary to the assumption that  $r$  and  $s$  are relatively prime. (See also Art. 10.)

Algebraic numbers that are not integral are called *fractional algebraic numbers*.<sup>1</sup>

ART. 88. That the algebraic integers are reproduced by the operations of addition, subtraction and multiplication is seen from the theorems below.

THEOREM I. *The sum of two algebraic integers is an algebraic integer.*

Let  $\alpha$  and  $\beta$  be integers which satisfy the equations

$$\begin{aligned}\alpha^r &= a_1\alpha^{r-1} + a_2\alpha^{r-2} + \dots + a_r, \\ \beta^s &= b_1\beta^{s-1} + b_2\beta^{s-2} + \dots + b_s,\end{aligned}$$

where the  $a$ 's and  $b$ 's are integers belonging to a fixed realm  $\mathfrak{R}$ . In the sequel, unless otherwise stated, this realm  $\mathfrak{R}$  is taken as the realm of natural numbers; and we shall denote it by  $R$  (see Art. 28). Further let

$$\mu = \alpha + \beta$$

and form the  $n = r \cdot s$  numbers

$$\alpha^\rho \beta^\sigma \quad (\rho = 0, 1, \dots, r-1; \quad \sigma = 0, 1, \dots, s-1),$$

which denote in any sequence by

$$w_1, w_2, \dots, w_n.$$

It is evident that

$$\mu w_\nu \quad (\nu = 1, 2, \dots, n)$$

may be written in the form (Art. 52):

$$\mu w_\nu = a_{\nu 1} w_1 + a_{\nu 2} w_2 + \dots + a_{\nu n} w_n \quad (\nu = 1, 2, \dots, n),$$

where  $a_{\nu 1}, a_{\nu 2}, \dots, a_{\nu n}$  are integers (including zero) of  $R$ .

<sup>1</sup> Dedekind, § 173 of the Dirichlet *Zahlentheorie*. Also see J. König, *Einführung in die allgemeine Theorie der algebraischen Grössen*. Teubner, Leipzig, 1903.

Through the elimination of  $w_1, w_2, \dots, w_n$ , we have

$$\begin{vmatrix} a_{11} - \mu, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22} - \mu, & \dots, & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} - \mu \end{vmatrix} = 0,$$

from which it is seen that  $\mu$  satisfies an algebraic equation in which the coefficient of the highest power  $= 1$ , the other coefficients being integers in  $\mathbb{R}$ .

In the realm  $\mathfrak{R}(i)$  for example, that is, in the plane of the complex variable, algebraic integers are of the form  $x + iy$  where  $x$  and  $y$  are natural integers including zero. Such integers offer easy illustrations of the theorem just proved, as also of the following theorems.

*Another Proof.* Write

$$\Phi(x) = \prod_{i=1}^r \prod_{j=1}^s (x - (\alpha^{(i)} + \beta^{(j)}))$$

and observe that the coefficients of this polynomial are symmetric functions of the conjugate numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(r)}$  as also of  $\beta^{(1)}, \dots, \beta^{(s)}$ .

**THEOREM II.** *The difference of two algebraic integers is an algebraic integer.*

This may be proved in an analogous manner as Theorem I.

**THEOREM III.** *The product of two algebraic integers is an algebraic integer.*

Let  $\alpha$  and  $\beta$  be two algebraic integers defined as above and let  $\mu = \alpha\beta$ . Further denote the numbers

$$\alpha^\rho \beta^\sigma \quad (\rho = 0, 1, \dots, r-1; \quad \sigma = 0, 1, \dots, s-1)$$

in any sequence by  $w_1, w_2, \dots, w_n$ . It is evident that

$$\mu w_\nu = c_{\nu 1} w_1 + c_{\nu 2} w_2 + \dots + c_{\nu n} w_n \quad (\nu = 1, 2, \dots, n),$$

where the  $c$ 's are integers (including zero) of  $R$ . The proof is in the same form now as in Theorem I.

If  $\alpha$  is an algebraic integer and  $a$  a rational integer, then  $a\alpha$  is an algebraic integer; for  $\alpha$  must satisfy an algebraic equation

$$\alpha^n = a_1\alpha^{n-1} + a_2\alpha^{n-2} + \dots + a_n,$$

where the  $a$ 's are rational integers. It is also evident that

$$(a\alpha)^n = aa_1(a\alpha)^{n-1} + a^2a_2(a\alpha)^{n-2} + \dots + a^na_n,$$

where the coefficients are also rational integers. Similarly it may be proved that any algebraic number multiplied by a suitably chosen rational integer gives an algebraic integer. (Art. 93). It follows further that every function integral in any number of algebraic integers with integral (rational in  $R$ ) coefficients is an algebraic integer. (Further see Art. 162).

There is still a fourth operation through which algebraic integers may be reproduced:

**THEOREM IV.** *If  $\mu$  satisfies an algebraic equation in which the coefficient of the highest power = 1, the other coefficients being algebraic integers, then  $\mu$  is an algebraic integer.*

For let

$$\mu^m = \alpha_1\mu^{m-1} + \alpha_2\mu^{m-2} + \dots + \alpha_m,$$

where  $\alpha_1, \alpha_2, \dots, \alpha_m$  are algebraic integers which satisfy the equations, say

$$\alpha_\nu^{r_\nu} = a_{\nu 1}\alpha_\nu^{r_\nu-1} + a_{\nu 2}\alpha_\nu^{r_\nu-2} + \dots + a_{\nu m} \quad (\nu=1, 2, \dots, m),$$

the quantities  $a_{\nu 1}, a_{\nu 2}, \dots, a_{\nu m}$  being integers in  $R$ . Further denote in any sequence the  $m \cdot r_1 \cdot r_2 \dots r_m = n$  quantities

$$\mu^\lambda \alpha_1^{\rho_1} \alpha_2^{\rho_2} \dots \alpha_m^{\rho_m} \left( \begin{array}{c} \rho_1=0, 1, \dots, r_1-1, \rho_2=0, 1, \dots, r_2-1, \\ \dots \\ \rho_m=0, 1, \dots, r_m-1, \lambda=0, 1, 2, \dots, m-1 \end{array} \right)$$



by  $w_1, w_2, \dots, w_n$ . It is evident as above that

$$\mu w_\nu = d_{\nu 1} w_1 + d_{\nu 2} w_2 + \dots + d_{\nu n} w_n \quad (\nu=1, 2, \dots, n),$$

where  $d_{\nu 1}, d_{\nu 2}, \dots, d_{\nu n}$  are integers (including zero) of  $\mathbb{R}$ . From now on the proof is the same as in Theorem I.

**COROLLARY.** It follows at once that if  $\mu$  is an algebraic integer, then  $\mu^{\frac{m}{n}}$  is also an algebraic integer. For write  $x = \mu^{\frac{m}{n}}$ ; then is  $1 \cdot x^n - \mu^m = 0$  and from above  $x$  is an algebraic integer. If further  $\mu^m$  is a rational integer and if  $x$  is a rational root of  $x^n - \mu^m = 0$ , then is  $x$  a rational integer. (See last article).

**EXAMPLE.** If  $\alpha$  is a root of  $x^3 + x^2 + x + 1 = 0$  and  $\beta$  a root of  $x^2 - 2x - 1 = 0$ , determine the equations which have as roots  $\alpha + \beta$ ,  $\alpha - \beta$ ,  $\alpha\beta$ .

If  $\beta$  is a root different from zero of the equation

$$x^n + B_1 x^{n-1} + B_2 x^{n-2} + \dots + B_{n-1} x + B_n = 0,$$

whose roots are rational numbers, then clearly

$$\left(\frac{1}{\beta}\right)^n + \frac{B_{n-1}}{B_n} \left(\frac{1}{\beta}\right)^{n-1} + \dots + \frac{B_1}{B_n} \frac{1}{\beta} + \frac{1}{B_n} = 0.$$

It follows that  $1/\beta$  satisfies the equation

$$x^n + \frac{B_{n-1}}{B_n} x^{n-1} + \dots + \frac{B_1}{B_n} x + \frac{1}{B_n} = 0$$

and is an algebraic number. It is clear, if we put  $\frac{1}{\beta} = \gamma$ , that  $\alpha + \gamma$ ,  $\alpha\gamma$ , etc., are algebraic numbers as in

Art. 88. Hence, any expression formed of algebraic numbers and rational integers in a rational manner is an algebraic number.

**ART. 89. Definitions.** If  $\alpha$  and  $\beta$  are two algebraic numbers (integral or fractional), then  $\alpha$  is said to be *divisible* by  $\beta$ , if  $\alpha/\beta$  is an algebraic integer.

The *spur*<sup>1</sup> and the *norm* of an algebraic quantity may be defined *relatively* with regard to an algebraic realm  $\Re(x)$  in which the given algebraic quantity is found. Let  $x$  be a root of the irreducible equation  $f(t)=0$  of degree  $a$  and let the conjugate roots be  $x^{(1)}, x^{(2)}, \dots, x^{(a-1)}$ . If then  $\alpha$  is a quantity that belongs to the realm  $\Re(x)$ , then is  $\alpha = \varphi(x)$  where  $\varphi$  is a rational function with coefficients that belong to the stock realm  $R$ . Relative to the realm  $\Re(x)$  the spur and norm of  $\alpha$  may be defined through the relations (see also Art. 59)

$$S(\alpha) = \varphi(x) + \varphi(x^{(1)}) + \varphi(x^{(2)}) + \dots + \varphi(x^{(a-1)}),$$

$$N(\alpha) = \varphi(x) \cdot \varphi(x^{(1)}) \cdot \dots \cdot \varphi(x^{(a-1)}).$$

If  $\alpha$  and  $\beta$  are two algebraic quantities that belong to  $\Re(x)$ , then

$$N(\alpha \cdot \beta) = N(\alpha)N(\beta)$$

and

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}.$$

Since the norm of an algebraic integer is a rational integer, it follows that if  $\alpha$  is divisible by  $\beta$ ,  $N(\alpha)$  is divisible by  $N(\beta)$ . The inverse of this theorem is not true: that an algebraic quantity  $x$  be integral, it is not only necessary that its norm be a rational integer, but also all the elementary symmetric functions of the conjugate quantities (of which it is one) must be integral.

As in the case of division for rational numbers the two following elementary theorems are true also of algebraic numbers:

**THEOREM I.** *If  $\alpha$  is divisible by  $\beta$ , and  $\beta$  by  $\gamma$ , then is  $\alpha$  divisible by  $\gamma$ .*

For if  $\alpha/\beta$  and  $\beta/\gamma$  are two algebraic integers, then the product (see Theorem II in Art. 88) of two such integers

<sup>1</sup> See Art. 59.

is an algebraic integer; it follows that  $\frac{\alpha}{\beta} \cdot \frac{\beta}{\gamma}$ , that is,  $\frac{\alpha}{\gamma}$  is an algebraic integer.

**THEOREM II.** *If  $\alpha$  and  $\beta$  are both divisible by  $\kappa$ , then  $\alpha\xi \pm \beta\eta$  is divisible by  $\kappa$ , where  $\xi$  and  $\eta$  are algebraic integers.*

For since  $\frac{\alpha}{\kappa}$  and  $\xi$  on the one hand, and  $\frac{\beta}{\kappa}$  and  $\eta$  on the other, are four algebraic integers,  $\frac{\alpha}{\kappa} \cdot \xi$  and  $\frac{\beta}{\kappa} \cdot \eta$  are algebraic integers, and also  $\frac{\alpha}{\kappa}\xi \pm \frac{\beta}{\kappa}\eta$ , i.e.,  $\frac{\alpha\xi \pm \beta\eta}{\kappa}$  is an algebraic integer.

The Theorem II may be generalized as follows: If the algebraic numbers,  $\alpha, \beta, \gamma, \dots$  are all divisible by  $\kappa$  and if  $\xi, \eta, \zeta, \dots$  are algebraic integers, then also

$$\frac{\alpha\xi \pm \beta\eta \pm \gamma\zeta \pm \dots}{\kappa}$$

is an algebraic integer.

**ART. 90. Algebraic Units.** An algebraic integer  $\epsilon$  is called a *unit* if 1 is divisible by  $\epsilon$ . Hence if  $\epsilon$  is a unit, both  $\epsilon$  and  $\frac{1}{\epsilon}$  are algebraic integers. This definition corresponds to the definition of the rational unit 1.

In the realm  $\mathfrak{N}(i)$  for example, the units are  $\pm 1$  and  $\pm i$ .

Every algebraic integer is divisible by any algebraic unit. For if  $\alpha$  is an algebraic integer and  $\epsilon$  an algebraic unit, then since  $\frac{1}{\epsilon}$  is an algebraic integer,  $\alpha \cdot \frac{1}{\epsilon}$  is an algebraic integer. If of two algebraic numbers (integers or fractions)  $\alpha$  and  $\beta$ , the one is divisible by the other, then each of the quotients is an algebraic unit. For put  $\beta/\alpha = \epsilon$  and  $\alpha/\beta = \epsilon'$ , where  $\epsilon$  and  $\epsilon'$  are algebraic integers; then is  $\beta/\alpha \cdot \alpha/\beta = \epsilon\epsilon' = 1$ , so that  $\epsilon = \frac{1}{\epsilon'}$ , and  $\epsilon' = \frac{1}{\epsilon}$  and con-

sequently 1 is divisible by  $\epsilon$  and also by  $\epsilon'$ , or  $\epsilon$  and  $\epsilon'$  are algebraic units.

A criterion by which it may be determined whether an algebraic integer is a unit, is as follows. If  $\epsilon$  is an algebraic integer, it satisfies an irreducible algebraic equation

$$\epsilon^n + e_1\epsilon^{n-1} + e_2\epsilon^{n-2} + \dots + e_{n-1}\epsilon + e_n = 0,$$

where the  $e$ 's are rational integers. Writing  $\epsilon' = \frac{1}{\epsilon}$  in this equation, we have

$$1 + e_1\epsilon' + e_2\epsilon'^2 + \dots + e_{n-1}\epsilon'^{n-1} + e_n\epsilon'^n = 0,$$

or

$$\epsilon'^n + \frac{e_{n-1}}{e_n}\epsilon'^{n-1} + \dots + \frac{e_1}{e_n}\epsilon' + \frac{1}{e_n} = 0.$$

This equation is also irreducible and in order that  $\epsilon'$  be an algebraic integer the coefficients in the last equation must be rational integers. Further since  $1/e_n$  is a rational integer, it follows that  $e_n = \pm 1$ . Hence a necessary condition that  $\epsilon$  be an algebraic unit is that  $e_n$ , [i.e.  $N(\epsilon)$ ] be  $= \pm 1$ . Here it is immaterial whether the *norm* is restricted (Art. 89) to a definite realm of rationality or not. For when restricted to a definite realm  $N(\epsilon)$  is a power of  $N(\epsilon)$  where  $N(\epsilon)$  is the product of the algebraic integers conjugate to  $\epsilon$  (including  $\epsilon$ ). (Art. 65). The *necessary* condition, viz.,  $N(\epsilon) = \pm 1$  is also a *sufficient* condition that  $\epsilon$  be an algebraic unit.

For if  $\alpha$  is an algebraic integer, then  $N(\alpha)$  is divisible by  $\alpha$ . To prove this note that if the irreducible equation which  $\alpha$  satisfies, is

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \dots + a_n = 0,$$

where  $a_1, a_2, \dots, a_n$  are rational integers, then

$$\begin{aligned} N(\alpha) &= (-1)^n a_n = (-1)^{n-1} (\alpha^n + a_1\alpha^{n-1} + \dots + a_{n-1}\alpha) \\ &= (-1)^{n-1} \alpha (\alpha^{n-1} + a_1\alpha^{n-2} + \dots + a_{n-1}); \end{aligned}$$

and consequently  $\frac{N(\alpha)}{\alpha}$  is an algebraic integer; or  $N(\alpha)$  is divisible by  $\alpha$ . Hence if  $\epsilon$  is an algebraic integer and  $N(\epsilon) = \pm 1$ , then is  $\frac{1}{\epsilon}$  an algebraic integer and consequently  $\epsilon$  is an algebraic unit. We have thus proved the theorem:

*The necessary and sufficient condition that an algebraic integer  $\epsilon$  be a unit, is that  $N(\epsilon) = \pm 1$ .*

ART. 91. A system of units is reproduced through the operations of multiplication and division; for we have the two following theorems:

THEOREM I. *The product of two units is a unit.*

THEOREM II. *The quotient of two units is a unit.*

For if  $\epsilon$  and  $\epsilon'$  are two algebraic units, then  $\epsilon$  and  $\epsilon'$ , as also  $1/\epsilon$  and  $1/\epsilon'$  are algebraic integers; hence also  $\epsilon\epsilon'$  and  $\frac{1}{\epsilon\epsilon'}$  are algebraic integers and consequently  $\epsilon\epsilon'$  is an algebraic unit.

Further  $\epsilon \cdot \frac{1}{\epsilon'} = \frac{\epsilon}{\epsilon'}$  and  $\epsilon' \cdot \frac{1}{\epsilon} = \frac{\epsilon'}{\epsilon}$  are algebraic integers, so

that  $\frac{\epsilon}{\epsilon'}$  is an algebraic unit.

If  $\alpha$  is an algebraic number and  $\epsilon$  a unit, then  $\alpha$  is divisible by  $\alpha\epsilon$  and also  $\alpha\epsilon$  is divisible by  $\alpha$ . Two such numbers which only differ through a multiplicative unit, of which the one is divisible by the other are called *associate numbers*. The one may be said to be an *associate* of the other. If  $\alpha$  is divisible by  $\beta$ , then every associate number of  $\alpha$  is divisible by every associate number of  $\beta$ . For if  $\frac{\alpha}{\beta}$  is an algebraic integer, then also

$\frac{\alpha\epsilon}{\beta\epsilon'}$  is an integer if  $\epsilon$  and  $\epsilon'$  are algebraic units. Hence in



the case of division any algebraic number may be replaced by one of its associate numbers.

The power of a unit with positive or negative exponent is always a unit, since the system of units is reproduced through multiplication and division; in fact, if  $\epsilon$  is an algebraic integer, then  $\epsilon^{r/s}$  is a unit. For if  $\epsilon$  and  $\epsilon' \left( = \frac{1}{\epsilon} \right)$  are algebraic integers, then also (Art. 88)  $\epsilon^{r/s}$  and  $\epsilon'^{r/s}$  are algebraic integers, so that  $\epsilon^{r/s}$  is an algebraic unit.

**ART. 92. Congruences.** If  $\alpha, \beta, \kappa$  are three arbitrary algebraic numbers, we write  $\alpha \equiv \beta \pmod{\kappa}$ , if  $\alpha - \beta$  is divisible by  $\kappa$ . From this definition we have the theorems as in the usual Theory of Numbers:

**THEOREM I.** *If  $\alpha \equiv \beta \pmod{\kappa}$ , then is also  $\beta \equiv \alpha \pmod{\kappa}$ .*

**THEOREM II.** *If two numbers are congruent to a third  $\pmod{\kappa}$ , they are congruent to each other.*

For if  $\alpha \equiv \beta \pmod{\kappa}$  and  $\beta \equiv \gamma \pmod{\kappa}$ , then  $\frac{\alpha - \beta}{\kappa}$  and  $\frac{\beta - \gamma}{\kappa}$  are algebraic integers and consequently  $\frac{\alpha - \beta}{\kappa} + \frac{\beta - \gamma}{\kappa}$  is an algebraic integer; that is,  $\frac{\alpha - \gamma}{\kappa}$  is an algebraic integer and  $\alpha \equiv \gamma \pmod{\kappa}$ .

**THEOREM III.** *If  $\alpha \equiv \beta \pmod{\kappa}$  and  $\alpha' \equiv \beta' \pmod{\kappa}$ , then is also  $\alpha \pm \alpha' \equiv \beta \pm \beta' \pmod{\kappa}$ .*

For since  $\frac{\alpha - \beta}{\kappa}$  and  $\frac{\alpha' - \beta'}{\kappa}$  are algebraic integers, then also

$$\frac{\alpha - \beta}{\kappa} \pm \frac{\alpha' - \beta'}{\kappa} = \frac{\alpha \pm \alpha' - (\beta \pm \beta')}{\kappa}$$

is integral. The analogous theorem for the multiplication of congruences is not true, neither is it true for

rational (fractional) numbers. For example, we have

$$10 \equiv 1 \pmod{3}$$

and

$$\frac{29}{2} \equiv \frac{5}{2} \pmod{3};$$

but

$$\frac{290}{2} \not\equiv \frac{5}{2} \pmod{3}.$$

If, however,  $\alpha, \beta, \alpha', \beta'$  are integers (rational or algebraic) and  $\kappa$  arbitrary (rational or algebraic) and if  $\alpha \equiv \alpha' \pmod{\kappa}$

and  $\beta \equiv \beta' \pmod{\kappa}$ , then are  $\frac{\alpha\beta - \alpha'\beta}{\kappa}$  and  $\frac{\alpha'\beta - \alpha'\beta'}{\kappa}$  integers, so that

$$\frac{\alpha\beta - \alpha'\beta}{\kappa} + \frac{\alpha'\beta - \alpha'\beta'}{\kappa} = \frac{\alpha\beta - \alpha'\beta'}{\kappa}$$

is integral, or  $\alpha\beta \equiv \alpha'\beta' \pmod{\kappa}$ .

If we wish to proceed as in The Theory of Rational Integers, we must first define a *prime* algebraic integer. If we define an algebraic integer as being *prime* when it can not be decomposed into two integers without one of these factors being a unit, we shall find that there is no integer which has this (see Arts. 28, 88, Corollary, 112) property. This difficulty may be overcome if we limit the algebraic integers to a fixed realm of rationality (Art. 112).

#### ALGEBRAIC INTEGERS OF A FIXED REALM

ART. 93. Suppose we have a definite realm of rationality, say  $\Omega = \mathfrak{R}(\vartheta)$  of the  $n$ th degree. The algebraic quantity  $\vartheta$  which determines the realm satisfies an irreducible equation (Art. 60) of the  $n$ th degree, say  $f(x) = 0$ .

If  $\alpha$  and  $\beta$  are two algebraic integers of this realm, then since  $\alpha$  and  $\beta$  are both rational functions of  $\vartheta$ , it

follows also that  $\mu = \alpha + \beta$  is a rational function of  $\vartheta$  and can be expressed in the form (Art. 44)

$$\mu = c_0 + c_1\vartheta + c_2\vartheta^2 + \dots + c_{n-1}\vartheta^{n-1},$$

where the  $c$ 's are rational numbers. Hence  $\mu$  belongs to the realm  $\mathfrak{R}(x)$ ; and, as we saw in (Art. 88)  $\mu$  is an algebraic integer. It follows that the realm  $\mathfrak{R}(\mu)$  is a divisor of  $\mathfrak{R}(x)$  and (Art. 67) the degree of the *irreducible* equation which  $\mu$  satisfies is a divisor of  $n$ . Hence the algebraic integers of  $\Omega$  are reproduced by addition. In the same way it is seen that they are reproduced by subtraction and multiplication.

In a similar manner as in Chapter III where all quantities of a definite realm were expressed through a *basis*, we shall now express all the integers of the realm  $\Omega$  through a basis.

We may first show that the basis of a finite realm  $\Omega$  may be so chosen that it consists only of algebraic integers:

If  $\vartheta$  is any algebraic number, it satisfies a certain algebraic equation of the form (Art. 87)

$$a_0\vartheta^n + a_1\vartheta^{n-1} + \dots + a_{n-1}\vartheta + a_n = 0,$$

where  $a_0, a_1, \dots, a_n$  are rational integers. If we multiply this equation by  $a_0^{n-1}$  and write  $a_0\vartheta = \eta$ , it follows that

$$\eta^n + a_1\eta^{n-1} + a_2a_0\eta^{n-2} + \dots + a_n a_0^{n-1} = 0,$$

where the coefficients are rational integers, the coefficient of the highest power being = 1. Hence  $\eta$  is an algebraic integer. We have thus shown that every fractional algebraic number  $\vartheta$  may be expressed in the form  $\eta/a_0$  where  $\eta$  is an algebraic integer and  $a_0$  a rational integer; or it is always possible to determine a rational integer  $a_0$  such that  $a_0\vartheta$  is an algebraic integer,  $\vartheta$  being any algebraic number.

If then  $\beta_1, \beta_2, \dots, \beta_n$  form a basis of the realm  $\Omega$ , we

may always determine  $n$  rational integers,  $k_1, k_2, \dots, k_n$ , such that  $k_1\beta_1, k_2\beta_2, \dots, k_n\beta_n$  are algebraic integers. Further since these  $n$  integers are linearly independent, they also form a basis of  $\Omega$ . Denote these  $n$  integers by  $\alpha_1, \alpha_2, \dots, \alpha_n$ . It is evident that the discriminant  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$  is a rational integer. For this discriminant is an integral function of the  $\alpha$ 's and of the quantities that are conjugate to the  $\alpha$ 's which are also algebraic integers; the discriminant is therefore integral. In Chapter II, Art. 22, end, we saw that the discriminant is also rational; hence it is a rational integer. Further since  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis,

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0.$$

If in the linear form  $\alpha_1x_1 + \alpha_2x_2 + \dots + \alpha_nx_n$  we write for the  $x$ 's all possible systems of rational numbers, we have all the quantities of the realm  $\Omega$  (Art. 57). Among these numbers are found all the algebraic integers of  $\Omega$ . If for  $x_1, x_2, \dots, x_n$  we write only rational integers, we have only algebraic integers of  $\Omega$ , although not necessarily all the integers of this realm. If all the integers of  $\Omega$  are not had in this manner, there is an algebraic integer, say  $\rho$ , such that

$$\rho = \frac{r_1\alpha_1 + r_2\alpha_2 + \dots + r_n\alpha_n}{r},$$

where  $r_1, r_2, \dots, r_n, r$  are rational integers without a greatest common divisor and  $r > 1$ . If  $r$  is *not* a prime integer, it is divisible by a prime integer,  $p$  say, so that  $r = pq$ , where  $p > 1$  and  $q$  is an integer. It follows that

$$\sigma = \rho q = \frac{r_1\alpha_1 + r_2\alpha_2 + \dots + r_n\alpha_n}{p}$$

is an algebraic integer in  $\Omega$ . Hence, if the expression  $\alpha_1x_1 + \alpha_2x_2 + \dots + \alpha_nx_n$  offers an algebraic integer for rational fractional values of the  $x$ 's, there is a system of

fractional values of the  $x$ 's in which the common denominator is  $p$  and for which the linear form  $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$  represents an algebraic integer  $\sigma$  of  $\Omega$ . As the integers  $r_1, r_2, \dots, r_n$  are *not* all divisible by  $p$ , suppose that  $r_1$  is relatively prime to  $p$ . Two integers  $s$  and  $t$  may always be determined such that

$$r_1 s - p t = 1.$$

It follows that

$$\sigma s - \alpha_1 t = \frac{\alpha_1 + s r_2 \alpha_2 + s r_3 \alpha_3 + \dots + s r_n \alpha_n}{p} = \beta_1,$$

say, is an algebraic integer in  $\Omega$ .

We thus have

$$\alpha_1 = p \beta_1 - s r_2 \alpha_2 - \dots - s r_n \alpha_n.$$

It is evident that the  $n$  quantities  $\beta_1, \alpha_2, \alpha_3, \dots, \alpha_n$  form a basis of  $\Omega$ ; for if there were a linear relation among them, there would exist a linear relation among the  $\alpha$ 's, when for  $\beta$ , its value in terms of the  $\alpha$ 's was written.

The realm  $\Omega$  of the  $n$ th degree contains a primitive quantity, say  $\vartheta$ , such that (Art. 61) all quantities of  $\Omega$  may be expressed linearly through  $1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}$ . Let the  $n$  quantities conjugate with  $\vartheta$  be  $\vartheta', \vartheta'', \dots, \vartheta^{(n)}$ , of which one is  $\vartheta$ . Represent next the quantities  $\beta_2, \alpha_1, \dots, \alpha_n$  through  $\vartheta$ . When this has been done the equation

$$\alpha_1 - p \beta_1 + s r_2 \alpha_2 + \dots + s r_n \alpha_n = 0$$

is an identical relation in  $\vartheta$  and consequently also in the quantities conjugate to  $\vartheta$ . We thus have the  $n$  relations

$$\alpha_1^{(\lambda)} = p \beta_1^{(\lambda)} - s r_2 \alpha_2^{(\lambda)} - s r_3 \alpha_3^{(\lambda)} - \dots - s r_n \alpha_n^{(\lambda)} \quad (\lambda = 1, 2, \dots, n).$$

From the theorem in determinants that the determinant remains unaltered if to one column the elements of another column multiplied by a constant factor are added, it follows that



$$\begin{vmatrix} \alpha'_1 & \alpha'_2 & \cdots & \alpha'_n \\ \alpha''_1 & \alpha''_2 & \cdots & \alpha''_n \\ \dots & \dots & \dots & \dots \\ \alpha^{(n)}_1 & \alpha^{(n)}_2 & \cdots & \alpha^{(n)}_n \end{vmatrix} = \begin{vmatrix} p\beta'_1 & \alpha'_2 & \cdots & \alpha'_n \\ p\beta''_1 & \alpha''_2 & \cdots & \alpha''_n \\ \dots & \dots & \dots & \dots \\ p\beta^{(n)}_1 & \alpha^{(n)}_2 & \cdots & \alpha^{(n)}_n \end{vmatrix};$$

and consequently  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = p^2 \Delta(\beta_1, \alpha_2, \dots, \alpha_n)$ . From this formula it is seen that  $\beta_1, \alpha_2, \alpha_3, \dots, \alpha_n$  form a basis; for  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$  is different from zero due to the fact that  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis. It is also evident, since  $p > 1$ , that

$$|\Delta(\beta_1, \alpha_2, \dots, \alpha_n)| < |\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)|.$$

Hence if there are any algebraic integers of  $\Omega$  which may be expressed through  $r_1\alpha_1 + r_2\alpha_2 + \dots + r_n\alpha_n$  when the  $r$ 's are rational (fractional) numbers, then it is always possible to determine a basis consisting of another set of algebraic integers, and such that the discriminant is less than  $|\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)|$ .

If further the linear form  $r_1\beta_1 + r_2\alpha_2 + \dots + r_n\alpha_n$  represents algebraic integers of  $\Omega$  for a system of fractional values of the  $r$ 's, by proceeding in the same manner we may derive another basis consisting of algebraic integers and such that the discriminant is less than  $|\Delta(\beta_1, \alpha_2, \dots, \alpha_n)|$ . By this process the absolute value of the discriminant which is a rational integer becomes smaller and smaller. We must therefore finally come to a basis  $\omega_1, \omega_2, \dots, \omega_n$  which consists of algebraic integers and is such that the linear form  $x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n$  no longer represents an algebraic integer for a system of fractional values of the  $x$ 's. This special basis is called the *basis of all algebraic integers of the realm  $\Omega$* . It has the following three properties: (1) The quantities  $\omega_1, \omega_2, \dots, \omega_n$  are all algebraic integers. (2) Its discriminant  $\neq 0$ . (3) If in  $x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n$  all possible systems of integral rational values are written for the  $x$ 's, we have all the algebraic integers of  $\Omega$  (and only these).

This last property which is the fundamental characteristic of the basis of all algebraic integers of  $\Omega$  may also be formulated as follows: *The basis of all algebraic integers of  $\Omega$  consisting of  $\omega_1, \omega_2, \dots, \omega_n$  is such that an algebraic integer of  $\Omega$  which is expressed through this basis in the form  $x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n$  is only divisible by a rational integer  $k$  when the integral rational coordinates (Art. 62),  $x_1, x_2, \dots, x_n$  are all divisible by  $k$ .*

ART. 94. Let  $\omega_1, \omega_2, \dots, \omega_n$  be a basis of all the integers of  $\Omega$  and let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be an arbitrary basis of  $\Omega$ . We have

$$\alpha_\nu = a_{\nu 1}\omega_1 + a_{\nu 2}\omega_2 + \dots + a_{\nu n}\omega_n \quad (\nu = 1, 2, \dots, n),$$

where  $a_{\nu 1}, a_{\nu 2}, \dots, a_{\nu n}$  are rational numbers. We again suppose that all the quantities of  $\Omega$  are expressed through  $\vartheta$ , where  $\vartheta$  is defined as in the preceding article. When for  $\vartheta$  we write its conjugate values, we obtain the  $n$  equations

$$\alpha_\nu^{(k)} = a_{\nu 1}\omega_1^{(k)} + a_{\nu 2}\omega_2^{(k)} + \dots + a_{\nu n}\omega_n^{(k)} \quad (\nu, k = 1, 2, \dots, n).$$

From these relations we have, due to the theorem for the multiplication of determinants,

$$|\alpha_\nu^{(k)}| = |a_{\nu, k}| \cdot |\omega_\nu^{(k)}|,$$

and consequently if  $A = |a_{\nu, k}|$ ,

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = A^2 \Delta(\omega_1, \omega_2, \dots, \omega_n).$$

It follows from this last expression that all discriminants of  $\Omega$  must have the same sign. If as we have supposed, the  $\alpha$ 's are linearly independent, then  $A$  must be different from zero (Art. 55); if however, the  $\alpha$ 's were linearly dependent, then  $A$  must be zero.

If further the  $\alpha$ 's are all algebraic integers, then the quantities  $a_{\nu, k}$  are all rational integers, as is therefore also  $A$ .

If the  $\alpha$ 's, like the  $\omega$ 's, form a basis of all algebraic

integers of  $\Omega$ , then is

$$\Delta(\omega_1, \omega_2, \dots, \omega_n) = A'^2 \Delta(\alpha_1, \alpha_2, \dots, \alpha_n).$$

It follows that  $A^2 A'^2 = 1$  or  $A^2 = A'^2 = 1$ , and consequently

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \Delta(\omega_1, \omega_2, \dots, \omega_n).$$

Thus we see that the discriminants of the different bases of all algebraic integers of  $\Omega$  are equal. We note then that the discriminant of the basis of all integers of  $\Omega$  is independent of what basis of all the integers of  $\Omega$  has been chosen. It is the most important invariant of the realm  $\Omega$ . We may call it the *basal invariant* (*Grundzahl*) of  $\Omega$ . It was denoted by  $D$  or  $\Delta(\Omega)$  by Dedekind (see p. 538 of the Dirichlet *Zahlentheorie*, Fourth Edition).

There are, of course, an infinite number of systems of  $n$  algebraic integers of  $\Omega$  whose discriminant  $= D$ , and these systems of  $n$  integers form bases of all integers of  $\Omega$ . The basal invariant  $D$  is in absolute value a minimum among all the discriminants (different from zero) of any  $n$  integers of  $\Omega$ . The basis  $\omega_1, \omega_2, \dots, \omega_n$  is sometimes called a *minimal* basis of  $\Omega$ . We have the discriminant of all other bases of  $\Omega$  consisting of  $n$  algebraic integers if  $D$  is multiplied by certain positive integers  $A^2$  which are different from zero.

If  $\alpha_1, \alpha_2, \dots, \alpha_n$  is an arbitrary basis of  $\Omega$  and if  $K = \pm |a_{\nu k}|$ , then is

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = K^2 \Delta(\omega_1, \omega_2, \dots, \omega_n).$$

The number  $K$  is called the *index* of the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$ . It follows that the discriminant of a basis is equal to the product of the square of its index by  $D$ . If the index of  $n$  algebraic integers,  $\alpha_1, \alpha_2, \dots, \alpha_n$  is equal to 1 and consequently also  $|a_{\nu k}| = \pm 1$ , these integers form a basis of all integers of  $\Omega$ . For if we solve the  $n$  equations

$$\alpha_\nu = a_{\nu 1} \omega_1 + a_{\nu 2} \omega_2 + \dots + a_{\nu n} \omega_n \quad (\nu = 1, 2, \dots, n),$$

with respect to  $\omega_1, \omega_2, \dots, \omega_n$ , then, since  $|a_{\nu k}| = \pm 1$ , it

follows that each of the  $\omega$ 's is a linear function of the  $\alpha$ 's with rational integral coefficients. Hence if all the integers of  $\Omega$  can be expressed linearly in terms of the  $\omega$ 's with rational integral coefficients, they can also be expressed linearly in terms of the  $\alpha$ 's with rational integral coefficients.

If as a special case, a basis consists of  $1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}$ , where  $\vartheta$  satisfies an irreducible equation of the  $n$ th degree,  $f(t) = 0$ , say, then is

$$\Delta(1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \cdot Nf'(\vartheta) = K^2D$$

with respect to the realm  $\Omega = \Re(\vartheta)$ . Here  $\Delta(1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1})$  is called the *discriminant* of the number  $\vartheta$  [and written  $\Delta(\vartheta)$ ], or the *discriminant* of the equation  $f(t) = 0$ , while  $K$  is called the *index* of the number  $\vartheta$  or the index of the equation  $f(t) = 0$ .

ART. 95. THEOREM. *If  $\alpha_1, \alpha_2, \dots, \alpha_n$  are  $n$  algebraic integers and if  $\frac{c_1\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n}{c}$  is also an algebraic integer, where  $c, c_1, c_2, \dots, c_n$  are rational integers without a common divisor, then is the index of the discriminant of the  $\alpha$ 's divisible by  $c$ .*

We have  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = K^2D$ , where  $K$  is a rational integer, since by hypothesis the  $\alpha$ 's are integral and  $K = \pm |a_{\nu k}|$ , and the quantities  $a_{\nu k}$  are rational integers defined through the  $n$  equations

$$\alpha_\nu = a_{\nu 1}\omega_1 + a_{\nu 2}\omega_2 + \dots + a_{\nu n}\omega_n \quad (\nu = 1, 2, \dots, n).$$

It follows that

$$\sum_{\nu=1}^{\nu=n} (c_\nu \alpha_\nu) = \sum_{\nu=1}^{\nu=n} (c_1 a_{\nu 1} + c_2 a_{\nu 2} + \dots + c_n a_{\nu n}) \omega_\nu.$$

If the left hand side of this expression is divisible by  $c$ , then since the coefficients of the linear form  $x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n$  must all be divisible by  $c$  (see end of Art. 93),

each of the  $n$  expressions  $c_1a_{\nu 1} + c_2a_{\nu 2} + \dots + c_na_{\nu n}$  must be divisible by  $c$ . If in the determinant  $|a_{\nu, k}|$  we denote the first minor of any element  $a_{\nu, k}$  by  $A_{\nu, k}$ , it is seen that the expression

$$(1) \quad \sum_{\nu=1}^{\nu=n} \{(c_1a_{\nu 1} + c_2a_{\nu 2} + \dots + c_na_{\nu n})A_{\nu k}\}$$

is divisible by  $c$ . But this expression is

$$c_1 \sum_{\nu=1}^{\nu=n} a_{\nu 1} A_{\nu k} + c_2 \sum_{\nu=1}^{\nu=n} a_{\nu 2} A_{\nu k} + \dots + c_n \sum_{\nu=1}^{\nu=n} a_{\nu n} A_{\nu k}.$$

Each of these summations is zero except  $c_k \sum_{\nu=1}^{\nu=n} a_{\nu k} A_{\nu k}$  which is equal to  $c_k A$ , where  $A = K$ . Since  $k$  may take the values  $1, 2, \dots, n$ , it is seen that the quantities  $c_1 A, c_2 A, \dots, c_n A$  and also  $cA$  are divisible by  $c$ .

But since the integers  $c_1, c_2, \dots, c_n, c$  have no common divisor, we may always determine  $n+1$  integers  $k_1, k_2, \dots, k_n, k$ , such that

$$k_1 c_1 + k_2 c_2 + \dots + k_n c_n + kc = 1.$$

It follows also that

$$c_1 A k_1 + c_2 A k_2 + \dots + c_n A k_n + c A k = A,$$

and as  $c_1 A, c_2 A, \dots, c_n A, cA$  are all divisible by  $c$ , it follows also that  $A$  is divisible by  $c$ . This proves the theorem since  $A = K$ .

ART. 96. Hilbert, *Bericht*, § 3, calls the product

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'') \dots (\alpha - \alpha^{(n-1)})$$

the *different* of the number  $\alpha$ .

Writing

$$f(x) = (x - \alpha)(x - \alpha') \dots (x - \alpha^{(n-1)}),$$

it is seen that

$$\delta(\alpha) = \left[ \frac{df(x)}{dx} \right]_{x=\alpha}.$$



And it is further seen that

$$N[\delta(\alpha)] = \prod_{i=1}^{i=n} \left[ \frac{df(x)}{dx} \right]_{x=\alpha_i} = (-1)^{\frac{n(n-1)}{2}} \Delta(\alpha).$$

Observe that if  $\alpha$  is an algebraic integer, its norm and discriminant are *rational* integers, while  $\delta(\alpha)$  is an algebraic integer. Observe further that if  $\vartheta$  is a number that determines the realm  $\mathfrak{R}(\vartheta)$ , then  $\delta(\vartheta)$  and  $\Delta(\vartheta)$  are both different from zero, and inversely (Arts. 61 and 63).

Another proof<sup>1</sup> that in a realm of the  $n$ th degree there are always  $n$  algebraic integers  $\omega_1, \omega_2, \dots, \omega_n$ , such that every other integer  $\omega$  of the realm may be expressed in the form

$$\omega = x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n,$$

where the  $x$ 's are rational integers is as follows:

*Proof.* Let  $\alpha$  be an algebraic integer which determines the realm so that  $\Omega = \mathfrak{R}(\alpha)$ . Then every number  $\omega$  of the realm may be expressed in the form (Art. 54)

$$\omega = r_1 + r_2\alpha + \dots + r_n\alpha^{n-1},$$

where the  $r$ 's are rational numbers, and the conjugate values are

$$\omega' = r_1 + r_2\alpha' + \dots + r_n\alpha'^{n-1},$$

$$\dots\dots\dots$$

$$\omega^{(n-1)} = r_1 + r_2\alpha^{(n-1)} + \dots + r_n(\alpha^{(n-1)})^{n-1}.$$

Solving these equations in determinant form, it is seen that

$$\begin{aligned} r_i &= \frac{|1, \alpha, \dots, \omega, \dots, \alpha^{n-1}|}{|1, \alpha, \dots, \alpha^{i-1}, \dots, \alpha^{n-1}|} \\ &= \frac{|1, \alpha, \dots, \omega, \dots, \alpha^{n-1}| |1, \alpha, \dots, \alpha^{i-1}, \dots, \alpha^{n-1}|}{|1, \alpha, \dots, \alpha^{n-1}|^2} \\ &= \frac{A_i}{d} \qquad (i=1, 2, \dots, n), \end{aligned}$$

<sup>1</sup> The kernel of this proof is found in Lagrange, "Réflexions sur la résolution algébrique des équations," *Oeuvres*, III, § 100. See also Kronecker, *Crelle*, Vol. 91, p. 307; Jordan, *Traité des substitutions*, p. 262; Netto, *Substitutionentheorie*, Chapter V; Hilbert, *Bericht*, § 3.

where  $d = \Delta(\alpha)$  is a rational integer and  $A_i$  being clearly integral (and  $= dr_i$ ), is rationally integral.

It is thus seen that every integer of the realm may be put in the form

$$\omega = \frac{A_1 + A_2\alpha + \dots + A_n\alpha^{n-1}}{d},$$

where  $d = \Delta(\alpha)$  is the discriminant of  $\alpha$  and where the  $A$ 's are rational integers.

Suppose that all the integers of the realm are collected in the  $n$  groups  $G_1, G_2, \dots, G_n$ . In the first group  $G_1$  let

all the integers of the form  $\omega_{1i} = \frac{C_{1i}^{(1)}}{d}$  be collected, where

$i = 1, 2, \dots$ . As all rational integers appear in the realm, it is seen that  $C_{1i} = id$ ,  $i = 1, 2, \dots$ ; and we may accordingly write as the first basal element  $\omega_1 = 1$ .

In the second group  $G_2$ , write all integers of the realm of the form

$$\omega_{2i} = \frac{C_{1i}^{(2)} + C_{2i}^{(2)}\alpha}{d} \quad (i = 1, 2, \dots).$$

Let the greatest common divisor of the integers  $C_{2i}^{(2)}$  ( $i = 1, 2, \dots$ ) be  $C_2^{(2)}$ . We may accordingly write

$$\sum_i c_{2i}^{(2)} C_{2i}^{(2)} = C_2^{(2)},$$

where  $c_{2i}^{(2)}$  are rational integers.

Since  $\sum c_{2i}^{(2)} \omega_{2i}$  are integers of the realm, it is seen that as a second basal element we may take

$$\omega_2 = \frac{C_1^{(2)} + C_2^{(2)}\alpha}{d},$$

which is an integer of the realm and  $C_1^{(2)}$  is reduced (mod.  $d$ ).

In the group  $G_3$  put all integers of the form

$$\omega_{3i} = \frac{C_{1i}^{(3)} + C_{2i}^{(3)}\alpha + C_{3i}^{(3)}\alpha^2}{d} \quad (i = 1, 2, 3, \dots).$$

Let  $C_3^{(3)}$  be the greatest common divisor of  $C_{3i}^{(3)}$  ( $i=1, 2, \dots$ ). Since integers  $c_{3i}^{(i)}$  may be determined such that  $\sum c_{3i}^{(3)} C_{3i}^{(3)} = C_3^{(3)}$  and since  $\sum_4 c_{3i}^{(3)} \omega_{3i}$  is an integer of the realm, we may take as a third basal element

$$\omega_3 = \frac{C_1^{(3)} + C_2^{(3)}\alpha + C_3^{(3)}\alpha^2}{d},$$

where  $C_2^{(3)} < C_2^{(2)}$ , use having been made of  $\omega_2$ , and where  $C_1^{(3)}$  is reduced, mod.  $d$ .

Continuing this process, we form the basal elements

$$\omega_k = \frac{C_1^{(k)} + C_2^{(k)}\alpha + \dots + C_{k-1}^{(k)}\alpha^{k-2} + C_k^{(k)}\alpha^{k-1}}{d},$$

where  $C_k^{(k)}$  is the greatest common divisor of all the integers  $C_i^{(k)}$  ( $i=1, 2, \dots$ ), and where

$$C_{k-1}^{(k)} < C_{k-1}^{(k-1)}, \quad C_{k-2}^{(k)} < C_{k-2}^{(k-2)}, \quad \dots, \quad (k=1, 2, \dots, n).$$

The integers  $\omega_1, \omega_2, \dots, \omega_n$  are the basal elements required in the theorem. For, if  $\omega$  is any integer of the realm, it may be written in the form indicated above. Observe that  $A_n$  is divisible by  $C_n^{(n)}$ , so that, say  $A_n = q_n C_n^{(n)}$ .

It follows that

$$\omega - q_n \omega_n = \frac{A_1^{(1)} + A_2^{(1)}\alpha + \dots + A_{n-1}^{(1)}\alpha^{n-2}}{d},$$

where  $A_{n-1}^{(1)}$  is an integer divisible by  $C_{n-1}^{(n-1)}$  and where  $A_1^{(1)}, A_2^{(1)}, \dots, A_{n-2}^{(1)}$  are rational integers. Writing  $A_{n-1}^{(1)} = q_{n-1} C_{n-1}^{(n-1)}$ , it is seen that

$$\omega - q_n \omega_n - q_{n-1} \omega_{n-1} = \frac{A_1^{(2)} + A_2^{(2)}\alpha + \dots + A_{n-2}^{(2)}\alpha^{n-3}}{d},$$

where  $A_1^{(2)}, A_2^{(2)}, \dots, A_{n-3}^{(2)}$  are rational integers and  $A_{n-2}^{(2)}$  is divisible by  $C_{n-2}^{(n-2)}$ . Proceeding in this manner it is seen that

$$\omega - q_n \omega_n - q_{n-1} \omega_{n-1} - \dots - q_2 \omega_2 - q_1 \omega_1 = 0,$$

as asserted in the theorem.

## QUADRATIC REALMS

ART. 97. Before going farther into the general theory, it may be well to apply certain of the principles already developed to some of the simpler realms, in particular to the quadratic and cubic realms. If  $\Omega$  is a quadratic realm, there exists in it a quantity  $\vartheta$  which satisfies an irreducible quadratic equation of the form

$$(1) \quad a\vartheta^2 + b\vartheta + c = 0,$$

$a, b, c$ , being rational integers without a common divisor. It follows that

$$\vartheta = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In this expression write  $b^2 - 4ac = k^2d$ , where the integer  $d$  does not contain any square factor. We then have

$$\vartheta = \frac{-b + k\sqrt{d}}{2a},$$

or

$$\sqrt{d} = \frac{2a\vartheta + b}{k}.$$

The quantity  $d$  is different from 0 or 1, otherwise the equation would be reducible. Note that the realms  $\Re(\sqrt{d})$  and  $\Omega = \Re(\vartheta)$  are equivalent. It may be observed also that every quantity of the realm has the form  $b_0 + b_1\vartheta$  (Art. 44). It is seen that 1 and  $\sqrt{d}$  are two numbers of the realm  $\Omega$  and are linearly independent. For if they were linearly dependent it would follow that

$$x_1 + x_2\sqrt{d} = 0,$$

where  $x_1$  and  $x_2$  are rational numbers. But this relation can exist only when  $x_1 = 0 = x_2$ . It follows also that 1 and  $\sqrt{d}$  form a basis of  $\Omega$  and that all numbers of this realm may be expressed through  $x_1 + x_2\sqrt{d}$  where  $x_1$  and  $x_2$  are rational numbers.

We further have

$$\left| \begin{array}{cc} 1, & 1 \\ \sqrt{d}, & -\sqrt{d} \end{array} \right| = -2\sqrt{d},$$

or

$$\Delta(1, \sqrt{d}) = 4d.$$

It must be determined next whether 1 and  $\sqrt{d}$  form a basis of all the integers of  $\Omega$ . Write

$$\Delta(1, \sqrt{d}) = 4d = DK^2,$$

where  $D$  is the basal invariant of  $\Omega$  and  $K$  the index of the basis 1,  $\sqrt{d}$ . Since  $d$  contains no square factor and  $K$  is a positive rational integer, it follows that  $K=1$  or  $=2$ .

In the *first case* where  $K=1$ ,  $D=4d$ , the form  $x_1+x_2\sqrt{d}$  represents for integral rational values of  $x_1$  and  $x_2$  all the algebraic integers of  $\Omega$ , and 1,  $\sqrt{d}$  form a basis of all the algebraic integers of this realm.

In the *second case* where  $K=2$ , there must be algebraic integers in  $\Omega$  which are expressed through the form  $x_1+x_2\sqrt{d}$  where  $x_1$  and  $x_2$  are rational (fractional) numbers. Let such an integer be  $\frac{x+y\sqrt{d}}{z}$ , where  $x, y, z$  are rational integers without a common divisor. Since (Art. 95)  $K$  is divisible by  $z$ , it follows here that  $z=2$ . Further write

$$x = 2t' + t \quad \text{and} \quad y = 2u' + u,$$

where  $t$  and  $u$  are either  $=0$  or  $=1$ . It results that

$$\frac{x+y\sqrt{d}}{z} = \frac{x+y\sqrt{d}}{2} = t' + u'\sqrt{d} + \frac{t+u\sqrt{d}}{2}.$$

Since  $\frac{x+y\sqrt{d}}{2}$  must be an algebraic integer, and as  $t'+u'\sqrt{d}$  is integral, it follows that  $\frac{t+u\sqrt{d}}{2}$  must be an algebraic integer.



ART. 98. As the case  $t=0=u$  must be excluded, since then  $x, y, z$  would have the greatest common divisor 2, the three following cases arise:

$$(1) t=1, u=0; \quad (2) t=0, u=1; \quad (3) t=1, u=1.$$

In the *first* case  $\frac{t+u\sqrt{d}}{2} = \frac{1}{2}$  and in the *second* case  $= \frac{\sqrt{d}}{2}$ .

Neither of these numbers being an algebraic integer, we have left only the *third* case. Hence when  $K=2$ ,  $\frac{1+\sqrt{d}}{2} = \eta$ , say, is an algebraic integer; and if  $\frac{1+\sqrt{d}}{2}$  is an algebraic integer, then inversely  $K$  must  $=2$ ; for if  $K=1$ , there would be no algebraic integer with fractional coördinates. The irreducible equation which  $\eta$  satisfies is

$$(2\eta - 1)^2 = d \quad \text{or} \quad \eta^2 - \eta - \frac{d-1}{4} = 0.$$

Hence if  $K$  is equal to 2, then  $\frac{d-1}{4}$  must be a rational integer and consequently  $d \equiv 1 \pmod{4}$ . Inversely if  $d \equiv 1 \pmod{4}$ , then  $K=2$  and  $\eta$  is an algebraic integer. Notice that

$$\Delta\left(1, \frac{1+\sqrt{d}}{2}\right) = \left| \frac{1}{1+\sqrt{d}}, \frac{1}{1-\sqrt{d}} \right|^2 = d.$$

*Summary.* Since  $d$  does not contain a square factor,  $d \not\equiv 0 \pmod{4}$ . If  $d \equiv 2$  or  $\equiv 3 \pmod{4}$  then is  $K=1$ , and  $D=4d$ . Hence when  $K=1$ ,  $\frac{D}{4} = d \equiv 2$  or  $3 \pmod{4}$ , and consequently  $D \equiv 8$  or  $12 \pmod{16}$ . From this we see that *not every arbitrary integer can be the basal invariant of a quadratic realm*. An odd integer can have this property only when it is  $\equiv 1 \pmod{4}$  and an even integer only when it  $\equiv 8$  or  $12 \pmod{16}$ . Further note, since  $D=4d$ , that an odd integer can occur only to the first

power as a factor of  $D$  since by hypothesis  $d$  is divisible by no integer squared; while 2 can occur only to the second or third power as a factor of  $D$ . Similarly in the case of realms of higher degree, every integer can not be a basal invariant.

It is thus seen that when  $K=1$ , then  $1, \sqrt{d}$  form a basis of all the algebraic integers of  $\Omega$  and when  $K=2$ , then  $1, \frac{1+\sqrt{d}}{2}$  form such a basis. In the first case the algebraic integers of  $\Omega$  may be expressed in the form  $x_1+x_2\sqrt{d}$ , that is in the form  $x_1+\frac{x_2\sqrt{D}}{2}$ , where  $x_1$  and  $x_2$  are rational integers. While in the second case all integers of  $\Omega$  are expressible in the form  $x+y\frac{1+\sqrt{d}}{2}$  where  $x$  and  $y$  are rational integers.

It is evident that in general all the integers of  $\Omega$  may be expressed in the form  $\frac{t+u\sqrt{D}}{2}$  where  $t$  and  $u$  are rational integers which must however satisfy the condition  $t^2 \equiv Du^2 \pmod{4}$ . For if  $\frac{t+u\sqrt{D}}{2}$  is an algebraic integer, it is necessary and sufficient that the coefficients of the irreducible equation which it satisfies, be rational integers, with unity as the coefficient of the first term; that is, the coefficients of

$$\left(x - \frac{t+u\sqrt{D}}{2}\right)\left(x - \frac{t-u\sqrt{D}}{2}\right) = x^2 - tx + \frac{t^2 - Du^2}{4} = 0$$

must be rational integers. Hence  $\frac{t^2 - Du^2}{4}$  must be a rational integer, or  $t^2 \equiv Du^2 \pmod{4}$ .

**ART. 99. The Units of a Quadratic Realm.** It is clear (Art. 90) that an integer  $\frac{t+u\sqrt{D}}{2}$  as defined above can

only be an algebraic unit when its norm =  $\pm 1$ . It follows that

$$N\left(\frac{t+u\sqrt{D}}{2}\right) = \frac{t+u\sqrt{D}}{2} \cdot \frac{t-u\sqrt{D}}{2} = \frac{t^2-Du^2}{4} = \pm 1,$$

or

$$t^2 - Du^2 = \pm 4. \quad (\text{i})$$

We note that all the units of  $\Omega$  whose norm =  $-1$ , are had through the multiplication of one of these units by all possible units of  $\Omega$  whose norm is  $+1$ . If we limit the discussion to those units of  $\Omega$  whose norm =  $+1$ , they

must have the form  $\frac{t+u\sqrt{D}}{2}$ , where  $t$  and  $u$  are rational integers that satisfy the equation of Pell <sup>1</sup>

$$t^2 - Du^2 = +4.$$

As is evident, the equation (i) for a *negative*  $D$  which  $\neq -3$  or  $\neq -4$ , has only the two solutions  $t = \pm 2, u = 0$ . We consequently have in this case the two units  $\pm 1$ .

If  $D = -4$ , Pell's equation has the four solutions

$$t = 0, \quad u = \pm 1,$$

$$t = \pm 2, \quad u = 0;$$

and correspondingly we have the four units

$$\pm 1; \quad \pm i,$$

which are had by taking the powers of the *one* unit,  $+i$ .

If  $D = -3$  the six solutions of Pell's equation are

$$u = 0, \quad t = \pm 2;$$

$$t = +1, \quad u = \pm 1;$$

$$t = -1, \quad u = \pm 1;$$

<sup>1</sup> See Dirichlet's *Zahlentheorie*, § 141. For an excellent history of Pell's equation, see Chapt. XII, Vol. II of the *History of the Theory of Numbers* by Prof. L. E. Dickson.

See also "Report" of H. J. S. Smith, *Collected Works*, Vol. I, p. 191, where the theorem is attributed to Lord Brouncker. In the latter connection see Wallis's *Algebra*, Chaps. 98 and 99. The *Canon Pellianus* of Degen Havniae, 1817, contains a table for values of  $D$  less than 1000. See also Cayley, *Crelle*, Vol. 53, p. 369.

and the units are

$$\pm 1; \quad \frac{+1 \pm i\sqrt{3}}{2}; \quad \frac{-1 \pm i\sqrt{3}}{2},$$

which are all had by taking the positive powers of  $\frac{1-i\sqrt{3}}{2}$  (a primitive sixth root of unity).

If  $D$  is positive, Pell's equation <sup>1</sup> has an infinite number of solutions, and then there exist in the quadratic realm  $\Omega$  an infinite number of units (see Art. 91). These, however, may be expressed in the form

$$\frac{t+u\sqrt{D}}{2} = \pm \left( \frac{T+U\sqrt{D}}{2} \right)^n,$$

where  $n$  takes all positive and negative integral values and where  $T, U$  are the least solution of Pell's equation in which  $U \neq 0$ . The quantity  $\frac{T+U\sqrt{D}}{2}$  is called the *fundamental unit*.

#### EXAMPLES

1. Show that  $-4$  is the basal invariant of  $\mathfrak{R}(i)$ , where  $i = \sqrt{-1}$ .
2. Show that  $1+i$  and  $3+2i$  constitute a basis of all integers in  $\mathfrak{R}(i)$ , as do also  $1, i$ .
3. Show that  $1, \frac{-1+i\sqrt{3}}{2}$  are the elements of a minimal basis of  $\mathfrak{R}(\sqrt{-3})$ , the basal invariant being  $-3$ .
4. Show that  $1$  and  $i\sqrt{3}$  do not form a basis of all integers in  $\mathfrak{R}(\sqrt{-3})$ .
5. Show that  $1$  and  $i\sqrt{5}$  form a basis of all integers in  $\mathfrak{R}(\sqrt{-5})$  and that the basal invariant is  $-20$ .
6. Determine algebraic realms whose basal invariants are  $8, 12, -8, 28, 13, -5$ .
7. Show that the fundamental unit of  $\mathfrak{R}(\sqrt{11})$  is  $10+3\sqrt{11}$ , and that of  $\mathfrak{R}(\sqrt{22})$  is  $197+42\sqrt{22}$ .

<sup>1</sup> See Chrystal's *Algebra*, Part II, p. 450; H. J. S. Smith, *Collected Papers*, Vol. I, p. 192.

8. Show that a minimal basis of  $\Re(\sqrt{21})$  is  $1, \frac{1+\sqrt{21}}{2}$  and that the fundamental unit is  $2 + \frac{1+\sqrt{21}}{2}$ .
9. Show that a minimal basis of  $\Re(\sqrt{73})$  is  $1, \frac{1+\sqrt{73}}{2}$ , and that the fundamental unit is  $943 + 250\frac{1+\sqrt{73}}{2}$ .
10. Show that  $4 + \sqrt{17}$  is the fundamental unit in the realm  $\Re(\sqrt{17})$ .

## CUBIC REALMS

ART. 100. LEMMA I. *In a determinant of the  $n$ th order, if the first row consists of the  $n$  integers  $a_{11}, a_{12}, \dots, a_{1n}$  whose greatest common divisor is  $d$ , integral elements of the other rows may be determined so that the determinant  $= d$ .*

If  $a$  and  $b$  are two integers whose greatest common divisor is  $d$ , it is possible to determine two other integers  $x$  and  $y$  such that  $ay - bx = d$ , or

$$\begin{vmatrix} a, & b \\ x, & y \end{vmatrix} = d.$$

The lemma is thus proved for the case  $n=2$ . On the assumption that the theorem to be demonstrated is true for the case  $n-1$ , it may be proved as follows for the case  $n$ .

Let  $d$  be the greatest common divisor of  $a_{11}, a_{12}, \dots, a_{1,n}$  and let  $d'$  be the greatest common divisor of  $a_{11}, a_{12}, \dots, a_{1,n-1}$  so that  $d$  is the greatest common divisor of  $d'$  and  $a_{1,n}$ .

By hypothesis we may so determine the elements  $a_{21}, a_{22}, \dots, a_{2,n-1}; a_{31}, \dots, a_{3,n-1}; \dots; a_{n-1,1}, \dots, a_{n-1,n-1}$ ,



that

$$\begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1,n-1} \\ a_{21}, & a_{22}, & \dots, & a_{2,n-1} \\ \dots & \dots & \dots & \dots \\ a_{n-1,1}, & a_{n-1,2}, & \dots, & a_{n-1,n-1} \end{vmatrix} = d'.$$

If  $x$  and  $y$  are two integers to be determined later, we have

$$\begin{vmatrix} a_{11}, & a_{12}, & \dots, & a_{1,n-1}, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2,n-1}, & 0 \\ a_{31}, & a_{32}, & \dots, & a_{3,n-1}, & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n-1,1}, & a_{n-1,2}, & \dots, & a_{n-1,n-1}, & 0 \\ x \frac{a_{11}}{d'}, & x \frac{a_{12}}{d'}, & \dots, & x \frac{a_{1,n-1}}{d'}, & y \end{vmatrix} = yd' + a_{1,n}(-1)^{n-1} \cdot \frac{x}{d'} \cdot d'(-1)^{n-2}.$$

Hence the determinant is equal to  $yd' - xa_{1,n}$ , where the  $x$  and  $y$  are integers which may be so determined that  $yd' - xa_{1,n} = d$ .

LEMMA II. *In every finite realm  $\Omega$  it is always possible to determine a basis of all integers of  $\Omega$  such that 1 is an element of this basis.*

From a basis of all integers of  $\Omega$  other bases of all integers of  $\Omega$  may be derived as follows:

Let  $\omega_1, \omega_2, \dots, \omega_n$  be a basis of all integers of  $\Omega$ , and further write

$$\alpha_\nu = a_{\nu 1}\omega_1 + a_{\nu 2}\omega_2 + \dots + a_{\nu n}\omega_n \quad (\nu = 1, 2, \dots, n),$$

where  $a_{\nu,k}$  are rational integers. The integers  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis of all integers of  $\Omega$  (Art. 94) if  $|a_{\nu k}| = \pm 1$ . Further the integer 1 may be expressed in the form

$$1 = b_{11}\omega_1 + b_{12}\omega_2 + \dots + b_{1,n}\omega_n,$$

where the greatest common divisor of the  $b$ 's is unity. Hence by the preceding lemma we may so determine

$n-1$  other integers  $\beta_2, \dots, \beta_n$ , say

$$\beta_\mu = b_{\mu 1}\omega_1 + b_{\mu 2}\omega_2 + \dots + b_{\mu n}\omega_n \quad (\mu=2, \dots, n),$$

such that  $|b_{\mu k}|=1$ . It follows that  $1, \beta_2, \beta_3, \dots, \beta_n$  form a basis of all integers of  $\Omega$ .

**LEMMA III.** *If in a finite realm  $\Omega$  there are  $r$  algebraic integers  $\alpha_1, \alpha_2, \dots, \alpha_r$  through which no algebraic integer (including zero) may be expressed with fractional coördinates, then a basis of all the algebraic integers of  $\Omega$  may be determined, which includes these  $r$  integers ( $r \leq n$ ) as elements.*

Since the number zero cannot be expressed through  $\alpha_1, \alpha_2, \dots, \alpha_r$  with fractional coefficients, these  $r$  numbers  $\alpha_1, \alpha_2, \dots, \alpha_r$  must be linearly independent. If  $r=n$ , the theory is proved of itself in accord with the definition of the basis of all the algebraic integers of  $\Omega$ . If, however,  $r < n$ , then there is a number  $\alpha'_{r+1}$  which is independent of  $\alpha_1, \alpha_2, \dots, \alpha_r$ ; if further  $r+1 < n$ , then there is a number  $\alpha'_{r+2}$  in  $\Omega$ , which is independent of  $\alpha_1, \alpha_2, \dots, \alpha_r, \alpha'_{r+1}$ , etc. In this manner  $n$  numbers  $\alpha_1, \alpha_2, \dots, \alpha_r, \alpha'_{r+1}, \alpha'_{r+2}, \dots, \alpha'_n$  are derived, which form a basis of  $\Omega$ , and we may further assume (Art. 93) that  $\alpha'_{r+1}, \dots, \alpha'_n$  are algebraic integers. If these  $n$  integers form a basis of all integers of  $\Omega$ , the theorem is proved. If, however, they do not form such a basis, there is an algebraic integer in  $\Omega$  which has, say, the form

$$\beta = \frac{c_1\alpha_1 + c_2\alpha_2 + \dots + c_r\alpha_r + c_{r+1}\alpha'_{r+1} + \dots + c_n\alpha'_n}{c},$$

where  $c_1, c_2, \dots, c_n, c$  are rational integers which have no common divisor. If  $c = p \cdot q$ , where  $p$  is a prime integer, then is also

$$q\beta = \frac{c_1\alpha_1 + \dots + c_n\alpha'_n}{p}$$

an algebraic integer in  $\Omega$ . Further the integers  $c_{r+1},$

$c_{r+2}, \dots, c_n$  cannot all be divisible by  $p$ ; for in this case there would result

$$q\beta - \frac{c_{r+1}}{p}\alpha'_{r+1} - \frac{c_{r+2}}{p}\alpha'_{r+2} - \dots - \frac{c_n}{p}\alpha'_n = \frac{c_1\alpha_1 + \dots + c_r\alpha_r}{p},$$

which contrary to the hypothesis, is an algebraic integer.

Suppose that  $c_n$ , say, is not divisible by  $p$ ; we may then determine two rational integers  $s$  and  $t$  such that

$$sc_n - tp = 1.$$

Make use of this relation and form a new basis of  $\Omega$  consisting of the integers which are had if we retain  $\alpha_1, \alpha_2, \dots, \alpha'_{n-1}$  and replace  $\alpha'_n$  through another integer as was done in Art. 93. The absolute value of the discriminant of the new basis is smaller than that of the original basis. By repetition of this process, the integers  $\alpha_1, \alpha_2, \dots, \alpha_r$  being retained while  $\alpha'_{r+1}, \dots, \alpha'_n$  are replaced by other integers, we must finally come to a basis of all the integer of  $\Omega$ .

**ART. 101. Basis of All Integers.**<sup>1</sup> Let the cubic realm be defined through the algebraic integer  $\vartheta$ , where  $\vartheta$  is a root of the irreducible equation of the third degree

$$G(t) \equiv t^3 + a_1t^2 + a_2t + a_3 = 0,$$

in which the  $a$ 's are rational integers, and let  $\Omega = \mathfrak{K}(\vartheta)$  be this realm. It is seen (Art. 44) that every algebraic number of  $\Omega$  is of the form  $\alpha = a + b\vartheta + c\vartheta^2$  where  $a, b, c$  are rational numbers in  $\mathbb{R}$ . Denote the conjugate roots of  $\vartheta$  by  $\vartheta'$  and  $\vartheta''$ . If then we write

$$\begin{aligned}\alpha &= a + b\vartheta + c\vartheta^2, \\ \alpha' &= a + b\vartheta' + c\vartheta'^2, \\ \alpha'' &= a + b\vartheta'' + c\vartheta''^2,\end{aligned}$$

<sup>1</sup> See Sommer, *Einführung in die Theorie der algebraischen Zahlkörper*, p. 257; and also Woronoj, *Fortschr. der math. Wissens.*, Vol. 25, 1894.

it is seen that

$$a = \frac{\begin{vmatrix} \alpha & \vartheta & \vartheta^2 \\ \alpha' & \vartheta' & \vartheta'^2 \\ \alpha'' & \vartheta'' & \vartheta''^2 \end{vmatrix}}{\begin{vmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \vartheta' & \vartheta'^2 \\ 1 & \vartheta'' & \vartheta''^2 \end{vmatrix}} = \frac{\begin{vmatrix} \alpha & \vartheta & \vartheta^2 \\ \alpha' & \vartheta' & \vartheta'^2 \\ \alpha'' & \vartheta'' & \vartheta''^2 \end{vmatrix} \cdot \begin{vmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \vartheta' & \vartheta'^2 \\ 1 & \vartheta'' & \vartheta''^2 \end{vmatrix}}{\begin{vmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \vartheta' & \vartheta'^2 \\ 1 & \vartheta'' & \vartheta''^2 \end{vmatrix}^2} = \frac{A}{\Delta(\vartheta)},$$

where the discriminant  $\Delta(\vartheta)$  is a rational integer. There are similar values for the rational numbers  $b = \frac{B}{\Delta(\vartheta)}$ ,  $c = \frac{C}{\Delta(\vartheta)}$ . If  $\alpha = a + b\vartheta + c\vartheta^2$  is an algebraic integer in  $\Omega$ , then is  $A$  a rational integer, as are also  $B$  and  $C$ . It is thus seen that the algebraic integers of  $\Omega$  are expressed in the form (see also Art. 96)

$$\alpha = \frac{A + B\vartheta + C\vartheta^2}{\Delta(\vartheta)},$$

where  $A$ ,  $B$ ,  $C$  and  $\Delta = \Delta(\vartheta)$  are rational integers. Writing

$$\alpha = \frac{A + B\vartheta + C\vartheta^2}{\Delta} = A_1 + B_1\vartheta + C_1\vartheta^2 + \frac{A_2 + B_2\vartheta + C_2\vartheta^2}{\Delta},$$

where  $A_2$ ,  $B_2$ ,  $C_2$  are the residues (mod.  $\Delta$ ), it is seen that there are only a finite number ( $< \Delta$ ) of different integers  $C_2$ . As  $\vartheta^2$  is also an integer in  $\Omega$ , it may be written in the form

$$\vartheta^2 = \frac{0 + 0\vartheta + \Delta\vartheta^2}{\Delta}.$$

If, mod.  $\Delta$ , the system of residues corresponding to  $C_2$  are  $C_2, C_2', C_2'', \dots, \Delta$ , we are able to find a system of integers  $c_2, c_2', c_2'', \dots, c$ , such that

$$c_2C_2 + c_2'C_2' + \dots + c\Delta = d_2,$$

where  $d_2$  is the greatest common divisor of  $C_2, C_2', \dots, \Delta$ . If further the corresponding algebraic integers  $\alpha$  are

multiplied by  $c_2, c'_2, \dots$ , it is seen through the addition of the resulting quantities that there exists an algebraic integer, say  $\omega_3$ , in  $\Omega$ , such that

$$\omega_3 = \frac{a_2 + b_2\vartheta + d_2\vartheta^2}{\Delta},$$

where  $d_2$  is a divisor of  $\Delta$ , besides being a divisor of the coefficient of  $\vartheta^2$  of every algebraic integer in  $\Omega$ , when this integer is expressed in the form of  $\alpha$  above.

If  $C_2 = d_2\bar{C}_2$ , it is evident that  $\alpha - \bar{C}_2\omega_3$  gives rise to an algebraic integer  $\beta$  of the form

$$\beta = \frac{A_3 + B_3\vartheta}{\Delta}.$$

Thus corresponding to every integer of the form  $\alpha$  there is an integer of the form  $\beta$ . By proceeding with the  $\beta$ 's in the same way as was done above with the  $\alpha$ 's, it is possible to derive an algebraic integer

$$\omega_2 = \frac{a_1 + d_1\vartheta}{\Delta},$$

where  $d_1$  is a divisor of  $\Delta$ , and also of the coefficient of  $\vartheta$  of every algebraic integer of  $\Omega$  which has been reduced to the form  $\beta$ . If  $B_3 = d_1\bar{B}_3$ , then

$$\beta - \bar{B}_3\omega_2 = \frac{A_3 - a_1\bar{B}_3}{\Delta}.$$

Since the left hand side of this expression is an algebraic integer in  $\Omega$ , the right hand side must also be an integer in

$\Omega$  and consequently  $\frac{A_3 - a_1\bar{B}_3}{\Delta}$  is a rational integer.

Since 1 is an integer in every algebraic realm  $\Omega$  (see Art. 100), it is evident that the algebraic integers

$$\omega_1 = 1, \quad \omega_2 = \frac{a_1 + d_1\vartheta}{\Delta}, \quad \omega_3 = \frac{a_2 + b_2\vartheta + d_2\vartheta^2}{\Delta},$$



form a basis of all integers in  $\Omega$ ; in fact (see Art. 100), every algebraic integer of  $\Omega$  may be expressed linearly through  $\omega_1, \omega_2, \omega_3$  with rational integral coefficients.

The rational integers  $d_1$  and  $d_2$  are divisors of  $\Delta$ , while the rational integers  $a_1, a_2, b_2$  are reduced, mod.  $\Delta$ . It will be seen below that  $\omega_2$  and  $\omega_3$  admit of further simplification.

In Art. 94, we denoted by  $D$  the discriminant  $\Delta(1, \omega_1, \omega_2)$  which is the basal invariant of  $\Omega$ .

If  $\sigma$  is any algebraic integer in  $\Omega$ , we may always write

$$\begin{aligned} 1 &= a_{11}\omega_1 + a_{12}\omega_2 + a_{13}\omega_3, \\ \sigma &= a_{21}\omega_1 + a_{22}\omega_2 + a_{23}\omega_3, \\ \sigma^2 &= a_{31}\omega_1 + a_{32}\omega_2 + a_{33}\omega_3, \end{aligned}$$

where  $a_{11}, a_{12}, \dots, a_{33}$  are rational integers. If the discriminant

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \pm 1,$$

then (Art. 94),  $1, \sigma, \sigma^2$  form a basis of all integers in  $\Omega$ . If this condition holds true for  $\vartheta$ , the quantity that defines  $\Omega$ , then  $1, \vartheta, \vartheta^2$  is a basis of all integers of  $\Omega$ . Further note that

$$\Delta(\omega_1, \omega_2, \omega_3) = \frac{d_1^2 d_2^2}{\Delta^3},$$

where  $\Delta$  (see above) is  $\Delta(1, \vartheta, \vartheta^2) = \Delta(\vartheta)$ . Again note that  $d_1$  and  $d_2$  are divisors of  $\Delta$  and that  $\frac{d_1^2 d_2^2}{\Delta}$  is a rational integer  $= \Delta(\omega_1, \omega_2, \omega_3) = D$ . The prime numbers that enter to an odd degree as factors of  $\Delta(\vartheta)$  are evidently factors of  $D$ .

**ART. 102. Numerical Computation of the Basis of All Integers.** We may write  $\Delta(\vartheta)$  in the form

$$\Delta(\vartheta) = \pm q_1^{6e_1} q_2^{6e_2} \dots q^{6e} p_1^{f_1} p_2^{f_2} \dots p^f,$$

where the  $q$ 's are prime numbers, the  $e$ 's rational integers, the  $p$ 's prime numbers not necessarily different from the  $q$ 's and the  $f$ 's are any of the integers 1, 2, 3, 4, 5.

Note that

$$\Delta(\omega_2) = \Delta(1, \omega_2, \omega_2^2) = \Delta\left[1, \frac{a_1 + d_1\vartheta}{\Delta(\vartheta)}, \left(\frac{a_1 + d_1\vartheta}{\Delta(\vartheta)}\right)^2\right] = \frac{d_1^6}{\Delta(\vartheta)^5},$$

which is a rational integer. Further  $d_1$  is a divisor of  $\Delta(\vartheta)$ . Hence  $d_1$  must be of the form

$$d_1 = kq_1^{5e_1}q_2^{5e_2}\cdots q^{5e}p_1^{f_1}p_2^{f_2}\cdots p^f, \\ k = \pm q_1^{\lambda_1}q_2^{\lambda_2}\cdots q^{\lambda_e},$$

where the  $\lambda$ 's have the values either 0 or 1; or

$$d_1 = kk_1,$$

if

$$k_1 = q_1^{5e_1}q_2^{5e_2}\cdots q^{5e}p_1^{f_1}p_2^{f_2}\cdots p^f.$$

It is seen that  $\omega_2$  may be written

$$\omega_2 = \frac{a_1 + d_1\vartheta}{\Delta(\vartheta)} = \frac{a_1 + kq_1^{5e_1}q_2^{5e_2}\cdots q^{5e}p_1^{f_1}p_2^{f_2}\cdots p^f\vartheta}{\Delta(\vartheta)},$$

so that

$$\omega_2 q_1^{e_1} q_2^{e_2} \cdots q^e = \frac{a_1 q_1^{e_1} q_2^{e_2} \cdots q^e}{\Delta(\vartheta)} + k\vartheta,$$

or

$$\omega_2 q_1^{e_1} q_2^{e_2} \cdots q^e - k\vartheta = \frac{a_1}{k_1} = b_1.$$

Note that  $b_1$  is an integer, since the left hand side of the expression is integral. Further note that the left hand side of the expression is divisible by the rational integer  $k$ , and consequently also  $b_1$  is divisible by  $k$ .

It follows that we may write  $\omega_2$  in the form

$$\omega_2 = \frac{b_1 + k\vartheta}{q_1^{e_1} q_2^{e_2} \cdots q^e},$$

where  $b_1$  as well as  $q_1^{e_1} q_2^{e_2} \cdots q^e$  is divisible by  $k$ . We may further write

$$\omega_2 = \frac{b + \vartheta}{d},$$

where the rational integer  $b$  is as yet undetermined and

$$d = q_1^{r_1} q_2^{r_2} \cdots q^r,$$

where

$$r_1 \leq e_1, \quad r_2 \leq e_2, \quad \cdots, \quad r \leq e.$$

It follows that  $d$  must occur at least to the sixth power in  $\Delta(\vartheta)$ . If then  $\Delta(\vartheta)$  does *not* contain any prime factors to at least the sixth power, then is  $d = 1$ .

Write  $\Delta(\vartheta)$  in the form  $d^2\delta$  where  $\delta$  contains  $d$  to at least the fourth power. We then have

$$\omega_3 = \frac{a_3 + b_3\vartheta + d_3\vartheta^2}{d^2\delta}$$

and

$$\omega_2^2 = \frac{b^2 + 2b\vartheta + \vartheta^2}{d^2}.$$

Note that  $d_2$  is a divisor of  $d^2\delta$  and that  $d$  occurs to the sixth power in  $\Delta(\vartheta)$ . It is evident that any factor common to  $d_2$  and  $d$  is also common to  $\delta$ . Hence if  $d_2$  is not already a divisor of  $\delta$ , it is always possible to *determine* rational integers  $x, y$  such that

$$xd_2 + y\delta = \delta_2,$$

where  $\delta_2$  is the greatest common divisor of  $\delta$  and  $d_2$ .

Writing  $\delta = \delta_1\delta_2$ , it is seen that

$$\bar{\omega}_3 = x\omega_3 + y\omega_2^2 = \frac{a_3 + b_3\vartheta + \delta_2\vartheta^2}{d^2\delta_1\delta_2}.$$

If we refer to the manner in which  $\omega_3$  was derived as an element of the basis, it is clear that  $\bar{\omega}_3$  may be substituted in its place; for  $x\omega_3 + y\omega_2^2$  is clearly one of the algebraic integers of  $\Omega$ . Noting that  $\omega_2^2$  is an integer in  $\Omega$ , it may be written in the form

$$\omega_2^2 = u + v\omega_2 + w\bar{\omega}_3, \quad (i)$$

where  $u, v, w$  are rational integers. Expressing both sides of this formula as an identity in  $\vartheta$ , we note, by equating the coefficients of like powers of  $\vartheta$ , that

$$w = \delta_1,$$

while  $a_3$  and  $b_3$  are both divisible by  $\delta_2$ . We may therefore write as the third basal element

$$\omega_3 = \frac{c + c_1\vartheta + \vartheta^2}{d^2\delta_1},$$

where  $c$  and  $c_1 (= 2b - vd)$  are rational integers. Since  $\omega_2$  is an algebraic integer in  $\Omega$ , it satisfies the equation

$$\left(t - \frac{b + \vartheta}{d}\right) \left(t - \frac{b + \vartheta'}{d}\right) \left(t - \frac{b + \vartheta''}{d}\right) = 0,$$

or, observing the equation which defines  $\vartheta$ ,

$$t^3 - \frac{3b - a_1}{d}t^2 + \frac{3b^2 - 2a_1b + a_2}{d^2}t - \frac{b^3 - a_1b^2 + a_2b - a_3}{d^3} = 0.$$

As each of the coefficients must be integral, it is seen that  $b$  must satisfy the three congruences

$$\left. \begin{aligned} 3b - a_1 &\equiv 0 \pmod{d} \\ 3b^2 - 2a_1b + a_2 &\equiv 0 \pmod{d^2} \\ b^3 - a_1b^2 + a_2b - a_3 &\equiv 0 \pmod{d^3} \end{aligned} \right\} \quad (\text{ii})$$

Write the first of these congruences in the form

$$3b - a_1 = gd$$

( $g$  an integer) and the second

$$3b^2 - 2a_1b + a_2 = g_1d^2.$$

We have

$$a_1b - a_2 = d(g_1d - bg),$$

and therefore

$$a_1b - a_2 \equiv 0 \pmod{d}.$$

From the third congruence in (ii) it follows that

$$b^3 - a_3 \equiv 0 \pmod{d}.$$

Due to the first of the congruences (ii) we may write  $\omega_2$  in any of the following forms:

$$\omega_2 = \frac{b + \vartheta}{d}; \quad \frac{a_1 - 2b + \vartheta}{d}; \quad \frac{a_1 - 2b + vd + \vartheta}{d} = \frac{a_1 - c_1 + \vartheta}{d},$$

where  $c_1 = 2b - vd$ .

Note that  $\frac{3b - a_1}{d}$  is an integer and write formula (i) in

the form

$$\omega_2^2 - \frac{3b - a_1}{d}v - k = \omega_1 + v\omega_2 + \delta_1\omega_3,$$

where  $k$  is an arbitrary integer; and that is,

$$\left(\frac{a_1 - c_1 + \vartheta}{d}\right)^2 - \frac{3b - a_1}{d}v - k = \omega_1 + v\frac{a_1 - c_1 + \vartheta}{d} + \delta_1\frac{c + c_1\vartheta + \vartheta^2}{d^2\delta_1}. \quad (\text{iii})$$

By equating the coefficients of  $\vartheta$  in this expression, it is seen that

$$2a_1 - 3c_1 = vd$$

or

$$2a_1 - 6b + 3vd = vd.$$

Hence  $b$  must satisfy integrally the equation

$$3b - a_1 = vd.$$

By equating the constant terms in (iii), it is seen that

$$c_1^2 - a_1c_1 + a_1^2 - a_1c_1 - (3b - c_1)dv = d^2(\omega_1 + k) + c.$$

If the second of the congruences (ii) is written in the form

$$a_2 + 3b^2 - 2a_1b = d^2g_1,$$

where  $g_1$  is an integer, and if to  $c_1$  is given its value

$$c_1 = 2b - vd$$

and if we note that

$$3b - a_1 = vd, \quad a_1 - c_1 = b,$$

it is clear that

$$c_1^2 - a_1c_1 + a_2 = d^2(v^2 + g_1 + \omega_1 + k) + c.$$

The integer  $k$  may be so determined that the coefficient of  $d^2$  vanishes leaving

$$c = c_1^2 - a_1c_1 + a_2.$$

If then  $A$  is written for  $c_1$ , the three basal elements may be written

$$\omega_1 = 1, \quad \omega_2 = \frac{-A + a_1 + \vartheta}{d}, \quad \omega_3 = \frac{A^2 - a_1A + a_2 + A\vartheta + \vartheta^2}{d^2\delta_1},$$



where  $a_1, a_2, a_3$  are the integral coefficients of the equation

$$G(t) \equiv t^3 + a_1 t^2 + a_2 t + a_3 = 0,$$

of which  $\theta$  is a root; while the integers  $A, d$ , must further satisfy the congruences (ii), namely

$$3(A - a_1) + a_1 \equiv 0 \pmod{d}$$

$$3(A - a_1)^2 + 2a_1(A - a_1) + a_2 \equiv 0 \pmod{d^2}$$

$$(A - a_1)^3 + a_1(A - a_1)^2 + a_2(A - a_1) + a_3 \equiv 0 \pmod{d^3}.$$

Note that  $\delta_1$  is further restricted in that the right hand side of the following expressions must be integral, namely:

$$\omega_3 \omega'_3 + \omega_3 \omega''_3 + \omega'_3 \omega''_3 = \frac{[3(A - a_1) + a_1]G(s)}{d^4 \delta_1^2},$$

where  $s = A - a_1$ , and that

$$\omega_2 \omega_3 = \frac{-G(s)}{d^3 \delta_1},$$

where  $s = A - a_1$ . And finally observe that  $d^6$  and  $\delta_1^2$  are divisors of  $\Delta(\theta)$ .

ART. 103. If  $\Omega$  is a cubic realm, the basis of the system of all algebraic integers of  $\Omega$  consists of 3 algebraic integers of  $\Omega$ , of which one may be taken = 1. Suppose that

$$1, \alpha, \beta$$

constitute a basis of all the integers of  $\Omega$ , so that consequently all such integers may be expressed in the form  $x + y\alpha + z\beta$ , where  $x, y, z$  are rational integers. Further since  $\alpha\beta$  is an algebraic integer of  $\Omega$ , it may be expressed in the form

$$\alpha\beta = a\beta + b\alpha + c_1,$$

where  $a, b$  and  $c$ , are rational integers. It follows that

$$(\alpha - a)(\beta - b) = ab + c_1 = c,$$

say. Write

$$\alpha - a = \alpha_1, \quad \beta - b = \beta_1.$$

It may be proved that  $1, \alpha_1, \beta_1$  also form a basis of all

algebraic integers of  $\Omega$ ; for  $1, \alpha, \beta$  may be linearly expressed through  $1, \alpha_1, \beta_1$  with rational integral coefficients, and inversely  $1, \alpha_1, \beta_1$  may be linearly expressed through  $1, \alpha, \beta$  with rational integral exponents in the form:

$$\begin{aligned} 1 &= 1, & 1 &= 1, \\ \alpha &= 1 \cdot a + \alpha_1, & \alpha_1 &= -1 \cdot a + \alpha, \\ \beta &= 1 \cdot b + \beta_1; & \beta_1 &= -1 \cdot b + \beta. \end{aligned}$$

It follows that every integer in  $\Omega$  of the form  $x + \alpha y + \beta z$  may be expressed through the form  $x' + \alpha_1 y' + \beta_1 z'$  and *inversely*, where  $x, y, z; x', y', z'$  are rational integers.

It has thus been shown that in every cubic realm there is a basis of all integers of  $\Omega$ , of which the one  $= 1$  and the product of the other two is a rational integer ( $= ab + c_1$ ).

Let  $1, \alpha, \beta$  be such a basis of all integers of  $\Omega$  where

$$\alpha\beta = c,$$

$c$  being a rational integer; and further let

$$\begin{aligned} \alpha^2 &= a'\alpha + a\beta - a'', \\ \beta^2 &= b\alpha + b'\beta - b'', \end{aligned}$$

where  $a', a, a'', b, b', b'', c$  are rational integers. That these seven integers are not independent may be seen by computing  $\alpha^2\beta$  in two different ways: on the one hand

$$\alpha^2\beta = \alpha(\alpha\beta) = \alpha c,$$

and on the other

$$\begin{aligned} \alpha^2\beta &= (a'\alpha + a\beta - a'')\beta = a'\alpha\beta + a\beta^2 - a''\beta \\ &= a'c + a(b\alpha + b'\beta - b'') - a''\beta \\ &= ab\alpha + (ab' - a'')\beta + a'c - ab''. \end{aligned}$$

It follows that

$$ab\alpha + (ab' - a'')\beta + a'c - ab'' = \alpha c.$$

Since  $1, \alpha, \beta$  are a basis of  $\Omega$ , there can be no linear relation among them. Hence the relation just written must be an identity. We therefore have:

$$ab = c, \quad ab' - a'' = 0, \quad a'c - ab'' = 0.$$

Since  $c = ab = \alpha\beta$ , it follows that  $a \neq 0$ . We therefore have from the three relations just written the following:

$$c = ab \quad a'' = ab', \quad b'' = a'b.$$

Besides these three relations among the seven rational constants there are no others; for however we may start, we always derive the three equations written above. From these relations there result

$$\alpha\beta = ab, \quad \alpha^2 = a'\alpha + a\beta - ab', \quad \beta^2 = b\alpha + b'\beta - ba',$$

from which follow at once the formulas

$$\alpha(\alpha - a') = a(\beta - b'),$$

$$\beta(\beta - b') = b(\alpha - a').$$

The cubic equations which 1,  $\alpha$ ,  $\beta$  satisfy are (Art. 67) either irreducible or the third power of a linear equation with rational integral coefficients. It is clear that 1 satisfies the cubic equation

$$(x - 1)^3 = 0$$

and further

$$\alpha^3 = a'\alpha^2 + a\alpha\beta - ab'\alpha,$$

or

$$\alpha^3 - a'\alpha^2 + ab'\alpha - a^2b = 0;$$

and similarly

$$\beta^3 - b'\beta^2 + ba'\beta - b^2a = 0.$$

These are the cubic equations which 1,  $\alpha$ ,  $\beta$  satisfy. If we use the symbol  $S(x)$  to denote the *spur* of  $x$ , it follows from the three equations just written that

$$S(1) = 3, \quad S(\alpha) = a', \quad S(\beta) = b',$$

$$N(1) = 1, \quad N(\alpha) = a^2b, \quad N(\beta) = b^2a.$$

If  $\alpha'$ ,  $\alpha''$  are the conjugate quantities with  $\alpha$ , it follows from the equation

$$\alpha^2 = a'\alpha + a\beta - ab'$$

that

$$\alpha'^2 = a'\alpha' + a\beta' - ab'$$

and

$$\alpha''^2 = a'\alpha'' + a\beta'' - ab',$$



*Note.* It may be observed that were the determinant  $D=0$ , it would be possible to determine  $n$  rational numbers  $x_1, x_2, \dots, x_n$  such that

$$x_1 S(\omega_i \omega_1) + x_2 S(\omega_i \omega_2) + \dots + x_n S(\omega_i \omega_n) = 0 \quad (i=1, 2, \dots, n).$$

And that is

$$S[\omega_i(x_1 \omega_1 + x_2 \omega_2 + \dots + x_n \omega_n)] = 0,$$

or

$$S(\omega_i \tau) = 0 \quad (i=1, 2, \dots, n),$$

where

$$\tau = x_1 \omega_1 + x_2 \omega_2 + \dots + x_n \omega_n.$$

If

$$\rho = \rho_1 \omega_1 + \rho_2 \omega_2 + \dots + \rho_n \omega_n$$

is an arbitrary number of the realm, then is

$$\rho \tau = x_1 \omega_1 \rho + x_2 \omega_2 \rho + \dots + x_n \omega_n \rho,$$

and therefore  $S(\rho \tau) = 0$  for every number  $\rho$  of the realm. How-

ever, writing  $\rho = \frac{1}{\tau}$ , it would follow that  $S(1) = 0$ , which is not true.

Accordingly the discriminant of the basal elements  $\omega_1, \omega_2, \dots, \omega_n$  cannot be zero. (See Art. 63.)

## EXAMPLES

1. If  $\omega$  is an arbitrary integer of the cubic realm  $\Omega$ , which may therefore be written in the form  $\alpha x + \beta y + z$ , where  $x, y, z$  are rational integers, and if  $\omega', \omega''$  are the two integers that are conjugate to  $\omega$ , derive the following relation:

$$(\omega' - \omega'')(\omega'' - \omega)(\omega - \omega') = \sqrt{D} \varphi(x, y),$$

where

$$\varphi(x, y) = ax^3 + a'x^2y + b'xy^2 + by^3.$$

2. If  $\rho$  is a primitive cube root of unity, viz.  $\rho = \frac{-1 \pm i\sqrt{3}}{2}$ , then is

$$(\omega + \rho\omega' + \rho^2\omega'')(\omega + \rho^2\omega' + \rho\omega'') = Ax^2 + Bxy + Cy^2 = \psi(x, y),$$

where

$$A = a'^2 - 3ab',$$

$$B = a'b' - 3ab,$$

$$C = b'^2 - 3ba'.$$



$\psi(x, y)$  is the Hessian (covariant) of  $\varphi(x, y)$ , viz.,

$$\begin{aligned} \psi(x, y) &= \frac{1}{4} \left\{ \left( \frac{\partial^2 \varphi}{\partial x \partial y} \right)^2 - \frac{\partial^2 \varphi}{\partial x^2} \frac{\partial^2 \varphi}{\partial y^2} \right\} \\ &= \frac{1}{4} \begin{vmatrix} \frac{\partial^2 \varphi}{\partial x \partial y} & \frac{\partial^2 \varphi}{\partial x^2} \\ \frac{\partial^2 \varphi}{\partial y^2} & \frac{\partial^2 \varphi}{\partial y \partial x} \end{vmatrix}. \end{aligned}$$

3. Show that

$$(\omega + \rho\omega' + \rho^2\omega'')^3 + (\omega + \rho^2\omega' + \rho\omega'')^3 = \chi(x, y),$$

where  $\chi(x, y)$  is the functional determinant (Jacobian) of  $\varphi(x, y)$  and  $\psi(x, y)$ , viz.,

$$\chi(x, y) = \begin{vmatrix} \frac{\partial \psi}{\partial x} & \frac{\partial \psi}{\partial y} \\ \frac{\partial \varphi}{\partial x} & \frac{\partial \varphi}{\partial y} \end{vmatrix} = \frac{\partial \psi}{\partial x} \frac{\partial \varphi}{\partial y} - \frac{\partial \psi}{\partial y} \frac{\partial \varphi}{\partial x}.$$

4. Show that

$$-2\chi(x, y) = \frac{\partial D}{\partial b} x^3 - 3 \frac{\partial D}{\partial b'} x^2 y + 3 \frac{\partial D}{\partial a'} x y^2 - \frac{\partial D}{\partial a} y^3.$$

5. Show that among the functions  $\varphi(x, y)$ ,  $\psi(x, y)$  and  $\chi(x, y)$  the following relation exists

$$\chi^2 + 27D\varphi^2 = 4\psi^3,$$

upon which relation the solution of a cubic depends. The functions  $\chi, \varphi, \psi$  are covariants, while  $D$  (the discriminant) is the only invariant of the cubic realm.

### CYCLOTOMIC (DIVISION-OF-THE-CIRCLE) REALMS

ART. 105. The so-called cyclotomic (division-of-the-circle) realms offer a further example of the general theory of algebraic realms. Such realms are defined through a root ( $\neq 1$ ) of the equation

$$y^m = 1.$$

The discussion will be limited here to the case where  $m$  is a prime integer  $\neq 2$ . It is evident that  $\vartheta$  satisfies the

equation

$$f(t) = \frac{t^m - 1}{t - 1} = t^{m-1} + t^{m-2} + t^{m-3} + \dots + 1 = 0.$$

The quantity  $\vartheta$  is an algebraic integer, in fact an algebraic unit since  $N(\vartheta) = \pm 1$ . It follows that

$$f(t) = \frac{t^m - 1}{t - 1} = (t - \vartheta)(t - \vartheta^2)(t - \vartheta^3) \dots (t - \vartheta^{m-1}).$$

If we write  $t = 1$ , it is seen that

$$f(1) = m = (1 - \vartheta)(1 - \vartheta^2) \dots (1 - \vartheta^{m-1}).$$

*The quotient of any two of the factors on the right-hand side is an algebraic unit.*

For consider first the quotient  $\frac{1 - \vartheta^r}{1 - \vartheta}$  ( $r = 1, 2, \dots, m - 1$ ). We note that  $\frac{1 - \vartheta^r}{1 - \vartheta} = 1 + \vartheta + \vartheta^2 + \dots + \vartheta^{r-1}$  is an algebraic integer. Further it may be shown that  $\frac{1 - \vartheta}{1 - \vartheta^r}$  is an algebraic integer; for, since  $r$  and  $m$  are relatively prime to each other, two other integers,  $r'$  and  $m'$  may be determined such that

$$rr' + mm' = 1.$$

It follows that

$$\vartheta = \vartheta^{rr' + mm'} = \vartheta^{rr'} \cdot \vartheta^{mm'} = \vartheta^{rr'},$$

so that

$$\frac{1 - \vartheta}{1 - \vartheta^r} = \frac{1 - \vartheta^{rr'}}{1 - \vartheta^r} = 1 + \vartheta^r + \vartheta^{2r} + \dots + \vartheta^{r(r'-1)},$$

which is an algebraic integer. It is thus seen (Art. 90) that  $\frac{1 - \vartheta^r}{1 - \vartheta}$  ( $r = 1, 2, \dots, m - 1$ ) are algebraic units. And, since the quotient of two units is a unit, it follows that

$$\frac{\frac{1 - \vartheta^r}{1 - \vartheta}}{\frac{1 - \vartheta^s}{1 - \vartheta}} = \frac{1 - \vartheta^r}{1 - \vartheta^s} \quad (r, s = 1, 2, \dots, m - 1)$$

are algebraic units. It is also evident from above that

$$m = (1 - \vartheta)^{m-1} \frac{1 - \vartheta^2}{1 - \vartheta} \cdot \frac{1 - \vartheta^3}{1 - \vartheta} \cdots \frac{1 - \vartheta^{m-1}}{1 - \vartheta}.$$

Since the quotients on the right are units and the product of several units is a unit, we have, if we put  $1 - \vartheta = \mu$ ,

$$m = \mu^{m-1} \epsilon,$$

$\epsilon$  being an algebraic unit. From this it is seen that

$$N(m) = N(\mu^{m-1})N(\epsilon) = N(\mu)^{m-1}N(\epsilon).$$

If  $\vartheta$  satisfies an irreducible equation of the  $n$ th degree, where  $n \leq m - 1$ , then the realm  $\mathfrak{R}(\vartheta)$  is of the  $n$ th degree, so that

$$N(m) = m^n$$

and

$$N(\epsilon) = \pm 1.$$

It follows that

$$m^n = \pm N(\mu)^{m-1}.$$

As  $m$  is a prime integer,  $N(\mu)$  must be some power of  $m$ , say

$$N(\mu) = m^l,$$

where  $l$  is an integer. We then have

$$m^n = \pm m^{l(m-1)},$$

so that

$$n = l(m - 1).$$

Since  $n \leq m - 1$ , it follows that

$$n = m - 1.$$

It is thus proved again (cf. Art. 12) that the equation  $f(t) = 0$  is irreducible and that the realm  $\mathfrak{R}(\vartheta)$  is of the  $m - 1$  degree.

**ART. 106. The Discriminant.** The  $m - 1$  quantities that are conjugate with  $\vartheta$  are:  $\vartheta, \vartheta^2, \dots, \vartheta^{m-1}$ , and the  $m - 1$  quantities that are conjugate with  $\mu$  are:  $1 - \vartheta, 1 - \vartheta^2, \dots, 1 - \vartheta^{m-1}$ . It follows that

$$N(\mu) = (1 - \vartheta)(1 - \vartheta^2) \cdots (1 - \vartheta^{m-1}) = f(1) = m;$$

or

$$N(\mu) = m,$$

where  $\mu = 1 - \vartheta$ . It is also seen that

$$\mu^2 = 1 - 2\vartheta + \vartheta^2,$$

$$\mu^3 = 1 - 3\vartheta + 3\vartheta^2 - \vartheta^3,$$

etc. And it may be further noted that every linear form of  $\mu^0, \mu^1, \mu^2, \dots, \mu^{m-2}$ , that is,

$$x_0 + x_1\mu + x_2\mu^2 + \dots + x_{m-2}\mu^{m-2},$$

where the  $x$ 's are rational integers, may, owing to the above relations be expressed through a linear form of  $\vartheta^0, \vartheta^1, \vartheta^2, \dots, \vartheta^{m-2}$  with rational integral coefficients; and *inversely* the quantities  $1, \vartheta, \vartheta^2, \dots, \vartheta^{m-2}$  may be expressed with rational integral coefficients through  $1, \mu, \mu^2, \dots, \mu^{m-2}$ . Owing to the fact that the two systems of numbers  $\vartheta^0, \vartheta^1, \vartheta^2, \dots, \vartheta^{m-2}$  and  $\mu^0, \mu^1, \mu^2, \dots, \mu^{m-2}$  may be expressed linearly and with integral rational coefficients the one through the other, it follows that (Arts. 22 and 63)

$$\Delta(1, \mu, \mu^2, \dots, \mu^{m-2}) =$$

$$\Delta(1, \vartheta, \vartheta^2, \dots, \vartheta^{m-2}) = (-1)^{\frac{(m-1)(m-2)}{2}} N\{f'(\vartheta)\}.$$

From the identical equation

$$t^m - 1 \equiv (t-1)f(t),$$

we have through differentiation

$$mt^{m-1} = f(t) + (t-1)f'(t),$$

so that for  $t = \vartheta$

$$m\vartheta^{m-1} = f(\vartheta) + (\vartheta-1)f'(\vartheta) = (\vartheta-1)f'(\vartheta).$$

We therefore have

$$N(m\vartheta^{m-1}) = N(\vartheta-1)N\{f'(\vartheta)\}.$$

Since

$$N(\vartheta) = 1, \quad N(m) = m^{m-1},$$

and

$$\begin{aligned} N(\vartheta - 1) &= (\vartheta - 1)(\vartheta^2 - 1) \cdots (\vartheta^{m-1} - 1) \\ &= (-1)^{m-1} (1 - \vartheta)(1 - \vartheta^2) \cdots (1 - \vartheta^{m-2}) \\ &= N(1 - \vartheta) = N(\mu) = m, \end{aligned}$$

it follows that

$$N\{f'(\vartheta)\} = m^{m-2},$$

and consequently

$$\begin{aligned} \Delta(1, \mu, \dots, \mu^{m-2}) &= (-1)^{\frac{(m-1)(m-2)}{2}} m^{m-2} = \{(-1)^{m-2}\}^{\frac{m-1}{2}} m^{m-2} \\ &= (-1)^{\frac{m-1}{2}} m^{m-2}. \end{aligned}$$

ART. 107. THEOREM. *The quantities  $1, \mu, \mu^2, \dots, \mu^{m-2}$  form a basis of all the integers of the cyclotomic realm of the  $(m-1)$ st degree.*

To show this let us first prove two lemmas.

(1) *If the rational integer  $r$  is divisible by  $\mu$ , it is also divisible by  $m$ .*

For if  $r$  is divisible by  $\mu$ , then  $N(r)$  is divisible by  $N(\mu)$ , that is,  $r^{m-1}$  is divisible by  $m$ ; but as  $m$  is a prime integer, it follows that  $r$  is divisible by  $m$ .

(2) *If the algebraic integer*

$$\alpha = x_0 + x_1\mu + x_2\mu^2 + \cdots + x_{m-2}\mu^{m-2},$$

where  $x_0, x_1, x_2, \dots, x_{m-2}$  are rational integers, is divisible by  $m$ , each of the integers  $x_0, x_1, \dots, x_{m-2}$  is divisible by  $m$ .

Since

$$m = \epsilon\mu^{m-1},$$

it follows, if  $\alpha$  is divisible by  $m$ , that  $\alpha$  must also be divisible by  $\mu$ ; and hence also that  $x_0$  must be divisible by  $\mu$ . But if the rational integer  $x_0$  is divisible by  $\mu$ , from the last lemma it follows that it must also be divisible by  $m$ . If then the integer  $\alpha$  is divisible by  $m$ , then also

$$x_1\mu + x_2\mu^2 + \cdots + x_{m-2}\mu^{m-2}$$

must be divisible by  $m$ . The expression is further divisible by  $\mu^2$  and consequently the rational integer  $x_1$



is divisible by  $\mu$ , and therefore also by  $m$ . Repeating this process it is seen that all the integers  $x_0, x_1, \dots, x_{m-2}$  are divisible by  $m$ .

To show that the integers  $1, \mu, \mu^2, \dots, \mu^{m-2}$  form a basis of all integers of their realm of rationality, suppose that this were *not* the case and that there was an integer of the cyclotomic realm that could be expressed through the quantities just written linearly with rational (but not integral) coefficients, in the form

$$\frac{c_0 + c_1\mu + c_2\mu^2 + \dots + c_{m-2}\mu^{m-2}}{c},$$

where  $c_0, c_1, \dots, c_{m-2}, c \neq 1$  are rational integers without a greatest common divisor. From the theorem (Art. 95) it follows that  $\Delta(1, \mu, \dots, \mu^{m-2})$ , that is  $(-1)^{\frac{m-1}{2}} m^{m-2}$  is divisible by  $c$ . It follows that  $c$  is a power of  $m$ .

If then  $c_0 + c_1\mu + c_2\mu^2 + \dots + c_{m-2}\mu^{m-2}$  is divisible by  $c$ , it must also be divisible by  $m$ , and consequently from lemma (2),  $c_0, c_1, \dots, c_{m-2}$  must be each divisible by  $m$ , which contradicts the hypothesis that the integers  $c_0, c_1, \dots, c_{m-2}, c$  had no common divisor. It is thus shown that  $1, \mu, \dots, \mu^{m-2}$  form a basis of the cyclotomic realm, and that the *basal invariant* is

$$D = \Delta(1, \mu, \dots, \mu^{m-2}) = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

*Note.* For examples see a paper by the author, "Trigonometric Realms of Rationality," *Rendiconti del circolo matematico di Palermo* (1925), Vol. 49, pp. 147-183.

## CHAPTER V

### THE MODULS OF DEDEKIND. DIVISIBILITY. GENERALIZED NOTIONS OF DIVISION

ART. 108. The problem of resolving uniquely an integral function or a rational integer into prime factors was made dependent upon Euclid's Algorithm (Art. 14 and Art. 24). This Algorithm, as we shall show below, is applicable to the realms  $\mathfrak{R}(i)$  and  $\mathfrak{R}(\omega)$ , where  $i = \sqrt{-1}$  and  $\omega = \frac{-1 + \sqrt{-3}}{2}$ , but it is not applicable to realms in general as we shall also see.

Consider first the realm of rationality  $\mathfrak{R}(i)$  where  $i^2 = -1$ , and let  $\xi = x + iy$  be a fractional number of this realm, at least one of the rational numbers  $x$  or  $y$  being fractional. Next note that it is always possible to find an algebraic integer  $\mu = m + ni$ , where  $m$  and  $n$  are rational integers, such that the norm of  $\xi - \mu$ , that is  $(x - m)^2 + (y - n)^2$  is not greater than  $\frac{1}{2}$ , for we need only choose  $m$  and  $n$  such that the absolute values of  $x - m$  and  $y - n$  are not greater than  $\frac{1}{2}$ .

As usual we shall denote *algebraic* integers by Greek letters.

If then  $\alpha$  and  $\alpha_1$  are two integers in  $\mathfrak{R}(i)$ ,  $\alpha_1$  being different from zero, it is possible to determine the integer  $\mu$  such that

$$\frac{\alpha}{\alpha_1} - \mu = \frac{\alpha'_1 \alpha}{\alpha'_1 \alpha_1} - \mu = \frac{\alpha_2}{\alpha_1},$$

where

$$N\left[\frac{\alpha}{\alpha_1} - \mu\right] = \frac{N(\alpha_2)}{N(\alpha_1)} \leq \frac{1}{2}.$$

It follows that

$$\alpha = \mu\alpha_1 + \alpha_2, \quad N(\alpha_2) < N(\alpha_1).$$

If  $\alpha_2$  is not zero, we may in the same way determine the algebraic integer  $\mu_1$  such that

$$\alpha_1 = \mu_1\alpha_2 + \alpha_3, \quad N(\alpha_3) < N(\alpha_2).$$

(See Smith's *Report*, p. 72.) Since the norms are rational integers, each being less than the preceding, it is evident that after a finite number of steps the norm must be zero. The following system of equations is thus presented.

$$\begin{aligned} \alpha &= \mu\alpha_1 + \alpha_2 \\ \alpha_1 &= \mu_1\alpha_2 + \alpha_3 \\ &\dots\dots\dots \\ \alpha_{h-2} &= \mu_{h-2}\alpha_{h-1} + \alpha_h \\ \alpha_{h-1} &= \mu_{h-1}\alpha_h. \end{aligned}$$

Observing the last of these equations, note that all the integers  $\alpha_{h-1}, \alpha_{h-2}, \dots, \alpha_3, \alpha_2, \alpha_1, \alpha$ , and in particular  $\alpha_1$  and  $\alpha$  are divisible by  $\alpha_h$ ; and reciprocally starting with the first of these equations it is seen that every common divisor of  $\alpha$  and  $\alpha_1$  is a divisor of all the following  $\alpha$ 's, and in particular of  $\alpha_h$ . Every other integer that has this property must be an *associate* (Art. 91) of  $\alpha_h$ . In the realm  $\mathfrak{R}(i)$  we may say that  $\alpha_h$  (and each of its associate numbers) is the *greatest common divisor* of  $\alpha$  and  $\alpha_1$ . In this realm an integer is *factorable* when it is the product of several integers in  $\mathfrak{R}(i)$  of which none is a unit. When an integer is not decomposable into such factors, it may be called a *prime* integer in  $\mathfrak{R}(i)$ .

From the system of equations above it is seen that if  $\delta$  is the greatest common divisor of two integers  $\alpha$  and  $\beta$  in  $\mathfrak{R}(i)$ , two other integers  $\kappa$  and  $\lambda$  in  $\mathfrak{R}(i)$  may always be found such that

$$\kappa\alpha + \lambda\beta = \delta,$$

and in particular if  $\alpha$  and  $\beta$  are *relatively prime* (having no divisors in common except units), the equation

$$\kappa\alpha + \lambda\beta = 1$$

can be satisfied through integers  $\kappa$  and  $\lambda$  in  $\mathfrak{R}(i)$ . In general *it is seen*, as in the case of rational integers (Art. 24), *that an integer in  $\mathfrak{R}(i)$  may always and in only one way be decomposed into its prime factors.*

A somewhat different exposition of the above method is the following:

Let  $\alpha$  and  $\beta$  be two integers of  $\mathfrak{R}(i)$ , say  $\alpha = a_1 + b_1i$ ,  $\beta = a_2 + b_2i$ , and such that  $N(\alpha) \geq N(\beta)$ . Through simple division it is seen that

$$\frac{\alpha}{\beta} = \frac{\alpha\beta'}{N(\beta)} = \gamma + \frac{r+si}{N(\beta)},$$

where  $\gamma$  is an integer in  $\mathfrak{R}(i)$  and  $r$  and  $s$  are rational integers such that

$$|r| \leq \frac{1}{2}N(\beta), \quad |s| \leq \frac{1}{2}N(\beta).$$

It follows that  $\alpha = \beta\gamma + \rho_0$  where  $\rho_0$  is integral, since  $\alpha - \beta\gamma$  is integral in  $\mathfrak{R}(i)$ . Further it is seen that

$$N(\rho_0) = \frac{r^2 + s^2}{N(\beta)} \leq \frac{1}{2}N(\beta).$$

Similarly it is seen that

$$\beta = \rho_0\gamma_1 + \rho_1 \quad \text{where} \quad N(\rho_1) \leq \frac{1}{2}N(\rho_0),$$

and the process may be continued with the same conclusion as above.

It may be shown (see for example Weber's *Algebra* 2<sup>nd</sup> Edition, Vol. I, p. 634 and p. 635) *first*, that every prime integer  $p$  (rational in  $\mathfrak{R}(1)$  of the form  $4n+1$  may be expressed as the sum of the squares of two integers. For example  $13 = 3^2 + 2^2$ ,  $29 = 5^2 + 2^2$ . It may be shown *secondly*, that *no* prime integer  $q$  of the form  $4n+3$  can be expressed as the sum of two such squares.

Since  $a^2 + b^2 = (a + ib)(a - ib)$ , it is clear that the prime integers  $p$  of the first category are *not* prime numbers in the realm  $\mathfrak{R}(i)$ . To this category belongs also  $2 = (1 + i)(1 - i)$ .

The four units of  $\mathfrak{R}(i)$  are  $\pm 1, \pm i$ ; and the four numbers  $a + ib, -a - ib, -b + ai, b - ai$  are associates and play a rôle in  $\mathfrak{R}(i)$  analogous to that played by two numbers with opposite sign in  $\mathfrak{R}(1)$ . On the other hand primes  $q$  of the second category remain primes in  $\mathfrak{R}(i)$ . Thus the primes in  $\mathfrak{R}(i)$  consist of the real primes  $q$  and the factors of the primes  $p$ .<sup>1</sup> Reid in his *Elements of the Theory of Algebraic Numbers* has given a very complete and instructive discussion of the numbers of the realm  $\mathfrak{R}(i)$ .

#### EXAMPLES

1. Show that the following are complex prime integers in  $\mathfrak{R}(i)$ :  $1 + i, 1 + 2i, 3 + 2i, 1 + 4i, 5 + 2i, 1 + 6i, 11 + 4i, 7 + 10i, 1 + 14i, 11 + 6i, 9 + 4i, 13 + 2i$ .

2. Determine for the realm  $\mathfrak{R}(i)$  all the complex prime integers whose norms lie between 350 and 400.

For tables of Complex Primes see Kummer in *Liouville's Journal*, Vol. 12, p. 206; Reuschle, *Berlin Monatsber.*, 1859, pp. 488, 694, and 1860, pp. 150 and 714; also Cayley, *Crelle*, Vol. 55, p. 192 and 56, p. 186.

ART. 109. **The Realm  $\mathfrak{R}(\omega) = \mathfrak{R}(\sqrt{-3})$ .** The numbers of this realm are of the form  $\gamma = x + \omega y$ , integral or fractional when  $x$  and  $y$  are rational integers or fractions, respectively. They have norms

$$\begin{aligned} N(\gamma) &= (x + \omega y)(x + \omega^2 y) = x^2 - xy + y^2 \\ &= \frac{2x - y + y\sqrt{-3}}{2} \cdot \frac{2x - y - y\sqrt{-3}}{2} = \frac{(2x - y)^2 + 3y^2}{4}. \end{aligned}$$

<sup>1</sup> See Gauss, "Theoria residuorum biquadraticorum, commentatio secunda," *Werke*, Vol. II, p. 95. Dedekind, "Sur la théorie des nombres algébriques," *Bulletin de Sc. Math.*, 1<sup>st</sup> Series, Vol. XI and 2<sup>nd</sup> Series, Vol. I.



Units in this realm are (Art. 99)  $\pm 1$ ,  $\pm\omega$ ,  $\pm\omega^2$  and therefore, since  $1 + \omega + \omega^2 = 0$ ,

$$\begin{aligned} \pm(x + \omega y), \quad \pm(\omega x + \omega^2 y) &= \pm[-y + (x - y)\omega], \\ \pm(x\omega^2 + y) &= \pm(y - x - x\omega) \end{aligned}$$

are associated integers. If  $\tau$  is any fractional number of  $\mathfrak{R}(\omega)$ , an integer  $\mu$  may be derived as in the preceding article such that

$$N(\tau - \mu) = x^2 - xy + y^2 \equiv \frac{3}{4};$$

and as in the preceding article, it is seen that the Euclid Algorithm is applicable and that factorization is a unique process.

#### EXAMPLES

1. If  $p$  is a prime integer of the form  $3k + 1$ , show that it may be expressed in the form  $a^2 - ab + b^2$  and that  $4p$  is of the form  $A^2 + 27B^2$ , where  $a$ ,  $b$ ,  $A$ ,  $B$ , are integers. (See Weber's *Algebra*, Vol. I, § 180).

2. If  $p$  has the form of the preceding example, show that

$$p = \left[ \frac{A + 3B}{2} + 3\omega B \right] \left[ \frac{A - 3B}{2} - 3\omega B \right].$$

3. Show that in  $\mathfrak{R}(\sqrt{-3})$  the following are prime integers:  $1 - \omega$ ,  $1 + 3\omega$ ,  $4 + 3\omega$ ,  $5 + 6\omega$ ,  $14 + 3\omega$ ,  $11 + 9\omega$ ,  $13 + 15\omega$ ,  $16 + 9\omega$ .

ART. 110. That the unique factorization theorem which is true for the realm  $\mathfrak{R}(i)$  and  $\mathfrak{R}(\omega)$  is *not* true in general even in the quadratic realms, may be surmised if an examination is made of the more general quadratic realm  $\mathfrak{R}(\sqrt{m})$ , where  $\sqrt{m}$  is a root of the equation  $x^2 - m = 0$ .

If  $m \equiv 2 \pmod{4}$  or  $m \equiv 3 \pmod{4}$ , it was seen in Art. 97 that  $1, \sqrt{m}$  constitute a basis of all integers of the realm  $\mathfrak{R}(\sqrt{m})$ ; if however  $m \equiv 1 \pmod{4}$  then  $1, \frac{-1 + \sqrt{m}}{2}$  constitute such a basis.

ART. 111. If  $\alpha$  and  $\beta$  are integers in  $\Re(\sqrt{m})$  it is evident that we may write,

$$\frac{\alpha}{\beta} = \frac{\alpha\beta'}{N(\beta)} = \gamma + \frac{r+s\sqrt{m}}{N(\beta)},$$

when  $m \not\equiv 1 \pmod{4}$  or

$$\alpha = \beta\gamma + \rho_0.$$

And we may again take

$$|r| \leq \frac{1}{2} |N(\beta)| \quad \text{and} \quad |s| \leq \frac{1}{2} |N(\beta)|,$$

$$N(\rho_0) = \frac{r^2 - s^2 m}{N(\beta)}.$$

It follows that

$$|N(\rho_0)| \leq \left| \frac{1-m}{4} \right| |N(\beta)|,$$

from which it is seen that for  $m \not\equiv 1 \pmod{4}$ ,  $N(\rho_0) < N(\beta)$  only when  $m = 2, 3, -1, -2$ .

In the second case when  $m \equiv 1 \pmod{4}$ , it is seen that

$$N\left[r_1 + s_1 \frac{1 + \sqrt{m}}{2}\right] = r_1^2 + r_1 s_1 - \frac{m-1}{4} s_1^2,$$

and the condition  $|r_1| \leq \frac{1}{2} |N(\beta)|$ ,  $|s_1| \leq \frac{1}{2} |N(\beta)|$ , is sufficient to make  $|N(\rho_0)| \leq |N(\beta)|$ , only when  $m = -3, 5, 13$ .<sup>1</sup>

When the Euclid Algorithm ceases to be applicable, it is clearly not permissible to assume a priori the results of theorems that depend on this algorithm.

To show that the methods hitherto employed do *not* lead to a unique decomposition into prime factors of all algebraic integers, take the integers of the realm  $\Re(\sqrt{-5})$ . Since  $-5 \equiv 3 \pmod{4}$ , such integers are of the form  $x + y\sqrt{-5}$ , where  $x$  and  $y$  are rational integers. If  $a + b\sqrt{-5}$  is a unit in this realm, its norm must be  $\pm 1$ ,

<sup>1</sup> So great a mathematician as Cauchy attempted to prove the false theorem that the norm of the remainder derived by dividing one complex number by another can always be made less than the norm of the divisor.

and that is

$$N(a+b\sqrt{-5}) = \pm 1,$$

or

$$a^2 + 5b^2 = \pm 1.$$

This relation can be satisfied only when  $a = \pm 1$ . It follows that  $+1$  and  $-1$  are the only units in this realm.

It is observed that  $21 = 3 \cdot 7$ ;  $21 = (4 + \sqrt{-5})(4 - \sqrt{-5})$ , and also  $21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ , where  $3$ ,  $7$ ,  $4 + \sqrt{-5}$ ,  $4 - \sqrt{-5}$ ,  $1 + 2\sqrt{-5}$ ,  $1 - 2\sqrt{-5}$  are irreducible integers in  $\mathfrak{R}(\sqrt{-5})$  and are all different from one another. If, for example,  $3$  were factorable in this realm, then is

$$3 = (x + y\sqrt{-5})(x_1 + y_1\sqrt{-5}),$$

where  $x$ ,  $y$ ,  $x_1$ ,  $y_1$  are rational integers.

By equating the real and the imaginary members of this expression, it is seen that

$$3 = xx_1 - 5yy_1,$$

$$0 = xy_1 + x_1y,$$

which equations can be satisfied integrally only when

$$x = \pm 1, \quad x_1 = \pm 3, \quad y = 0 = y_1$$

or

$$x = \pm 3, \quad x_1 = \pm 1, \quad y = 0 = y_1.$$

It follows that  $3$ , neglecting the unit factors  $\pm 1$ , is irreducible in  $\mathfrak{R}(\sqrt{-5})$ .

It is further seen that the above factors of  $21$  are essentially different. For put

$$4 + \sqrt{-5} = (1 + 2\sqrt{-5})(x + y\sqrt{-5}),$$

where  $x$  and  $y$  must be rational integers.

Equating the real and imaginary parts, it is seen that

$$4 = x - 10y, \quad 1 = 2x + y,$$

equations which can *not* be satisfied integrally.

Similarly it may be proved that all of the six factors of  $21$ , namely  $3$ ,  $7$ ,  $4 + \sqrt{-5}$ ,  $4 - \sqrt{-5}$ ,  $1 + 2\sqrt{-5}$ ,  $1 - 2\sqrt{-5}$

are different and irreducible in the realm  $\Re(\sqrt{-5})$ .

Further examples in this realm are

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

etc.

In the *real* realm  $\Re(\sqrt{10})$  it is seen that the algebraic integers are of the form  $x + y\sqrt{10}$ , where  $x$  and  $y$  are rational integers, since  $10 \equiv 2 \pmod{4}$ , and the basis of this realm consists of the integers  $1, \sqrt{10}$ .

If we put

$$\epsilon = x + y\sqrt{10},$$

and

$$N(\epsilon) = x^2 - 10y^2 = -1,$$

it is seen (Art. 99) that

$$x = \pm 3, \quad y = \pm 1,$$

so that

$$\begin{aligned} -1 &= (-3 + \sqrt{10})(-3 - \sqrt{10}), \\ (-1)^2 &= (19 - 6\sqrt{10})(19 + 6\sqrt{10}), \end{aligned}$$

etc., the units being  $\epsilon^e = (-3 + \sqrt{10})^e$ ,  $e$  any rational integer.

In this realm it is again seen that the integer 6 may be factored in the two essentially different ways

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

However the two factors of 6, namely  $(16 + 5\sqrt{10})(16 - 5\sqrt{10})$  are *not* essentially different from  $(4 + \sqrt{10})(4 - \sqrt{10})$ ; for it is seen that  $(4 + \sqrt{10})\epsilon^2$ , that is

$$(4 + \sqrt{10})(19 - 6\sqrt{10}) = 16 - 5\sqrt{10},$$

while

$$(4 - \sqrt{10})(19 + 6\sqrt{10}) = 16 + 5\sqrt{10}.$$

Thus it is seen that the fundamental theorem in the theory of rational integers, namely that such integers are uniquely factorable into products of prime factors, is *no* longer true of the algebraic integers of quadratic

realms; nor is this theorem true of the integers of the cubic, biquadratic, and the higher realms.

This leads us necessarily to something that must take the place of prime factors in their respective realms when it comes to the consideration of the unique factorization of algebraic integers into such factors. Thus we are brought to the study of *ideals* which are special kinds of moduls, the general treatment of which is now given. With Dedekind we make these moduls fundamental in this generalized theory of numbers.

ART. 112. An algebraic integer of a realm  $\Omega$  might be defined as *factorable*, if there exist two algebraic integers  $\alpha$  and  $\beta$  which are not units and which are such that

$$\omega = \alpha\beta.$$

Then clearly every algebraic integer is factorable, since we always have

$$\omega = \sqrt{\omega} \cdot \sqrt{\omega},$$

and  $\sqrt{\omega}$  (Art. 88, end) is an algebraic integer which is different from a unit. For if  $\sqrt{\omega}$  is a unit, then also  $\omega$  is a unit which case is naturally excluded. This troublesome condition that every algebraic integer is factorable may be obviated if in the definition of the resolution into factors the discussion is limited to a *definite* realm. Accordingly the following definition may be offered:

*An algebraic integer  $\omega$  of  $\Omega$  is resolvable into factors if there exist in  $\Omega$  two integers  $\alpha$  and  $\beta$  that are different from units and are such that  $\omega = \alpha\beta$ .*

This definition corresponds to that of the resolution of a rational integer into its factors; for if  $\omega = \alpha\beta$ , then is

$$N(\omega) = N(\alpha)N(\beta).$$

Thus it is shown that the resolution of  $\omega$  into the product of two algebraic integers  $\alpha$  and  $\beta$  corresponds to that of the rational integer  $N(\omega)$  into the product of the two



rational integers  $N(\alpha)$  and  $N(\beta)$ , of which neither  $= 1$ . In the case of this definition an algebraic integer cannot be resolved into an infinite number of factors; and further there are integers which are irreducible, this being clearly the case of such an algebraic integer whose norm is a rational prime integer. An example is found in Art. 108. Although we have thus obviated one troublesome condition in the definition of *divisibility*, we still meet with another:

*The factorization of a composite algebraic integer is not unique, but may be performed in different ways.*

For example (as is discussed in Art. 205), it is seen that in the realm  $\Re(\sqrt{-5})$ ,

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

where the factors are all different algebraic integers. It is thus seen that an algebraic integer in  $\Omega = \Re(\sqrt{-5})$  may be resolved in several different ways with irresolvable factors. In accord, then, with the last definition of *divisibility*, an algebraic integer may be resolved into a finite number of irreducible factors, but in *several different ways*. This is owing to the fact that in the *theory of algebraic integers* the theorem is *not* true that *if a product is divisible by an irreducible integer, one of the factors of this product is divisible by that integer*.

EXAMPLE. Observe that in the realm  $\Re(\sqrt{-7})$ ,

$$2^3 = 2 \cdot 4 = 2 \cdot 2 \cdot 2 = (1 + \sqrt{-7})(1 - \sqrt{-7});$$

and show that  $2^n (n > 2)$  is factorable in products of complex factors.

ART. 113. The troublesome condition just mentioned was in part overcome by Kummer ("Zur Theorie der komplexen Zahlen," *Crelle*, 35), who recognized the fact that prime numbers are not the *extreme* elements. To introduce this theory of Kummer, *the conception of*

*divisibility* must be extended. Let us return for a moment to the realm of rational numbers. Suppose that  $a$  and  $b$  are two rational fractional or integral numbers. Note that the linear form

$$ax + by,$$

for integral values of  $x$  and  $y$ , represents all those rational numbers that are divisible by the greatest common divisor of  $a$  and  $b$ . We may therefore define *any number  $v$  as divisible by the complex of numbers  $a$  and  $b$ , say  $[a, b]$ , if it is possible to determine two rational integers  $x$  and  $y$  such that*

$$v = ax + by.$$

This is an extension of the usual conception of divisibility in that  $v$  is divisible by  $a$ , if  $v = ax$  where  $x$  is an integer. This extension is clearly superfluous, so long as we remain in the usual realm of rational numbers; for evidently every number that is divisible by the complex  $[a, b]$  is, so long as  $a$  and  $b$  are rational numbers, divisible by the greatest common divisor  $d$ , say, of  $a$  and  $b$ , and every number that is divisible by  $d$  is divisible by  $[a, b]$ . We may therefore write

$$[a, b] = [d],$$

or

$$ax + by = dz,$$

where  $x, y, z$  are rational integers. For evidently corresponding to any two integral values of  $x, y$ , there is an integral value of  $z$ , and reciprocally corresponding to every integral value of  $z$ , there are two integral values of  $x$  and  $y$ . Hence the conception of divisibility by the complex  $[a, b]$  is, so long as  $a$  and  $b$  are rational numbers, *identical* with the conception of divisibility by  $d$ . It is otherwise if we pass to the realm of algebraic numbers. Accordingly the following definition is introduced: *The*

integral or fractional algebraic number  $\lambda$  is said to be divisible by the complex  $[\alpha, \beta]$  consisting of the two algebraic numbers  $\alpha$  and  $\beta$ , if there exist two algebraic integers  $\xi$  and  $\eta$  such that

$$\lambda = \alpha\xi + \beta\eta.$$

This conception is no longer superfluous: for suppose that  $\delta$  is a third algebraic number through which  $\alpha$  and  $\beta$  are both divisible, say  $\frac{\alpha}{\delta} = \gamma_1$  and  $\frac{\beta}{\delta} = \gamma_2$ , where  $\gamma_1$  and  $\gamma_2$  are algebraic integers. It is evident that every number that is divisible by  $[\alpha, \beta]$  is divisible by  $\delta$ , for if

$$\tau = \alpha\xi_0 + \beta\eta_0,$$

where  $\xi_0$  and  $\eta_0$  are algebraic integers, then also

$$\tau = \delta\gamma_1\xi_0 + \delta\gamma_2\eta_0,$$

so that

$$\frac{\tau}{\delta} = \gamma_1\xi_0 + \gamma_2\eta_0,$$

which is an algebraic integer. However, every number that is divisible by  $\delta$  is not divisible by  $[\alpha, \beta]$ ; for if this were true then  $\delta$  itself must be divisible by  $[\alpha, \beta]$  and hence expressible in the form

$$\delta = \alpha\xi_1 + \beta\eta_1,$$

where  $\xi_1$  and  $\eta_1$  are algebraic integers. Hence  $\delta$  would be divisible by every *common* divisor of  $\alpha$  and  $\beta$ , so that  $\delta$  would be the *greatest common divisor* of these numbers in the sense that is usual in the theory of the rational numbers. But such a greatest common divisor of two algebraic numbers exists only so long as we remain in the *infinite* realm of all algebraic numbers. We have on the other hand just seen in the discussion of the resolvability of an algebraic integer into its irreducible factors, that this investigation must be restricted to a *definite* realm. Hence with such a restriction the conception of the

greatest common divisor of two algebraic numbers does *not* in general exist (Art. 111). On this account the conception of the divisibility through the complex  $[\alpha, \beta]$  consisting of two algebraic integers  $\alpha, \beta$  is no longer superfluous. It becomes *necessary* when the restriction is made that all quantities belong to a definite finite realm.

**ART. 114. The Modul Defined.** The above considerations and definitions are also true of such complexes as  $[\alpha, \beta, \gamma, \dots]$  which consist of more than two algebraic numbers. *The algebraic number  $\lambda$  is said to be divisible by the complex of algebraic numbers of the realm  $\Omega$ , say  $[\alpha, \beta, \gamma, \dots]$ , if it is possible to determine algebraic integers  $\xi, \eta, \zeta, \dots$  in  $\Omega$  such that*

$$\lambda = \alpha\xi + \beta\eta + \gamma\zeta + \dots$$

Through these definitions the theory of linear forms  $\alpha\xi + \beta\eta + \gamma\zeta + \dots$  is introduced, the variables  $\xi, \eta, \zeta, \dots$  being algebraic integers, while the coefficients  $\alpha, \beta, \gamma, \dots$ , are integral or fractional algebraic numbers. All the quantities introduced belong to a definite realm of rationality, say  $\Omega$ . We shall next limit the investigation by restricting the variables  $\xi, \eta, \zeta, \dots$  of the linear form, in that they are allowed to take only *rational* integral values, while the coefficients are any arbitrary algebraic numbers of the fixed realm  $\Omega$ .

The collectivity of all algebraic numbers which are expressed through the linear form  $\alpha x + \beta y + \gamma z + \dots$ , where  $x, y, z, \dots$ , are rational integers is called<sup>1</sup> a *modul*. It is denoted by the symbol  $[\alpha, \beta, \gamma, \dots]$ . The quantities  $\alpha, \beta, \gamma, \dots$  are the *elements* of the modul. A

<sup>1</sup> See Dedekind, § 165 of the 2<sup>nd</sup> edition of Dirichlet's *Zahlentheorie*. In the derivation of this word, following the Germans, I use the stem of the Latin word *Modulus*. See further *Encyklopaedie der math. Wissenschaften*, Vol. I, p. 307.

number  $\lambda$  is said to be *divisible* by a modul  $[\alpha, \beta, \gamma, \dots]$ , if  $\lambda$  is a number of this modul, that is, if  $\lambda$  is contained in this modul, and that is, if rational integers  $x, y, z, \dots$  may be determined such that

$$\lambda = \alpha x + \beta y + \gamma z + \dots$$

Here we have encountered something which at first may appear as a "confusion of language" in that the conception of "divisibility" and of "being contained in," which *heretofore* have been opposed are *now* identical.

ART. 115. The conception of modul may be made more general, if we are freed from the conception of the linear form. Having this in view, note that if  $\lambda$  and  $\lambda'$  are two numbers that are divisible by the modul  $[\alpha, \beta, \gamma, \dots]$  then also  $\lambda \pm \lambda'$  is divisible by this modul; for, if

$$\lambda = \alpha x + \beta y + \gamma z + \dots,$$

and

$$\lambda' = \alpha x' + \beta y' + \gamma z' + \dots,$$

then is

$$\begin{aligned} \lambda \pm \lambda' &= \alpha(x \pm x') + \beta(y \pm y') + \dots \\ &= \alpha x'' + \beta y'' + \dots, \end{aligned}$$

where  $x'', y'', \dots$  are rational integers.

Accordingly the following definition of a modul may be offered: *A modul is a system of numbers, such that the difference of any two numbers of the system is again a number of the system.* (*Report on Algebraic Numbers*, p. 91.)

It is seen from this definition of a modul that every realm of rationality is a modul,<sup>1</sup> but reciprocally every modul is *not* a realm of rationality. For a realm of rationality  $\Omega = \mathfrak{R}(\vartheta)$ , say, consists of all rational functions

<sup>1</sup> Excepting the modul that consists of the one element 0, which is once for all excluded, the simplest modul is the realm of rational integers. This modul may be denoted by  $\mathfrak{Z}$ .



of  $\mathfrak{a}$ , and the difference of two rational functions is a rational function.

The moduls are represented by small German letters. A number  $\alpha$  is said to be divisible by the modul  $\mathfrak{a}$ , if  $\alpha$  belongs to the modul  $\mathfrak{a}$ . The number 0 forms for itself a modul, and is the only modul that consists of a finite number of numbers. This modul we exclude from further consideration. All other moduls consist of an infinite number of numbers and are reproduced not only through the operation of subtraction but also through the operation of addition. For if there appears in a modul any number  $\alpha (\neq 0)$ , then by the definition of a modul there appears also in this modul the number  $\alpha - \alpha = 0$ ; from which it is seen that the number 0 belongs to every modul. If then  $\alpha$  is divisible by the modul  $\mathfrak{a}$ , then also  $\alpha - \alpha - \alpha = -\alpha$  is also divisible by  $\mathfrak{a}$ . If further  $\alpha$  is divisible by  $\mathfrak{a}$  and also  $\beta$  is divisible by  $\mathfrak{a}$ , using the definition just given of a modul, then also  $-\beta$  is divisible by  $\mathfrak{a}$  and consequently  $\alpha - (-\beta)$  is divisible by  $\mathfrak{a}$ ; that is,  $\alpha + \beta$  is divisible by  $\mathfrak{a}$ .

It follows that if  $\alpha$  is divisible by the modul  $\mathfrak{a}$  then  $\alpha x$  is divisible by  $\mathfrak{a}$ , where  $x$  takes all rational integral values. There are two possibilities: either the quantities represented by  $\alpha x$  constitute all the quantities of the modul  $\mathfrak{a}$ , or there are also other numbers that are divisible by  $\mathfrak{a}$ . In the latter case, if  $\beta$  is a number divisible by  $\mathfrak{a}$ , and not found among the numbers  $\alpha x$ , then also the numbers  $\alpha x + \beta y$ , where  $x$  and  $y$  take all possible rational integral values, are divisible by  $\mathfrak{a}$ . It may happen that these are all the numbers divisible by  $\mathfrak{a}$ ; if not, suppose that  $\gamma$  is divisible by  $\mathfrak{a}$  and is not found among the numbers  $\alpha x + \beta y$ , then also the numbers  $\alpha x + \beta y + \gamma z$ , where  $x, y, z$  take all possible rational integral values, are divisible by the modul  $\mathfrak{a}$ , etc.

This process may continue indefinitely, or it may cease. In the latter case we come to a linear form  $\alpha x + \beta y + \cdots + \eta w$  such that  $\alpha x + \beta y + \cdots + \eta w$  for integral rational values of the variables  $x, y, \cdots, w$  represents all the numbers that are divisible by the modul  $\alpha$ , and reciprocally every number that is divisible by the modul  $\alpha$  may be expressed through the form

$$\alpha x + \beta y + \cdots + \eta w,$$

where  $x, y, \cdots, w$ , are rational integers. In the latter case the modul  $\alpha$  agrees with the definition given above of the modul  $[\alpha, \beta, \cdots, \eta]$ . Such a modul is said to be finite and is called a *modul of finite order*. The system of numbers  $\alpha, \beta, \cdots, \eta$  is called the *basis* of the finite modul, and the number of these elements is called the *order* (or *rank*) of the modul.

The representation of all numbers of a modul  $\alpha$  through a basis is clearly *not* unique, since the basis of a modul may be chosen in an infinite number of different ways (Art. 93).

ART. 116. It was seen above that a realm of rationality (excepting the one which consists only of the number 0) is a modul, and from what was just given it is evident that the order of such a modul is in general *not* finite. For it is evident that the numbers  $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \cdots$  cannot be represented by a finite modul although they belong to the realm  $\mathfrak{R}(1)$ . We shall have little to do in the sequel with moduls whose orders are not finite.

DEFINITION. A modul  $\mathfrak{b}$  is said to be divisible by the modul  $\mathfrak{a}$  if every number that is divisible by  $\mathfrak{b}$  is divisible also by  $\mathfrak{a}$ .

If we apply this definition of divisibility to that of one modul by another modul, both of order unity, we have the theorem:

If the rational number  $b$  is divisible by the rational number  $a$ , then also  $[b]$  is divisible by  $[a]$ .

For any number  $bx$  where  $x$  is a rational integer may be written  $a \cdot \frac{b}{a}x = ay$  where  $y$  is a rational integer; for example:  $[6]$  is divisible by  $[3]$ ;  $[\frac{1}{3}]$  is divisible by  $[\frac{1}{12}]$ .

If  $\alpha$  is divisible by the modul  $a$ , then every number  $\alpha x$  where  $x$  is a rational integer is divisible by  $a$ ; if  $\alpha$  and  $\beta$  are both divisible by  $a$ , then also every number of the form  $\alpha x + \beta y$ , where  $x$  and  $y$  are rational integers, is divisible by  $a$ , that is,  $[\alpha, \beta]$  is divisible by  $a$ , etc. Proceeding in this manner we reach the same conclusion that was given in the preceding article.

The following definition at once presents itself:

*Two moduls  $a$  and  $b$  are said to be equal ( $a = b$ ), if  $a$  is divisible by  $b$  and at the same time  $b$  is divisible by  $a$ .*

From this definition are had at once the theorems:

- (1) *Every modul is equal to itself;*
- (2) *if  $a = b$ , then  $b = a$ ;*
- (3) *if  $a = b$ , and  $b = c$ , then also  $a = c$ .*

If  $b$  is divisible by  $a$ , we say the modul  $a$  is a *divisor* of the modul  $b$  and that the modul  $b$  is a *multiple* of the modul  $a$ ; if  $b$  is divisible by  $a$ , but  $a$  is not divisible by  $b$ , we say that  $a$  is a *pure divisor* of  $b$  and that  $b$  is a *pure multiple* of  $a$ . The sign  $b > a$ , which has hitherto not been defined for moduls, denotes that the modul  $b$  is divisible by the modul  $a$  (including equality). From this definition follows the important theorem:

*If  $c > b$  and  $b > a$ , then is also  $c > a$ .*

**ART. 117. The Least Common Multiple of Moduls.** If  $f$  is a modul which is divisible by both the moduls  $a$  and  $b$ , we say that  $f$  is a common multiple of  $a$  and  $b$ ; in this case all numbers of  $f$  appear also in *both*  $a$  and  $b$ . It may be

possible that the moduls  $a$  and  $b$  have still other numbers in common. All numbers that belong to both  $a$  and  $b$  form a modul; for if  $\mu$  and  $\mu'$  are two numbers which are divisible by both  $a$  and  $b$ , then since  $a$  and  $b$  are moduls,  $\mu - \mu'$  is divisible by both  $a$  and  $b$ . The modul  $m$  which consists of all the numbers that are divisible by both  $a$  and  $b$ , is called the *least common multiple* of the moduls  $a$  and  $b$  and is denoted<sup>1</sup> by  $a-b$  or  $b-a$ . Since this relation has nothing to do with the difference of the two moduls, we say *a dash b* and *not a minus b*. Since the modul  $m = a-b = b-a$  consists of all numbers which are divisible by both  $a$  and  $b$ , we have  $m > a$  and  $m > b$ . Note that the aggregate of numbers in  $m$  is less than that in either  $a$  or  $b$  unless one of these moduls is  $m$ . If further  $f$  is a common multiple of  $a$  and  $b$ , that is, a modul which is divisible both by  $a$  and  $b$ , then is  $f > m$ ; hence we say  $m$  is the *least common multiple* of  $a$  and  $b$ .

The modul  $m = a-b = b-a$  is therefore characterized by the two properties, (1) *m is a common multiple of a and b, viz.,  $m > a$  and  $m > b$* ; (2) *every common multiple f of a and b is divisible by m*.

We have at once  $a-a = a$ ; if further  $a > b$ , then is  $a-b = a$ .

The above definition of the least common multiple of two moduls may be at once extended to three or more moduls; if  $a$ ,  $b$ ,  $c$  are three moduls, then *all numbers* which are divisible by  $a$  as well as by  $b$  and  $c$  form a modul  $m$  which we call the *least common multiple* of the three moduls  $a$ ,  $b$  and  $c$ . We then have  $m > a$ ,  $m > b$ ,  $m > c$ . If  $f$  is any modul such that  $f > a$ ,  $f > b$ ,  $f > c$ , then is  $f > m$ .

<sup>1</sup> See Dedekind's *Festschrift: Ueber die Anzahl*, etc. (Braunschweig, 1877). See also Dedekind, Supplement XI of Dirichlet, *Vorlesungen über Zahlentheorie*, Fourth Edition. Reference to this supplement will be made by the word Dedekind.

We have further

$$m = (a - b) - c = a - (b - c) = (a - c) - b,$$

and consequently the sign  $a - b - c$  may be used for  $m$ . If  $a > b$ , then the least common multiple of  $a$ ,  $b$ ,  $c$  is  $a - b - c = a - c$ .

If  $a$  and  $b$  are two moduls whose least common multiple is  $m$ , and if further  $a_1$  and  $b_1$  are two moduls whose least common multiple is  $m_1$  and if  $a > a_1$  and  $b > b_1$ , then is  $m > m_1$ . For if  $\mu$  is an arbitrary number divisible by  $m$ , then since  $m$  is divisible by  $a$  and  $a$  by  $a_1$ , it follows that  $\mu$  is divisible by  $a_1$ ; and since  $m > b$  and  $b > b_1$ , it follows also that  $\mu$  is divisible by  $b_1$ . Hence every number that is divisible by  $m$  is also divisible by both  $a_1$  and  $b_1$ , and such a number is consequently also divisible by  $m_1$ , so that  $m > m_1$ .

If  $a$  and  $b$  are two rational numbers and  $m$  their least common multiple, then is

$$[m] = [a] - [b],$$

for since the rational number  $m$  is divisible by  $a$  and by  $b$ , then every number that is divisible by  $[m]$  is divisible by both  $[a]$  and  $[b]$ ; that is,  $[m]$  is a common multiple of  $[a]$  and  $[b]$ . On the other hand  $[m]$  is the least common multiple of  $[a]$  and  $[b]$ ; for if  $[k]$  is an arbitrary common multiple of  $[a]$  and  $[b]$ , so that  $[k] > [a]$  and  $[k] > [b]$ , then  $k$  is a common multiple of  $a$  and  $b$  and consequently divisible by  $m$ . But if  $k$  is divisible by  $m$ , then is  $[k] > [m]$ , so that  $[m]$  is the least common multiple of  $[a]$  and  $[b]$ .

#### ART. 118. The Greatest Common Divisor of Moduls.

If  $a$ ,  $b$ ,  $f$  are three different moduls and if  $a > f$  and also  $b > f$ , then the modul  $f$  is called a common divisor of  $a$  and  $b$ . Of the three moduls  $f$  consists of the greatest number of numbers; for  $f$  is constituted not only of all



the numbers which constitute  $a$ , but of those also that constitute  $b$  and there may be in addition other numbers that are divisible by  $f$  and which are not divisible by either  $a$  or  $b$ ; that is, all numbers of the form  $\alpha + \beta$  where  $\alpha$  is divisible by  $a$  and where  $\beta$  is divisible by  $b$ , are divisible by  $f$ , and in addition there may be other numbers that are divisible by  $f$  which are not of the form  $\alpha + \beta$ . All numbers of the form  $\alpha + \beta$ , where  $\alpha$  is any number divisible by  $a$ , and  $\beta$  is any number divisible by  $b$ , form a modul; for if  $\delta$  and  $\delta'$  belong to the complex of numbers  $\alpha + \beta$  so that, say,  $\delta = \alpha + \beta$  and  $\delta' = \alpha' + \beta'$ , then  $\delta - \delta' = (\alpha - \alpha') + (\beta - \beta')$  belongs to the same complex, since clearly  $\alpha - \alpha'$  is divisible by  $a$  and  $\beta - \beta'$  is divisible by  $b$ . This modul which is constituted of all numbers of the form  $\alpha + \beta$  we call the *greatest common divisor* of the two moduls  $a$  and  $b$ . We denote it by  $a + b$ . If  $f$  is a modul through which both  $a$  and  $b$  are divisible, that is, a common divisor of  $a$  and  $b$ , then  $a + b > f$ ; for if  $\alpha$  is divisible by  $a$  and  $\beta$  by  $b$ , then  $\alpha$  and  $\beta$  are both divisible by  $f$ , consequently since  $f$  is a modul, it follows (Art. 116) that the sum  $\alpha + \beta$  is divisible by  $f$ . Hence any arbitrary number which has the form  $\alpha + \beta$ , and which in consequence is divisible by  $a + b$ , is divisible by  $f$ , so that  $a + b > f$ .

The greatest common divisor of  $a$  and  $b$ , say  $d = a + b$  is characterized by the two properties:

- (1)  $d$  is a common divisor of  $a$  and  $b$ , so that  $a > d$  and  $b > d$ .
- (2) Every other common divisor, say  $f$ , of  $a$  and  $b$  is a divisor of  $a + b$ , that is  $a + b > f$ .

This denotation of the greatest common divisor of  $a$  and  $b$  through the symbol  $a + b$  has more justification than that of the least common multiple through  $a - b$ , since the modul  $a + b$  consists of all numbers of the form  $\alpha + \beta$ , while the analog for the modul  $a - b$  is *not* true.

ART. 119. If we have to do with finite moduls, the greatest common divisor of two such moduls, say  $[\alpha, \beta, \gamma, \dots, \eta]$  and  $[\alpha', \beta', \gamma', \dots, \eta']$ , is determined through the addition of the two linear forms which represent these moduls; for the modul  $[\alpha, \beta, \gamma, \dots, \eta]$  consists of the collectivity of numbers which are expressed through the form  $\alpha x + \beta y + \gamma z + \dots + \eta w$ , where for the variables  $x, y, z, \dots, w$  rational integers are written, and the modul  $[\alpha', \beta', \dots, \eta']$  consists of those numbers which may be expressed through the linear form  $\alpha'x' + \beta'y' + \gamma'z' + \dots + \eta'w'$ , where rational integers are written for  $x', y', \dots, w'$ . Hence the modul  $[\alpha, \beta, \gamma, \dots, \eta] + [\alpha', \beta', \gamma', \dots, \eta']$  consists of the collectivity of numbers that may be expressed in the form  $\alpha x + \beta y + \gamma z + \dots + \eta w + \alpha'x' + \beta'y' + \gamma'z' + \dots + \eta'w'$ , where the variables are rational integers.

It follows that

$$[\alpha, \beta, \gamma, \dots, \eta] + [\alpha', \beta', \gamma', \dots, \eta'] \\ = [\alpha, \beta, \dots, \eta, \alpha', \beta', \dots, \eta'].$$

If  $a$  and  $b$  are two rational numbers and  $d$  their greatest common divisor, then is

$$[d] = [a] + [b].$$

For the modul  $[d]$  consists of all numbers of the form  $dx$ , the modul  $[a]$  of all numbers of the form  $ay$  and  $[b]$  of all numbers of the form  $bz$ ,  $x, y, z$  being rational integers, and the collectivity of all numbers of the form  $by + cz$  is identical with the collectivity of all numbers of the form  $dx$ , so that

$$[d] = [a] + [b] = [a, b].$$

If  $a$  and  $b$  are two arbitrary moduls and if  $d$  is their greatest common divisor and if further  $a_1$  and  $b_1$  are two other moduls and  $d_1$  is their greatest common divisor; if further  $a > a_1$  and  $b > b_1$ , then is  $d > d_1$ , or in other words,

$a+b > a_1+b_1$ . For if  $\delta$  is an arbitrary number that is divisible by  $b$ , we must have  $\delta = \alpha + \beta$ , where  $\alpha$  is divisible by  $a$  and  $\beta$  is divisible by  $b$ . It follows then that  $\alpha$  is divisible by  $a_1$  and  $\beta$  by  $b_1$  and consequently  $\delta = \alpha + \beta$  is divisible by  $b_1$  so that  $b > b_1$ .

The conception of the *greatest common divisor* may be extended to more than two moduls: If  $a, b, c, \dots$  are moduls, then all numbers of the form  $\alpha + \beta + \gamma + \dots$ , where  $\alpha$  is any number that is divisible by  $a$ ,  $\beta$  any number that is divisible by  $b$ ,  $\gamma$  any number that is divisible by  $c$ , etc., constitute a modul which is called the *greatest common divisor* of the moduls  $a, b, c, \dots$ . This modul is represented by  $a+b+c+\dots$ . This modul  $a+b+c+\dots$  is divisible by every other common divisor of  $a, b, c, \dots$ . We further have for  $a+b+c+\dots$  the same rules as we have for the addition of numbers, viz.:

$$\begin{aligned} a+b+c &= (a+b)+c = c+(a+b) \\ &= a+(b+c) = \text{etc.} \end{aligned}$$

For finite moduls, the modul  $a+b+c+\dots$  represents in reality a sum, viz., the sum of the corresponding linear forms.

ART. 120. If  $a$  and  $b$  are two moduls, we have at once

$$\begin{aligned} a-b &> a, & a-b &> b, \\ a &> a+b, & b &> a+b. \end{aligned}$$

LEMMA. If  $a > a_1$ , and also  $a > b_1$ ; if further  $b > a_1$  and  $b > b_1$ , then is  $a+b > a_1-b_1$ .

For  $a+b > a_1$  and  $a+b > b_1$  and consequently  $a+b > a_1-b_1$ .

From this may be derived the following important theorem:

If  $a, b, m$  are three moduls of which  $m > b$ , then is

$$(a-b)+m = (a+m)-b.$$

In order to prove the equality of two moduls, we must prove that either modul is divisible by the other.

We note that

$$\begin{aligned} a - \delta &> a > a + m \\ a - \delta &> \delta \\ m &> a + m \\ m &> \delta. \end{aligned}$$

From the above lemma

$$(a - \delta) + m > (a + m) - \delta. \quad (i)$$

On the other hand let  $\eta$  be a number divisible by the modul  $(a + m) - \delta$ , then is  $\eta$  divisible by  $a + m$  and further  $\eta$  is divisible by  $\delta$ . Hence  $\eta = \alpha + \mu$  where  $\alpha$  is divisible by  $a$  and  $\mu$  by  $m$ ; further since  $\eta$  is divisible by  $\delta$ , it is seen that  $\eta = \delta$  where  $\delta$  is a number divisible by the modul  $\delta$ . It follows that

$$\eta = \alpha + \mu = \delta \quad \text{or} \quad \alpha = \delta - \mu.$$

Since  $\delta$  is divisible by  $\delta$  and  $\mu$  by  $m$ , and as by hypothesis  $m$  is divisible by  $\delta$ , we note that  $\mu$  is divisible by  $\delta$ . Hence  $\delta - \mu$  is divisible by  $\delta$ , that is,  $\alpha$  is divisible by  $\delta$ , and since  $\alpha$  is divisible by  $a$ , it is seen that the modul to which  $\alpha$  belongs is a common multiple of  $a$  and  $\delta$  and consequently is divisible by the least common multiple of  $a$  and  $\delta$ , that is by  $a - \delta$ . Hence the number  $\eta = \alpha + \mu$  is divisible by  $(a - \delta) + m$ ; and since this is true of every number  $\eta$  of the modul  $(a + m) - \delta$ , it follows that

$$(a + m) - \delta > (a - \delta) + m. \quad (ii)$$

We therefore have from (i) and (ii)

$$(a - \delta) + m = (a + m) - \delta,$$

where  $m > \delta$  (cf. Dedekind, § 169).

**ART. 121. Multiplication of Moduls by Algebraic Integers.** If  $a$  is a modul whose elements belong to  $\Omega$  and  $\eta$  an arbitrary number of this same realm, then the complex of numbers  $\alpha\eta$ , where for  $\alpha$  is written every

number that is divisible by  $a$ , forms a modul; for if  $\alpha\eta$  and  $\alpha'\eta$  are two numbers of this complex, then the difference  $\alpha\eta - \alpha'\eta = (\alpha - \alpha')\eta$  belongs to this complex. This modul, which is formed of the numbers  $\alpha\eta$ , we call the product of the modul  $a$  and the number  $\eta$ . We denote it by

$$a\eta = \eta a.$$

It is also evident, if  $\eta'$  is another number of the realm  $\Omega$ , that

$$(a\eta)\eta' = a(\eta\eta').$$

If  $a$  is a finite modul, say  $a = [\alpha_1, \alpha_2, \dots, \alpha_n]$ , then is

$$a\eta = [\alpha_1\eta, \alpha_2\eta, \dots, \alpha_n\eta];$$

for the modul  $a = [\alpha_1, \alpha_2, \dots, \alpha_n]$  consists of all numbers of the form  $\alpha_1x + \alpha_2y + \alpha_3z + \dots + \alpha_nw$ , where  $x, y, z, \dots, w$  take all rational integral values, and the modul  $a\eta$  consists of all numbers of the form  $\alpha_1\eta x + \alpha_2\eta y + \alpha_3\eta z + \dots + \alpha_n\eta w$  for rational integral values of  $x, y, z, \dots, w$ . (Dedekind, § 170.)

If the modul  $b$  is divisible by the modul  $a$ , then is the modul  $\eta b$  divisible by the modul  $\eta a$ . For if  $\eta\beta$  is any number divisible by the modul  $\eta b$ , then is  $\beta$  divisible by  $b$ , and consequently since  $b > a$  it follows that  $\beta$  is divisible by  $a$ ; hence also  $\eta\beta > \eta a$  and therefore  $\eta b > \eta a$ . If reciprocally  $\eta b$  is divisible by  $\eta a$ , then from what we just had,  $\eta^{-1}\eta b$  is divisible by  $\eta^{-1}\eta a$ , and consequently  $b > a$ .

If  $\eta b = \eta a$ , then  $b = a$  and if  $b = a$ , then is  $\eta b = \eta a$ . If  $m$  is the *least common multiple* of  $a$  and  $b$ , we have

$$\eta m = \eta(a - b) = \eta a - \eta b.$$

For if  $\mu$  is a number that is divisible by  $m$ , then  $\mu$  is divisible by both  $a$  and  $b$ ; and  $\eta\mu$ , an arbitrary number divisible by  $\eta m$ , is divisible by  $\eta a$  and  $\eta b$ , and consequently by  $\eta a - \eta b$ . Reciprocally, every number that is divisible by  $\eta a$  and also by  $\eta b$ , is divisible by  $\eta m$ ; for every number that is divisible by  $a$  and also by  $b$  is divisible by  $m$ .



If  $\delta = a + b$ , then is

$$\eta\delta = \eta(a + b) = \eta a + \eta b;$$

for the modul  $\delta$  consists of all numbers of the form  $\alpha + \beta$ , where for  $\alpha$  is written all numbers divisible by  $a$  and for  $\beta$  all numbers that are divisible by  $b$ . The modul  $\eta\delta$  consists therefore of all numbers of the form

$$\eta(\alpha + \beta) = \eta\alpha + \eta\beta.$$

In an analogous manner we have

$$\eta(a + b + c) = \eta a + \eta b + \eta c$$

and

$$\eta(a - b - c) = \eta a - \eta b - \eta c,$$

etc.

**ART. 122. The Product of Moduls.** If the product of two moduls  $a$  and  $b$  were defined simply as the complex of numbers  $\alpha\beta$  where for  $\alpha$  are written all numbers divisible by  $a$  and for  $\beta$  are written all numbers divisible by  $b$ , it is seen that this complex is *not* a modul; for  $\alpha\beta - \alpha'\beta'$  is not of the form  $\alpha''\beta''$ . Accordingly a definition as follows must be offered:

*The product  $ab$  is the complex of those numbers which are had if we sum in all possible manners the products of the form  $\alpha \cdot \beta$ , where for  $\alpha$  are written all numbers divisible by  $a$  and for  $\beta$  all numbers that are divisible by  $b$ ; that is, the product  $a \cdot b$  is the complex of all possible numbers of the form*

$$\sum_{(0)} \alpha^{(i)}\beta^{(i)} = \alpha^{(1)}\beta^{(1)} + \alpha^{(2)}\beta^{(2)} + \alpha^{(3)}\beta^{(3)} + \dots,$$

where  $\alpha^{(1)}, \alpha^{(2)}, \dots$  individually run through all the numbers that are divisible by  $a$ , and for each of the quantities  $\alpha^{(i)}$  the quantity  $\beta^{(i)}$  goes through all numbers that are divisible by  $b$ .

In other words, if  $a = (\alpha_1, \alpha_2, \alpha_3, \dots)$ , and if  $\alpha^{(i)}$  is any number that is divisible by  $a$ , then  $\alpha^{(i)}$  may be added as

an element, so that

$$a = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha^{(i)}, \dots);$$

and similarly

$$b = (\beta_1, \beta_2, \beta_3, \dots, \beta^{(j)}, \dots).$$

Hence in the product  $ab$ , every number of the form  $\alpha^{(i)}\beta^{(j)}$  is found.

Note that the difference of any two numbers of the complex is again a number of the complex. The product  $a \cdot b$  may be regarded as the greatest common divisor of all the moduls which are had if the modul  $b$  is multiplied by all possible numbers that are divisible by  $a$ , that is

$$a \cdot b = \alpha^{(1)}b + \alpha^{(2)}b + \alpha^{(3)}b + \dots,$$

when for  $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}, \dots$ , are written all possible numbers that are divisible by  $a$ ; for if  $\alpha^{(1)}\beta^{(1)}$  is any number divisible by  $\alpha^{(1)}b$ , and if  $\alpha^{(2)}\beta^{(2)}$  is any number divisible by  $\alpha^{(2)}b$ , etc., then is  $\alpha^{(1)}\beta^{(1)} + \alpha^{(2)}\beta^{(2)} + \dots$  a number divisible by  $\alpha^{(1)}b + \alpha^{(2)}b + \dots$ , which modul is also divisible by  $a \cdot b$ ; and reciprocally every number that is divisible by  $a \cdot b$  may be expressed in the form

$$\alpha^{(1)}\beta^{(1)} + \alpha^{(2)}\beta^{(2)} + \dots.$$

ART. 123. As a special case, suppose that the modul  $a$  is *finite*,<sup>1</sup> say

$$a = [\alpha_1, \alpha_2, \dots, \alpha_n];$$

we then have

$$a \cdot b = \alpha_1 b + \alpha_2 b + \dots + \alpha_n b.$$

In other words, we have the product of the moduls  $a \cdot b$ , if we take all possible moduls  $\alpha b$ , where for  $\alpha$  are written only the  $n$  numbers  $\alpha_1, \alpha_2, \dots, \alpha_n$  which form a basis of  $a$ , and *not* necessarily *all* the numbers that are divisible by  $a$ . The product  $a \cdot b$  (where  $a$  is a finite modul) is the greatest common divisor of the  $n$  moduls  $\alpha_1 b, \alpha_2 b, \dots$ ,

<sup>1</sup> The simplest case is when one of the moduls is  $\mathfrak{z}$ , the complex of all rational integers. In this case  $\mathfrak{z}a = a$ , where  $a$  is any modul. If further  $\mathfrak{f}a = a$ , where  $\mathfrak{f}$  is a modul and  $a$  any modul, then is  $\mathfrak{f} = \mathfrak{z}$ .

$\alpha_n \mathfrak{b}$ ; for if  $\lambda$  is a number that is divisible by  $\mathfrak{a}\mathfrak{b}$ , then is

$$\lambda = \alpha^{(1)}\beta^{(1)} + \alpha^{(2)}\beta^{(2)} + \dots,$$

where all the numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots$ , are divisible by  $\mathfrak{a}$ . They may therefore be written in the form

$$\alpha^{(1)} = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n,$$

$$\alpha^{(2)} = \alpha_1 x'_1 + \alpha_2 x'_2 + \dots + \alpha_n x'_n,$$

etc. It follows that

$$\begin{aligned} \lambda &= \alpha_1(x_1\beta^{(1)} + x'_1\beta^{(2)} + \dots) + \alpha_2(x_2\beta^{(1)} + x'_2\beta^{(2)} + \dots) + \dots \\ &= \alpha_1\eta_1 + \alpha_2\eta_2 + \dots, \end{aligned}$$

where the  $\eta$ 's are divisible by the modul  $\mathfrak{b}$ . The number  $\alpha_1\eta_1$  is divisible by the modul  $\alpha_1\mathfrak{b}$ , the number  $\alpha_2\eta_2$  is divisible by the modul  $\alpha_2\mathfrak{b}$ , etc. Hence  $\lambda$  is divisible by the greatest common divisor of  $\alpha_1\mathfrak{b}, \alpha_2\mathfrak{b}, \dots$ , that is by  $\alpha_1\mathfrak{b} + \alpha_2\mathfrak{b} + \dots + \alpha_n\mathfrak{b}$ . *Reciprocally*, every number that is divisible by  $\alpha_1\mathfrak{b} + \alpha_2\mathfrak{b} + \dots + \alpha_n\mathfrak{b}$  has the form

$$\alpha_1\eta_1 + \alpha_2\eta_2 + \dots + \alpha_n\eta_n,$$

where  $\eta_1, \eta_2, \dots, \eta_n$  are numbers that are divisible by  $\mathfrak{b}$ . It follows that each of the numbers  $\alpha_1\eta_1, \alpha_2\eta_2, \dots, \alpha_n\eta_n$  is divisible by  $\mathfrak{a}\mathfrak{b}$  and consequently the sum of these numbers is divisible by  $\mathfrak{a}\mathfrak{b}$ .

Having shown that each of the two moduls  $\mathfrak{a}\mathfrak{b}$  and  $\alpha_1\mathfrak{b} + \alpha_2\mathfrak{b} + \dots + \alpha_n\mathfrak{b}$  is divisible by the other, it follows that

$$\mathfrak{a}\mathfrak{b} = \alpha_1\mathfrak{b} + \alpha_2\mathfrak{b} + \dots + \alpha_n\mathfrak{b}.$$

If then  $\alpha_1, \alpha_2, \dots, \alpha_n$  is a basis of the finite modul  $\mathfrak{a}$ , then the modul  $\mathfrak{a}\mathfrak{b}$  consists of the collectivity of numbers which are expressed through

$$\alpha_1\eta_1 + \alpha_2\eta_2 + \dots + \alpha_n\eta_n,$$

where the variables  $\eta_1, \eta_2, \dots, \eta_n$  are all the possible numbers that are divisible by  $\mathfrak{b}$ .

ART. 124. As a still more special case, suppose that both the moduls  $\mathfrak{a}$  and  $\mathfrak{b}$  are finite, say

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_r],$$

$$\mathfrak{b} = [\beta_1, \beta_2, \dots, \beta_s],$$

then is

$$\mathfrak{a}\mathfrak{b} = [\alpha_1\beta_1, \alpha_1\beta_2, \dots, \alpha_1\beta_s, \alpha_2\beta_1, \alpha_2\beta_2, \dots, \alpha_2\beta_s, \dots, \alpha_r\beta_s];$$

for if  $\mathfrak{a}$  is a finite modul, then all numbers divisible by  $\mathfrak{a} \cdot \mathfrak{b}$  may be expressed through

$$\alpha_1\eta_1 + \alpha_2\eta_2 + \dots + \alpha_r\eta_r,$$

where  $\eta_1, \eta_2, \dots, \eta_r$  are all numbers that are divisible by  $\mathfrak{b}$ . Since  $\mathfrak{b}$  is also finite, we have

$$\eta_\nu = \beta_1x_{\nu 1} + \beta_2x_{\nu 2} + \dots + \beta_sx_{\nu s} \quad (\nu = 1, 2, \dots, r).$$

It follows that

$$\alpha_1\eta_1 + \alpha_2\eta_2 + \dots + \alpha_r\eta_r = \alpha_1\beta_1x_{11} + \alpha_1\beta_2x_{12} + \dots + \alpha_r\beta_sx_{rs}.$$

The quantities  $\alpha_1\beta_1, \alpha_1\beta_2, \dots, \alpha_1\beta_s$  do not necessarily form a basis of  $\mathfrak{a}\mathfrak{b}$ , as this basis may consist of fewer than  $r \cdot s$  elements; that is, the order of  $\mathfrak{a} \cdot \mathfrak{b}$  may be less than  $r \cdot s$ . It is evident that if  $\alpha_1\beta_1$  could be expressed linearly in the form

$$\alpha_1\beta_1 = x_2\alpha_2\beta_2 + x_3\alpha_3\beta_3 + \dots,$$

where the  $x$ 's are rational integers, then  $\alpha_1\beta_1$  could be dropped as an element of the basis on the right hand side.

ART. 125. The conception of the *product* may be extended to more than two moduls. If  $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$  are several moduls, then by uniting always a number of the modul  $\mathfrak{a}$  with a number of the modul  $\mathfrak{b}$  with a number of the modul  $\mathfrak{c}$  into a product and making a summation of all possible products of this kind, we have the complex of numbers

$$\begin{aligned} \sum \alpha^{(i)}\beta^{(i)}\gamma^{(i)} \dots &= \alpha^{(1)}\beta^{(1)}\gamma^{(1)} + \dots \\ &+ \alpha^{(2)}\beta^{(2)}\gamma^{(2)} + \dots + \alpha^{(3)}\beta^{(3)}\gamma^{(3)} + \dots + \dots, \end{aligned}$$

where  $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}, \dots$  are all possible numbers divisible by  $a$ , and also the quantity  $\beta^{(i)}$  goes through all possible numbers divisible by  $b$ , while  $\gamma^{(i)}$  goes through all possible numbers divisible by  $c, \dots$ . This complex of numbers forms a modul, since the difference of two numbers of the form  $\sum \alpha\beta\gamma \dots$  has again this form; it is called the *product* of the moduls  $a, b, c, \dots$  and denoted by  $abc \dots$ , or by  $bac \dots$ , or by  $cab \dots$ , etc.

For the multiplication of moduls as thus defined the two fundamental principles of multiplication as seen for example in rational numbers are also true, namely the commutative and associative principles. For it is evident that

$$\begin{aligned} ab &= ba \\ abc &= (ab)c = a(bc). \end{aligned}$$

From these fundamental principles of multiplication arise at once the other principles of multiplication, in particular uniqueness in raising to a power, which is due to the associative and *not* to the commutative principle; for in raising to a power the factors are all equal and consequently *eo ipso* interchangeable. We define  $a^n$  where  $n$  is a positive integer  $\neq 0$  as the product of  $n$  moduls of which each one is equal to  $a$ , that is

$$a^n = a \cdot a \cdot a \cdot \dots \cdot a.$$

From the associative principle follows the important theorem

$$a^r \cdot a^s = a^{r+s} \quad (r, s > 0);$$

and from the commutative principle we have

$$a^r b^r = (ab)^r \quad (r > 0).$$

*Remark.* A product of several moduls cannot  $= 0$  unless at least one of the factors is 0; for if  $abc = 0$  and if  $a \neq 0, b \neq 0, c \neq 0$ , then in  $a$  there is a number  $\alpha \neq 0$ , in  $b$  there is a number  $\beta \neq 0$ , and in  $c$  there is a number  $\gamma \neq 0$  and consequently there is in  $abc$  a number  $\alpha\beta\gamma \neq 0$  which contradicts the hypothesis that  $abc = 0$ .



ART. 126. If  $\alpha$  is a number divisible by  $a$  and  $\beta$  is a number divisible by  $b$ , then it follows from the definition of  $ab$  that the number  $\alpha\beta$  is divisible by  $ab$ . This may be generalized into the following:

THEOREM. *If  $a > a_1$  and  $b > b_1$ , then is  $ab > a_1b_1$ .*

For since  $a > a_1$ , every arbitrary number  $\alpha$  that is divisible by  $a$  is also divisible by  $a_1$ , and since  $b > b_1$ , every arbitrary number  $\beta$  that is divisible by  $b$  is also divisible by  $b_1$ . It follows that  $\alpha\beta$  is divisible by  $a_1b_1$ . If further  $\alpha'$  is another number divisible by  $a$  and  $\beta'$  is another number divisible by  $b$ , then also  $\alpha'\beta'$  is divisible by  $a_1b_1$ , etc. We thus see that all numbers of the form

$$\sum \alpha\beta = \alpha\beta + \alpha'\beta' + \alpha''\beta'' + \dots$$

are divisible by  $a_1b_1$ , but all these numbers constitute the modul  $ab$ . We therefore have

$$ab > a_1b_1.$$

The following special case may be noted:<sup>1</sup>

If  $b > a$ , then is  $bc > ac$ .

The inverse of this theorem is *not* true in general, viz., if  $bc > ac$ , then it does not follow that  $b > a$ . If  $a = [1]$  and  $a_1 = [i]$ , where  $i^2 = -1$ , and  $b = [1, i]$ , then is  $ab = b = a_1b$  and consequently  $ab > a_1b$ ; but  $a$  is *not* divisible by  $a_1$ .

The conclusion that if  $bc > ac$ , then is  $b > a$  can only be drawn if  $c$  is a one-term modul equal to, say,  $[\eta]$ . If  $b[\eta] > a[\eta]$ , then is  $b > a$ ; for  $b[\eta] = b\eta$  and  $a[\eta] = a\eta$  and if  $b\eta > a\eta$ , then is  $b\eta\eta^{-1} > a\eta\eta^{-1}$  or  $b > a$ .

We observe in general that a product of moduls is *not* divisible by one of the factors; that is the modul  $ab$  is in general divisible by *neither*  $a$  nor  $b$ . The analogous theorem is true for rational integers but it is *not* true for

<sup>1</sup> Observe that  $a > ab$ , if  $\mathfrak{z} > b$ , since  $\mathfrak{z}a > ab$ , and  $\mathfrak{z}a = a$ , where the modul  $\mathfrak{z}$  consists of the collectivity of rational integers.

rational fractional numbers, for  $\frac{8}{3} \cdot \frac{9}{4} = 6$  although 6 is divisible by neither of these factors.

ART. 127. If  $a, b, c$  are three moduls and if  $d = a + b$ , then is

$$dc = (a + b)c = ac + bc.$$

*Proof:*

$$\begin{array}{ll} a > b & b > c \\ c > c & c > c \\ \therefore ac > bc & \therefore bc > bc. \end{array}$$

Since both  $ac$  and  $bc$  are divisible by  $bc$ , it follows that (1)  $ac + bc > bc$ .

On the other hand let  $\gamma$  be a number divisible by  $c$  and  $\delta$  a number divisible by  $b$  so that also  $\delta = \alpha + \beta$  where  $\alpha$  is divisible by  $a$  and  $\beta$  by  $b$ . We note also that  $\alpha\gamma$  is divisible by  $ac$  and  $\beta\gamma$  by  $bc$  and consequently  $\alpha\gamma + \beta\gamma = \delta\gamma$  is divisible by  $ac + bc$ . Similarly  $\delta'\gamma'$  is divisible by  $ac + bc$  if  $\delta'$  is divisible by  $b$  and  $\gamma'$  by  $c$ , etc. It follows that  $\gamma\delta + \gamma'\delta' + \dots = \sum \gamma\delta$ , which is any arbitrary number divisible by  $bc$ , is divisible by  $ac + bc$ . Hence also (2)  $cb > ac + bc$ , and from (1) and (2),

$$dc = ac + bc.$$

This may easily be extended to the following (Dedekind, § 170):

$$\begin{aligned} (a + b)(a_1 + b_1) &= (a + b)b_1 \\ &= ab_1 + bb_1 \\ &= a(a_1 + b_1) + b(a_1 + b_1) \\ &= aa_1 + ab_1 + a_1b + bb_1. \end{aligned}$$

We have at once

$$(a + b)^2 = a^2 + ab + b^2,$$

since

$$ab + ab = ab.$$

We further have the following important relations for three moduls,  $a, b, c$ :

$$(b + c)(c + a)(a + b) = (a + b + c)(ab + bc + ca),$$



and consequently

$$(\alpha - \beta)c > ac \quad (\alpha - \beta)c > bc.$$

It follows that  $(\alpha - \beta)c$  is divisible by the least common multiple of  $ac$  and  $bc$ , or

$$(\alpha - \beta)c > ac - bc.$$

If  $a$  and  $b$  are two moduls and if  $d = a + b$  and  $m = a - b$ , then is

$$md > ab,$$

or

$$(\alpha - \beta)(\alpha + \beta) > ab.$$

For if  $\delta$  is a number divisible by  $d$ , then is  $\delta = \alpha + \beta$ , where  $\alpha$  is a number divisible by  $a$  and  $\beta$  is a number divisible by  $b$ ; and if  $\mu$  is a number divisible by  $m$ , then is  $\mu = \alpha_1 - \beta_1$ , where  $\alpha_1$  is divisible by  $a$  and  $\beta_1$  by  $b$ .

It follows that

$$\mu\delta = (\alpha + \beta)\mu = \alpha\mu + \beta\mu = \alpha\beta_1 + \beta\alpha_1,$$

where  $\alpha\beta_1$  and  $\beta\alpha_1$  are both divisible by  $ab$  and consequently every number of the form

$$\mu^{(1)}\delta^{(1)} + \mu^{(2)}\delta^{(2)} + \mu^{(3)}\delta^{(3)} + \dots = \sum \mu^{(i)}\delta^{(i)}$$

is divisible by  $ab$ . The equality

$$md = ab$$

is in general *not* true as in the analogous case of rational integers.

**ART. 129. The Quotient of Moduls.** To define the quotient of two moduls, consider first the quotient  $\frac{b}{a}$  where  $a$  is an arbitrary number. It is evident that the modul  $a^{-1}b$  is the aggregate of all those numbers  $\kappa$  which are divisible by  $\frac{1}{a}b$ ; or better expressed,  $a^{-1}b$  is the aggregate of all those numbers  $\kappa$  which are such that  $\kappa a$  is divisible by  $b$ . In an analogous manner we define  $\frac{b}{a}$

as the *aggregate of all numbers  $\kappa$  which have the property that  $\kappa a$  is divisible by  $b$* .

The aggregate of numbers thus defined is a modul; for if  $\kappa$  and  $\kappa'$  are two arbitrary numbers that are divisible by  $\frac{b}{a}$  so that  $\kappa a > b$  and  $\kappa' a > b$ , and if  $\alpha$  is a number divisible by  $a$ , then are  $\kappa \alpha$  and  $\kappa' \alpha$  both divisible by  $b$  and consequently also  $(\kappa - \kappa') \alpha$  is divisible by  $b$ ; and this is true of all numbers  $\alpha$  that are divisible by  $a$ . It follows that  $\kappa - \kappa'$  belongs to the aggregate  $\frac{b}{a}$ .

This modul  $\frac{b}{a}$  is called the *quotient* of the two moduls  $b$  and  $a$ .

The characteristic properties of the modul  $\frac{b}{a}$  are the following:

- (1) *If  $\kappa$  is a quantity divisible by  $\frac{b}{a}$ , then is  $\kappa a > b$ ;*
- (2) *if  $\kappa a > b$ , then is  $\kappa > \frac{b}{a}$ .*

This definition of the quotient of moduls is also expressed through the following two important theorems:

**THEOREM I.** *If  $a, b, f$  are three arbitrary moduls and if  $fa > b$ , then is also  $f > \frac{b}{a}$ .*

For if  $\kappa$  is a number that is divisible by  $f$ , then is  $\kappa a > fa$ ; if further  $fa > b$  then is  $\kappa a > b$  and consequently every number  $\kappa$  that is divisible by  $f$ , in view of the definition given above of the quotient  $\frac{b}{a}$ , is divisible by  $\frac{b}{a}$  and consequently  $f$  is divisible by  $\frac{b}{a}$ .



**THEOREM II.** *If  $f > \frac{b}{a}$ , then is also  $fa > b$ .*

For if  $f > \frac{b}{a}$  and if  $\kappa$  is an arbitrary number divisible by  $f$ , then is  $\kappa$  divisible by  $\frac{b}{a}$ ; or in accordance with the definition given above of  $\frac{b}{a}$ , it follows that  $\kappa a > b$  and similarly also  $\kappa' a > b$  where  $\kappa'$  is a number divisible by  $f$ , and consequently also the sum

$$\kappa a + \kappa' a + \dots > b;$$

and that is, due to the definition of multiplication,

$$fa > b.$$

*Remark.* Since every modul is divisible by itself, we have  $\frac{b}{a} > \frac{b}{a}$  so that  $\frac{b}{a} \cdot a > b$ . The equality of these two moduls in general does *not* follow.

**ART. 130.** Theorems I and II of the preceding article may be expressed as follows:

*The quotient  $\frac{b}{a}$  is the least common multiple of all those moduls  $f$  which have the property that  $fa > b$ .*

We may consider first this theorem for the case where the denominator  $a$  is a one-term modul  $[\alpha]$ .

We assert that

$$\frac{b}{[\alpha]} = \frac{b}{\alpha}.$$

For if  $\kappa$  is a number that is divisible by  $\frac{b}{\alpha}$ , then  $\kappa\alpha$  and consequently  $\kappa\alpha x$  is divisible by  $b$ , where  $x$  is a rational integer; or  $\kappa[\alpha]$  is divisible by  $b$ , or finally  $\kappa$  is divisible by  $\frac{b}{[\alpha]}$ , so that (1)  $\frac{b}{\alpha} > \frac{b}{[\alpha]}$ .

Reciprocally, if  $\kappa$  is divisible by  $\frac{b}{[\alpha]}$ , then is  $\kappa[\alpha] > b$  and consequently  $\kappa\alpha x$ , where  $x$  is a rational integer, is divisible by  $b$ . It follows also when  $x=1$ , that  $\kappa\alpha$  is divisible by  $b$  so that  $\kappa$  is divisible by  $\frac{b}{\alpha}$ , or (2)  $\frac{b}{[\alpha]} > \frac{b}{\alpha}$ . From (1) and (2) we have

$$\frac{b}{[\alpha]} = \frac{b}{\alpha}.$$

If *next*  $a$  is a finite modul, equal, say, to  $[\alpha_1, \alpha_2, \dots, \alpha_n]$ , then is

$$a = [\alpha_1] + [\alpha_2] + \dots + [\alpha_n].$$

We assert that

$$\frac{b}{a} = \alpha_1^{-1}b - \alpha_2^{-1}b - \alpha_3^{-1}b - \dots - \alpha_n^{-1}b = m,$$

say. Note that the least common multiple  $m$  of the moduls  $\frac{1}{\alpha_\nu}b$  ( $\nu=1, 2, \dots, n$ ) is such that

$$m > \frac{1}{\alpha_\nu}b \quad (\nu=1, 2, \dots, n).$$

If  $\mu$  is a number divisible by  $m$ , then is  $\mu$  divisible by  $\frac{1}{\alpha_\nu}b$ , and consequently  $\mu\alpha_\nu$  is divisible by  $b$  ( $\nu=1, 2, \dots, n$ ).

We denote by  $x_1, x_2, \dots, x_n$ ,  $n$  rational integers. It is evident that  $\mu\alpha_1x_1, \mu\alpha_2x_2, \dots, \mu\alpha_nx_n$  and consequently also  $\mu[\alpha_1x_1 + \alpha_2x_2 + \dots + \alpha_nx_n]$  is divisible by  $b$ . It follows that  $\mu a$  is divisible by  $b$ , or (1)  $m > \frac{b}{a}$ .

Reciprocally, let  $\kappa$  be an arbitrary number divisible by  $\frac{b}{a}$ , so that  $\kappa a > b$ . It follows that the quantities  $\kappa\alpha_1, \kappa\alpha_2, \dots, \kappa\alpha_n$  are all divisible by  $b$ . Hence the quantity  $\kappa$  is

divisible by  $\frac{b}{\alpha_1}$  as well as by  $\frac{b}{\alpha_2}, \dots$ , as well as by  $\frac{b}{\alpha_n}$ , and consequently also by the least common multiple  $m$  of these moduls. Since this is true for every number  $\kappa$  that is divisible by  $\frac{b}{a}$ , it follows that (2)  $\frac{b}{a} > m$ . From (1) and (2) we have

$$\frac{b}{a} = m = \frac{1}{\alpha_1}b - \frac{1}{\alpha_2}b - \frac{1}{\alpha_3}b - \dots - \frac{1}{\alpha_n}b.$$

In the same way the following may be proved for moduls which are not finite:

*The modul  $\frac{b}{a}$  is the least common multiple of all moduls of the form  $\alpha^{-1}b$ , when for  $\alpha$  are written all numbers that are divisible by  $a$ .*

ART. 131. It is well to consider next certain formulas relative to the quotients of moduls.

FORMULA I. *If  $b > b_1$  and  $a_1 > a$ , then is*

$$\frac{b}{a} > \frac{b_1}{a_1} \quad \text{and} \quad \frac{a_1}{b_1} > \frac{a}{b}.$$

For write  $f = \frac{b}{a}$ , so that  $fa > b$ ; then is  $fa > b_1$ . Since however  $fa_1 > fa$ , it follows that  $fa_1 > b_1$ , or  $f > \frac{b_1}{a_1}$ .

FORMULA II. *If  $a, b, c$  are three moduls, then is*

$$\frac{b}{a} > \frac{bc}{ac}.$$

For

$$\frac{b}{a} \cdot a > b,$$

$$c > c;$$

therefore

$$\frac{b}{a} \cdot a \cdot c > bc,$$

or

$$\frac{b}{a} > \frac{bc}{ac}.$$

FORMULA III.

$$\frac{b}{a} \cdot \frac{b_1}{a_1} > \frac{bb_1}{aa_1}.$$

For  $\frac{b}{a} > b$  and  $\frac{b_1}{a_1} > b_1$ , so that  $\frac{b}{a} \frac{b_1}{a_1} > bb_1$ . It follows that

$$\frac{b}{a} \cdot \frac{b_1}{a_1} aa_1 > bb_1,$$

or

$$\frac{b}{a} \cdot \frac{b_1}{a_1} > \frac{bb_1}{aa_1}.$$

In the case of Formula II, if  $c$  is a one-term modul  $= [\eta]$ , say, we have the *equality*

$$\frac{b[\eta]}{a[\eta]} = \frac{b\eta}{a\eta} = \frac{b}{a}.$$

For  $\frac{b\eta}{a\eta} > b\eta$ , or  $\frac{b\eta}{a\eta} > b$ , or (1)  $\frac{b\eta}{a\eta} > \frac{b}{a}$ .

On the other hand, from Formula II we have

$$(2) \quad \frac{b}{a} > \frac{b\eta}{a\eta}.$$

From (1) and (2) it follows that

$$\frac{b}{a} = \frac{b\eta}{a\eta} = \frac{b[\eta]}{a[\eta]}.$$

Further, if in Formula III, we put  $b_1 = [\lambda]$  and  $a_1 = [\kappa]$ , we have

$$\frac{b}{a} \cdot \frac{[\lambda]}{[\kappa]} = \frac{b[\lambda]}{a[\kappa]}.$$

For  $\frac{b[\lambda]}{a[\kappa]} > b[\lambda]$ , so that

$$\frac{b[\lambda]}{a[\kappa]} > \frac{b[\lambda]}{[\kappa]} \left( = \frac{b\lambda}{\kappa} = b \cdot \frac{\lambda}{\kappa} \text{ (Art. 121)} \right),$$

and consequently

$$(1) \quad \frac{b[\lambda]}{a[\kappa]} > \frac{b}{a} \cdot \frac{[\lambda]}{[\kappa]}.$$

But from Formula III, we have (2)  $\frac{b}{a} \cdot \frac{[\lambda]}{[\kappa]} > \frac{b[\lambda]}{a[\kappa]}$ , and from (1) and (2) it follows that the two expressions are equal.

FORMULA IV.

$$\frac{c}{b} : a = \frac{c}{ba}.$$

For  $\frac{c}{ba}ba > c$ , or  $\left(\frac{c}{ba}a\right)b > c$ , or  $\frac{c}{ba}a > \frac{c}{b}$  or (1)  $\frac{c}{ba} > \frac{c}{b} : a$ .

On the other hand

$$\left(\frac{c}{b} : a\right)a > \frac{c}{b}$$

and

$$\left(\frac{c}{b} : a\right)ab > \frac{c}{b}b > c,$$

so that

$$(2) \quad \frac{c}{b} : a > \frac{c}{ab},$$

and from (1) and (2) we have the equality desired.

FORMULA V. *If m is the least common multiple of the two moduls a and b, then is  $\frac{m}{c}$  the least common multiple of  $\frac{a}{c}$  and  $\frac{b}{c}$ , and that is*

$$\frac{m}{c} = \frac{a-b}{c} = \frac{a}{c} - \frac{b}{c}.$$

For

$$\begin{array}{ccc} m > a & \text{and} & m > b \\ c > c & & c > c. \end{array}$$

Hence from Formula I

$$\frac{m}{c} > \frac{a}{c} \quad \text{and} \quad \frac{m}{c} > \frac{b}{c},$$



and therefore

$$(1) \quad \frac{m}{c} > \frac{a}{c} - \frac{b}{c}.$$

On the other hand

$$\frac{a}{c} - \frac{b}{c} > \frac{a}{c} \quad \text{and} \quad \frac{a}{c} - \frac{b}{c} > \frac{b}{c},$$

so that

$$\left(\frac{a}{c} - \frac{b}{c}\right)c > a \quad \text{and} \quad \left(\frac{a}{c} - \frac{b}{c}\right)c > b.$$

Hence

$$\left(\frac{a}{c} - \frac{b}{c}\right)c > a - b,$$

or

$$(2) \quad \left(\frac{a}{c} - \frac{b}{c}\right) > \frac{m}{c}.$$

From (1) and (2) follows the equality of the two expressions.

FORMULA VI. *The least common multiple of  $\frac{c}{a}$  and  $\frac{c}{b}$  is  $\frac{c}{\delta}$  where  $\delta = a + b$ , or  $\frac{c}{a} - \frac{c}{b} = \frac{c}{a + b}$ .*

For let  $m_1 = \frac{c}{a} - \frac{c}{b}$ , then since  $c > c$  and  $a > b$ , it follows from Formula I that  $\frac{c}{\delta} > \frac{c}{a}$  and similarly  $\frac{c}{\delta} > \frac{c}{b}$ . It follows that

$$(1) \quad \frac{c}{\delta} > m_1.$$

On the other hand

$$m_1 > \frac{c}{a} \quad \text{and} \quad m_1 > \frac{c}{b},$$

so that

$$m_1 a > c \quad \text{and} \quad m_1 b > c.$$

It follows that  $m_1 a + m_1 b > c$ ; and since

$$m_1 a + m_1 b = m_1 (a + b) = m_1 \delta,$$

we have  $m_1 b > c$ , or

$$(2) \quad m_1 > \frac{c}{b}.$$

From (1) and (2) follows the equality desired.

FORMULA VII. *The greatest common divisor of  $\frac{a}{a_1}$  and  $\frac{b}{b_1}$  is divisible by  $\frac{a+b}{a_1-b_1}$ , that is  $\frac{a}{a_1} + \frac{b}{b_1} > \frac{a+b}{a_1-b_1}$ .*

For

$$\begin{array}{l} a > a+b \quad \text{and} \quad b > a+b \\ a_1 - b_1 > a_1 \quad \quad \quad a_1 - b_1 > b_1. \end{array}$$

From Formula I it follows that

$$\frac{a}{a_1} > \frac{a+b}{a_1-b_1} \quad \text{and} \quad \frac{b}{b_1} > \frac{a+b}{a_1-b_1},$$

and consequently

$$\frac{a}{a_1} + \frac{b}{b_1} > \frac{a+b}{a_1-b_1}.$$

ART. 132. The following formulas have to do with the special modul  $\frac{a}{a}$ . This modul is denoted by  $a^0$  and consists of all numbers  $\kappa$  such that  $\kappa a > a$ . To these numbers belongs clearly  $\kappa = 1$ , so that the modul  $[1]$  which consists of all rational integers is divisible by the modul  $a^0$ , or  $[1] > a^0$ . The modul  $[1]$  is sometimes denoted by  $\mathfrak{z}$  (see Art. 115, footnote). If  $\mathfrak{f}$  is a modul such that  $\mathfrak{f} a > a$ , then is  $\mathfrak{f} > \frac{a}{a}$ , that is  $\mathfrak{f} > a^0$ , and if  $\mathfrak{f} > a^0$  then is  $\mathfrak{f} a > a$ . The modul  $a^0$  we call the *order-modul* of  $a$ . See also Art. 133.

FORMULA VIII.

$$a a^0 = a.$$

For since  $a^0 = \frac{a}{a}$ , we have also  $a^0 > \frac{a}{a}$  and consequently

$$(1) \quad a^0 a > a.$$

On the other hand

$$\begin{aligned} \alpha &> \alpha \\ [1] &> \alpha^0. \end{aligned}$$

Hence

$$\alpha[1] > \alpha\alpha^0$$

or

$$(2) \quad \alpha > \alpha\alpha^0.$$

From (1) and (2) follows the equality required.

FORMULA IX.

$$\frac{\alpha}{\alpha^0} = \alpha.$$

For from VIII

$$\alpha\alpha^0 = \alpha,$$

and hence also

$$\alpha\alpha^0 > \alpha,$$

so that

$$(1) \quad \alpha > \frac{\alpha}{\alpha^0}.$$

On the other hand

$$\begin{aligned} \alpha &> \alpha \\ [1] &> \alpha^0, \end{aligned}$$

so that from Formula I

$$(2) \quad \frac{\alpha}{\alpha^0} > \alpha.$$

From (1) and (2) we have the required identity.

FORMULA X.

$$\alpha^0\alpha^0 = \alpha^0.$$

For from Formula VIII

$$\alpha\alpha^0 = \alpha,$$

and consequently

$$\alpha\alpha^0\alpha^0 = \alpha\alpha^0 = \alpha.$$

From this it follows that

$$\alpha^0\alpha^0 > \frac{\alpha}{\alpha},$$

or

$$(1) \quad a^0 a^0 > a^0.$$

On the other hand

$$a^0 > a^0 \\ [1] > a^0.$$

Hence

$$(2) \quad a^0 > a^0 a^0.$$

From (1) and (2) follows the identity required.

FORMULA XI.

$$\frac{a^0}{a^0} = a^0.$$

For since

$$a^0 > a^0 \quad \text{and} \quad [1] > a^0,$$

it follows from Formula I that

$$(1) \quad \frac{a^0}{a^0} > a^0.$$

Further since

$$a^0 a^0 = a^0,$$

it follows that

$$a^0 a^0 > a^0,$$

and consequently also

$$(2) \quad a^0 > \frac{a^0}{a^0},$$

from which with (1) the required identity is proved.

$\frac{a^0}{a^0}$  is sometimes written  $(a^0)^0$ .

FORMULA XII.  $a^r a^0 = a^r$  ( $r$  a positive integer).

For from VIII,

$$a a^0 = a.$$

If we multiply by  $a^{r-1}$ , we have

$$a^r a^0 = a^r$$

and similarly

$$a^0 a^r = a^r.$$

From X and XII it follows that the formula (Art. 125)  $a^r a^s = a^{r+s}$ , which was true when both  $r, s$  were positive

integers, is also true if one or both of the exponents = 0. For negative values of  $r$  and  $s$  the formula is *not* true. A modul with negative exponents has *not* been defined. Such a definition would be hard to give, since a modul  $a^{-1}$  which satisfies the equation

$$a^{-1}a = a^0$$

in general does *not* exist. Such a modul is had when  $a$  is a very special modul which is considered later in Vol. II, Chapt. II. The theorem  $\frac{a^r}{a^s} = a^0$ , which is true for numbers, is *not* true for moduls.

ART. 133. A modul  $\mathfrak{o}$  which has the two properties

$$(1) \quad \mathfrak{o}\mathfrak{o} = \mathfrak{o},$$

$$(2) \quad [1] > \mathfrak{o}$$

may be called an *order-modul*.<sup>1</sup>

Note that if  $\lambda$  and  $\mu$  are two numbers that are divisible by  $\mathfrak{o}$  then also  $\lambda\mu$  is divisible by  $\mathfrak{o}$ . It follows that the numbers of an order-modul are reproduced by the operation of multiplication. Thus an order-modul consists of a system of numbers which includes 1. These numbers are reproduced not only through the operations of addition and subtraction, as in the case of the usual moduls, but also through the operation of multiplication. Such order-moduls, since they contain 1 as an element, contain all rational integers, and that is  $[1]$  or the modul  $\mathfrak{z}$ .

Since  $\mathfrak{o} > \mathfrak{o}$  and  $[1] > \mathfrak{o}$ , it follows that  $\mathfrak{o}[1]$  or  $\mathfrak{o} > \mathfrak{o}\mathfrak{o}$ ; and since by definition  $\mathfrak{o}\mathfrak{o} > \mathfrak{o}$ , it follows that  $\mathfrak{o}\mathfrak{o} = \mathfrak{o}$ .

Further, since  $\mathfrak{o}\mathfrak{o} > \mathfrak{o}$ , it is seen that  $\mathfrak{o} > \frac{\mathfrak{o}}{\mathfrak{o}}$ , and from For-

<sup>1</sup>Dirichlet and Kronecker, *Grundzüge*, etc., § 5, used the word "Art" or "Species" to designate such moduls, while Dedekind, XI Supp. to Dirichlet's *Zahlentheorie* employed the term "Ordnung."



mula I applied to  $0 > 0$  and  $[1] > 0$ , it follows that  $\frac{0}{0} > 0$ . We thus have  $\frac{0}{0} = 0$ .

The order-modul  $a^0$  has for the modul  $a$  the same signification as unity has for ordinary numbers.

### CONGRUENCE WITH REGARD TO A MODUL

ART. 134. All numbers  $\mu$  of the modul  $m$  are said to be divisible by  $m$ ; they are  $\equiv 0 \pmod{m}$ . In general it may be said that  $\alpha$  is congruent to  $\beta \pmod{m}$ , and written  $\alpha \equiv \beta \pmod{m}$ , if  $\alpha - \beta$  is divisible by  $m$ , and that is, if  $\alpha - \beta$  is a number of the modul  $m$ . From this definition are had the three following *fundamental principles* of congruence (which exist also for the rational numbers):

- (1) If  $\alpha \equiv \beta \pmod{m}$ , then is  $\beta \equiv \alpha \pmod{m}$ ;
- (2)  $\alpha \equiv \alpha \pmod{m}$ ;
- (3) if  $\alpha \equiv \beta \pmod{m}$  and if  $\beta \equiv \gamma \pmod{m}$ , then is also  $\alpha \equiv \gamma \pmod{m}$ .

If  $\alpha \equiv \beta \pmod{m}$ , we say that  $\alpha$  is a *residue of*  $\beta \pmod{m}$ , and also that  $\beta$  is a *residue of*  $\alpha \pmod{m}$ .

If  $\alpha$  is *not* congruent to  $\beta \pmod{m}$ , then  $\alpha$  is said to be *incongruent to*  $\beta \pmod{m}$ .

If  $\alpha \equiv \alpha' \pmod{m}$  and  $\beta \equiv \beta' \pmod{m}$ , then is also

$$\alpha \pm \beta \equiv \alpha' \pm \beta' \pmod{m}.$$

For since  $\alpha - \alpha'$  and  $\beta - \beta'$  are both divisible by  $m$ , it follows that the sum and the difference of these quantities are divisible by  $m$ .

*Congruences added to or subtracted from congruences give congruences. For multiplication, it is clear that if  $\alpha \equiv \beta \pmod{m}$  and if  $g$  is a rational integer, then also*

$$\alpha g \equiv \beta g \pmod{m}.$$

In general if  $\nu$  is a number divisible by  $m^0$ , where  $m^0$  is the order-modul of  $m$ , then is

$$\nu \alpha \equiv \nu \beta \pmod{m} \quad \text{if} \quad \alpha \equiv \beta \pmod{m}.$$

For if  $\alpha - \beta$  is divisible by  $m$ , then  $\nu(\alpha - \beta)$  is divisible by  $mm^0$  (Art. 122) and consequently by  $m$ .

For numbers  $\nu$  that are *not* divisible by  $m^0$ , the above congruence cannot be proved; in fact, it is *not* true even for rational numbers; for

$$8 \equiv 3 \pmod{5},$$

but

$$8/2 \not\equiv 3/2 \pmod{5}.$$

If  $\alpha \equiv \beta \pmod{m}$  and if  $m > d$ , then also  $\alpha \equiv \beta \pmod{d}$ ; for if  $\alpha - \beta$  is divisible by  $m$  and if  $m$  is divisible by  $d$ , then also  $\alpha - \beta$  is divisible by  $d$ .

If  $\alpha \equiv \beta \pmod{a}$  and if  $\alpha \equiv \beta \pmod{b}$ , then also  $\alpha \equiv \beta \pmod{m}$  where  $m = a - b$ ; for if  $\alpha - \beta$  is divisible by both the moduli  $a$  and  $b$ , then  $\alpha - \beta$  is divisible by the least common multiple of these moduli.

ART. 135. Let  $\mathfrak{M}$  be an arbitrary complex or aggregate of numbers. The complex which is formed of all numbers  $\alpha + \mu$ , where  $\mu$  takes all values that belong to  $\mathfrak{M}$ ,  $\alpha$  being an arbitrary number, is denoted by  $\alpha + \mathfrak{M}$  or  $\mathfrak{M} + \alpha$ .

Let  $\mathfrak{M}$  be a modul, then in general  $\alpha + \mathfrak{M}$  is *not* a modul, but another system of numbers. For example, if  $\mathfrak{M}$  is a finite modul, then  $\mathfrak{M}$  consists of all numbers which may be expressed in the homogeneous form  $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ , where  $\alpha_1, \alpha_2, \cdots, \alpha_n$  form a basis of  $\mathfrak{M}$  and where  $x_1, x_2, \cdots, x_n$  are rational integers; on the other hand,  $\alpha + \mathfrak{M}$  represents all numbers that can be expressed through the non-homogeneous linear form  $\alpha + \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ . All numbers that are  $\equiv \alpha \pmod{\mathfrak{M}}$  form the complex  $\alpha + \mathfrak{M}$ . If  $\gamma$  is a number divisible by  $\mathfrak{M}$ , where  $\mathfrak{M}$  is a modul, then is  $\gamma + \mathfrak{M} = \mathfrak{M}$ ; for every arbitrary number of the complex  $\gamma + \mathfrak{M}$  has the form  $\gamma + \mu$ , where  $\mu$  belongs to the modul  $\mathfrak{M}$ , and conse-

quently, since  $\gamma$  is also divisible by  $\mathfrak{M}$ , it follows that  $\gamma + \mathfrak{M}$  is divisible by  $\mathfrak{M}$ .

If  $\alpha \equiv \beta \pmod{\mathfrak{M}}$ , then is

$$\alpha + \mathfrak{M} = \beta + \mathfrak{M}.$$

For if  $\alpha - \beta$  is divisible by  $\mathfrak{M}$ , then from what we have just seen

$$\alpha - \beta + \mathfrak{M} = \mathfrak{M},$$

and consequently also

$$\alpha - \beta + \mathfrak{M} + \beta = \mathfrak{M} + \beta,$$

or

$$\alpha + \mathfrak{M} = \beta + \mathfrak{M}.$$

Reciprocally, if  $\alpha + \mathfrak{M} = \beta + \mathfrak{M}$ , then is

$$\alpha \equiv \beta \pmod{\mathfrak{M}}.$$

For if

$$\alpha + \mathfrak{M} = \beta + \mathfrak{M},$$

then also

$$\alpha + 0 = \beta + \mu,$$

where  $\mu$  is divisible by  $\mathfrak{M}$ . Hence  $\alpha - \beta = \mu$  is divisible by  $\mathfrak{M}$ , or

$$\alpha \equiv \beta \pmod{\mathfrak{M}}.$$

If therefore two such *aggregates of numbers*  $\alpha + \mathfrak{M}$  and  $\beta + \mathfrak{M}$  are completely identical, then is

$$\alpha \equiv \beta \pmod{\mathfrak{M}}.$$

If on the other hand two such aggregates of numbers  $\alpha + \mathfrak{M}$  and  $\beta + \mathfrak{M}$  are not completely identical, then they haven't a single number in common. For suppose they had the number  $\kappa$  common, so that

$$\kappa = \alpha + \mu' = \beta + \mu'',$$

where both  $\mu'$  and  $\mu''$  are divisible by  $\mathfrak{M}$ ; it would follow that

$$\alpha - \beta = \mu'' - \mu',$$

a number divisible by  $\mathfrak{M}$ . We should then have

$$\alpha \equiv \beta \pmod{\mathfrak{M}},$$

and consequently from above

$$\alpha + \mathfrak{M} = \beta + \mathfrak{M}.$$

It is thus shown that the two complexes of numbers  $\alpha + \mathfrak{M}$  and  $\beta + \mathfrak{M}$  have either *all* numbers or *no* numbers in common. This fact is evident from the theorem that if two numbers are congruent to a third (mod.  $\mathfrak{M}$ ), they are also congruent to each other (mod.  $\mathfrak{M}$ ). For if  $\alpha \equiv \gamma$  (mod.  $\mathfrak{M}$ ) and  $\beta \equiv \gamma$  (mod.  $\mathfrak{M}$ ), then is  $\alpha \equiv \beta$  (mod.  $\mathfrak{M}$ ), or  $\alpha + \mathfrak{M} = \beta + \mathfrak{M}$ .

ART. 136. Let  $a$  and  $b$  be two moduls and consider *first* the special case where  $b > a$ . Let  $\alpha^{(1)}$  be any arbitrary number that is divisible by  $a$  and let  $\beta$  be any number that is divisible by  $b$ . Then since  $b > a$ , it follows that  $\alpha^{(1)} + \beta$  is divisible by  $a$ , and consequently all numbers of the complex  $\alpha^{(1)} + b$  are divisible by  $a$ . Two cases may happen, *either* the numbers of the complex  $\alpha^{(1)} + b$  comprise *all* the numbers of the modul  $a$ , *or* they do *not*. In the latter case let  $\alpha^{(2)}$  be a number of the modul  $a$ , which does not belong to the complex  $\alpha^{(1)} + b$ . We again have, since  $b > a$ ,  $\alpha^{(2)} + b > a$ , that is, every number of the complex  $\alpha^{(2)} + b$  is found in  $a$ . Further as seen above, the complexes  $\alpha^{(1)} + b$  and  $\alpha^{(2)} + b$  have no number in common. Two cases may again appear, *either* the numbers of the two complexes  $\alpha^{(1)} + b$  and  $\alpha^{(2)} + b$  constitute *all* the numbers of the modul  $a$ , *or* they do *not*. In the latter case let  $\alpha^{(3)}$  be a number that does not appear in either of the complexes  $\alpha^{(1)} + b$  and  $\alpha^{(2)} + b$ , and form the complex  $\alpha^{(3)} + b$ . This complex has no number in common with the two former complexes. Continuing this process it is seen that after a finite number of times we either obtain all the numbers of the given complex or we do not. In the former case we have a finite number of aggregates or classes of numbers

$$\alpha^{(1)} + b, \alpha^{(2)} + b, \alpha^{(3)} + b, \dots, \alpha^{(k)} + b,$$

where the numbers of these complexes constitute all the numbers of the modul  $a$ . In this case we shall use the symbol  $(a, b)$  to denote the number  $k$  of these classes. In the other event, where the number of classes is infinite, we shall put

$$(a, b) = 0.$$

When the number of classes is finite, we shall take a number from each of the classes, thus having  $k$  numbers

$$\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)},$$

(of which *one* is zero, say  $\alpha^{(1)} = 0$ ), which form a *complete system of representatives of the modul  $a$  with respect to the modul  $b$* . These  $k$  numbers have the following characteristics:

- (1) *They are all divisible by  $a$ ;*
- (2) *the difference of no two is divisible by  $b$ ;*
- (3) *every number that is divisible by  $a$  is congruent to one of these numbers (mod.  $b$ ) and from (2), to only one of these numbers.*

ART. 137. For the *general* case we may proceed as follows: Let  $a$  and  $b$  be two arbitrary moduls and distribute<sup>1</sup> the numbers that are divisible by  $a$  into classes with respect to the modul  $b$ . The number of these classes may be finite or infinite. A system of  $k$  numbers,  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  is called a *complete system of representatives* of the modul  $a$  with respect to the modul  $b$ , if it has the properties just enumerated. Each of the  $k$  numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  represents a definite class of numbers of the modul  $a$ . (Dedekind, § 171 of Dirichlet's *Zahlentheorie*, 4<sup>th</sup> Edition.)

Let  $m = a - b$  and suppose that the system  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  forms a complete system of representatives of

<sup>1</sup> That is, let  $\alpha^{(1)}$  be a number divisible by  $a$ , and take all numbers belonging to  $a$  which are congruent to  $\alpha^{(1)}$  (mod.  $b$ ) and put them in a class or group, and similarly with  $\alpha^{(2)}, \alpha^{(3)}, \dots, \alpha^{(k)}$ .



the modul  $a$  with respect to the modul  $b$ ; then this system of numbers also forms a complete system of representatives of the modul  $a$  with respect to the modul  $m$ . For the  $k$  numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  have the following three properties:

(1) *They are all divisible by  $a$ ;*

(2) *the difference of no two is divisible by  $m$ ; for if such a difference were divisible by  $m$ , it would also be divisible by  $b$  since  $m > b$ , and this is not true since  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  by hypothesis form a complete system of representatives of the modul  $a$  with respect to the modul  $b$ ;*

(3) *every number divisible by  $a$  is congruent to one of the numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)} \pmod{m}$ ; for if  $\alpha$  is congruent to a definite one of the numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)} \pmod{b}$ , say to  $\alpha^{(v)}$ , then is  $\alpha - \alpha^{(v)}$  divisible by  $b$ ; and since  $\alpha - \alpha^{(v)}$  is also divisible by  $a$ ; it follows that  $\alpha - \alpha^{(v)}$  is divisible by  $m$ , so that*

$$\alpha \equiv \alpha^{(v)} \pmod{m}.$$

It is thus seen that

$$(a, b) = (a, m);$$

or more definitely expressed: *If the  $k$  numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  form a complete systems of representatives of  $a$  with respect to  $b$ , then also they form a complete system of representatives of  $a$  with respect to the modul  $m$ .*

Further let  $b = a + b$ ; then if  $k$  numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  form a complete system of representatives of the modul  $a$  with respect to the modul  $b$ , they also form a complete system of representatives of the modul  $b$  with respect to  $b$ . For the  $k$  numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  have the properties:

(1) *they are all divisible by  $b$  since  $a > b$ ;*

(2) *the difference of no two is divisible by  $b$ , since they form a complete system of residues of the modul  $a$  with respect to the modul  $b$ ;*

(3) every number  $\delta$  that is divisible by  $b$  is congruent to a definite one of the  $k$  numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)} \pmod{b}$ ; for observe that  $\delta = \alpha + \beta$  where  $\alpha$  is divisible by  $a$  and  $\beta$  by  $b$ ; and since  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  form a complete system of residues of the modul  $a$  with respect to the modul  $b$ , it follows that

$$\alpha \equiv \alpha^{(v)} \pmod{b},$$

where  $\alpha^{(v)}$  is one of the numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$ , and consequently  $\alpha = \alpha^{(v)} + \beta'$ , where  $\beta'$  is a number divisible by  $b$ .

It is thus seen that

$$\delta = \alpha^{(v)} + \beta + \beta' = \alpha^{(v)} + \beta'',$$

where  $\beta''$  is divisible by  $b$ ; and therefore

$$\delta \equiv \alpha^{(v)} \pmod{b}.$$

Through the two formulas just derived, viz.,

$$(a, b) = (a, a - b),$$

$$(a, b) = (a + b, b),$$

it is seen that the general case has been reduced to the special case already considered, where  $b > a$ .

ART. 138. *If  $a > b$ , then is  $(a, b) = 1$ , and vice versa.*

For if  $a > b$ , then every number  $\alpha$  that is divisible by  $a$  is also divisible by  $b$ , and we have  $\alpha \equiv 0 \pmod{b}$ . We thus have only *one* class and therefore  $(a, b) \equiv 1$ .

On the other hand, if  $(a, b) = 1$  there can be only *one* class. Since 0 is divisible by  $a$ , this one class may be represented through the number 0, and all the numbers  $\alpha$  that are divisible by  $a$  must be  $\equiv 0 \pmod{b}$  and consequently divisible by  $b$ . It follows that  $a > b$ .

A special case of this theorem is

$$(a, a) = 1.$$

*If  $\eta$  is an arbitrary quantity different from 0, then is*

$$(a\eta, b\eta) = (a, b);$$

and further, if  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  form a complete system of residues of the modul  $a$  with respect to the modul  $b$ , then also  $\eta\alpha^{(1)}, \eta\alpha^{(2)}, \dots, \eta\alpha^{(k)}$  form a complete system of residues of the modul  $\eta a$  with respect to the modul  $\eta b$ .

For  $\eta\alpha^{(1)}, \eta\alpha^{(2)}, \dots, \eta\alpha^{(k)}$  have the three required properties:

(1) they are all divisible by  $\eta a$  since  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  are divisible by  $a$ ;

(2) the difference of any two  $\eta\alpha^{(\mu)} - \eta\alpha^{(\nu)}$  is not divisible by  $\eta b$ ; for otherwise  $\alpha^{(\mu)} - \alpha^{(\nu)}$  would be divisible by  $b$ ;

(3) every number divisible by  $\eta a$  is congruent to one of the definite numbers  $\eta\alpha^{(1)}, \eta\alpha^{(2)}, \dots, \eta\alpha^{(k)}$  with respect to the modul  $b$ ; for every number that is divisible by  $\eta a$  has the form  $\eta\alpha$ , where  $\alpha$  is divisible by  $a$ ; hence  $\alpha$  must be congruent to one of the numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  with respect to the modul  $b$  and therefore  $\eta\alpha$  is congruent to a definite one of the numbers  $\eta\alpha^{(1)}, \eta\alpha^{(2)}, \dots, \eta\alpha^{(k)} \pmod{\eta b}$ .

ART. 139. Suppose that  $b > a$  and  $c > b$ , then is

$$(a, c) = (a, b)(b, c);$$

and in fact if  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  is a complete system of residues of the modul  $a$  with respect to the modul  $b$ , and if  $\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(m)}$  is a complete system of residues of the modul  $b$  with respect to the modul  $c$ , the quantities  $\alpha^{(\nu)} + \beta^{(\mu)}$  ( $\nu = 1, 2, \dots, k; \mu = 1, 2, \dots, m$ ) form a complete system of residues of the modul  $a$  with respect to the modul  $c$ .

If this is proved, the correctness of the formula

$$(a, c) = (a, b)(b, c)$$

is established, since the number of the quantities  $\alpha^{(\nu)} + \beta^{(\mu)}$  is  $k \cdot m$ . The quantities  $\alpha^{(\nu)} + \beta^{(\mu)}$  have the three required properties:

(1) the quantities  $\alpha^{(\nu)} + \beta^{(\mu)}$  are divisible by  $a$ , since  $b$  is divisible by  $a$ ;

(2) *the difference of any two of these quantities is not divisible by c*; for if  $\alpha + \beta \equiv \alpha' + \beta' \pmod{c}$ , where  $\alpha$  and  $\alpha'$  are of the numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  and  $\beta, \beta'$  are of the numbers  $\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(m)}$ ; then since  $c > b$  and  $\beta \equiv \beta' \pmod{b}$  it would follow that

$$\alpha \equiv \alpha' \pmod{b},$$

which contradicts the assumption that  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  form a complete system of residues of the modul  $a$  with respect to the modul  $b$ , unless  $\alpha = \alpha'$ . But in this case

$$\beta \equiv \beta' \pmod{c},$$

which contradicts the hypothesis that  $\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(m)}$  form a complete system of residues of the modul  $b$  with respect to the modul  $c$ , unless  $\beta = \beta'$ . It follows that two *different* quantities  $\alpha^{(\nu)} + \beta^{(\mu)}$  is *not* divisible by  $c$ ;

(3) *every number that is divisible by a is congruent to one of the  $k \cdot m$  numbers  $\alpha^{(\nu)} + \beta^{(\mu)}$  ( $\nu = 1, 2, \dots, k$ ) ( $\mu = 1, 2, \dots, m$ ) ( $\text{mod. } c$ )*; for if  $\alpha$  is any of the numbers of  $a$ , then  $\alpha$  must be congruent to one of the numbers  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)} \pmod{b}$ , since  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  form a complete system of residues of the modul  $a$  with respect to  $b$ . It follows that

$$\alpha \equiv \alpha^{(\lambda)} \pmod{b}$$

or

$$\alpha = \alpha^{(\lambda)} + \beta,$$

where  $\beta$  is divisible by  $b$ . Since the quantities  $\beta^{(1)}, \beta^{(2)}, \dots, \beta^{(m)}$  form a complete system of residues of the modul  $b$  with respect to  $c$ , it follows that  $\beta$  must be congruent to one of these  $m$  numbers, say

$$\beta = \beta^{(\tau)} \pmod{c},$$

or

$$\beta = \beta^{(\tau)} + \gamma,$$

where  $\gamma$  is divisible by  $c$ . Hence we have

$$\alpha = \alpha^{(\lambda)} + \beta^{(\tau)} + \gamma \quad \text{or} \quad \alpha \equiv \alpha^{(\lambda)} + \beta^{(\tau)} \pmod{c}.$$

With this is established the formula

$$(a, c) = (a, b)(b, c),$$

a formula which is also true if either  $(a, b)$  or  $(b, c)$  or both are zero.

**ART. 140. THEOREM.** *If  $a, b, c$  are three arbitrary moduls, the following relation is true, namely*

$$(a, b)(b, c)(c, a) = (a, c)(c, b)(b, a).$$

The following lemma is useful in the proof of this remarkable theorem.

**LEMMA.** *If  $a_1 > a, a_1 > b, b_1 > a, b_1 > b$ , then is*

$$(a, a_1)(b, b_1) = (a, b_1)(b, a_1).$$

For put

$$m = a - b.$$

Since

$$\begin{array}{ll} a_1 > a & b_1 > a \\ a_1 > b & b_1 > b, \end{array}$$

it follows that

$$a_1 > m \quad \text{and} \quad b_1 > m.$$

From the formula we have just proved, it follows, since

$$\begin{array}{ll} m > a & \text{and} \quad m > b, \\ (a, a_1) = (a, m)(m, a_1) \\ (a, b_1) = (a, m)(m, b_1) \\ (b, a_1) = (b, m)(m, a_1) \\ (b, b_1) = (b, m)(m, b_1). \end{array}$$

Through multiplication we have

$$\begin{aligned} (a, a_1)(b, b_1) &= (a, m)(m, a_1)(b, m)(m, b_1) \\ &= (a, b_1)(b, a_1). \end{aligned}$$

In Art. 137 we saw that

$$(a, b) = (a + b, b)$$

and

$$(b, c) = (b, b - c),$$

so that

$$(a, b)(b, c) = (a + b, b)(b, b - c).$$



But since

$$b > a + b \quad \text{and} \quad b - c > b,$$

it follows that

$$(a + b, b)(b, b - c) = (a + b, b - c),$$

and consequently

$$(a, b)(b, c) = (a + b, b - c).$$

On the other hand

$$(c, a) = (c, a - c),$$

so that

$$(a, b)(b, c)(c, a) = (a + b, b - c)(c, a - c).$$

But

$$b - c > c \quad b - c > b + a \quad a - c > c \quad a - c > a + b.$$

Hence from the above lemma,

$$(a + b, b - c)(c, a - c) = (a + b, a - c)(c, b - c),$$

and consequently

$$(a, b)(b, c)(c, a) = (a + b, a - c)(c, b - c).$$

The expression on the right remains unchanged when  $a$  and  $b$  are interchanged, and consequently

$$\begin{aligned} (a, b)(b, c)(c, a) &= (b, a)(a, c)(c, b) \\ &= (a, c)(c, b)(b, a). \end{aligned}$$

The formula of the preceding Article may be derived at once from this formula; for in the special cases  $c > b$  and  $b > a$ , we have

$$(b, a) = 1, \quad (c, b) = 1, \quad (c, a) = 1$$

(Art. 138), so that the formula just written is

$$(a, b)(b, c) = (a, c).$$

**ART. 141. A Generalization<sup>1</sup> of Fermat's Theorem.**

**THEOREM.** *If  $a$  and  $b$  are two arbitrary moduls, then*

$$(a, b)a > b.$$

In the first place it is evident that the theorem is true, if the number of representatives of a complete system of

<sup>1</sup> See Dickson's *History*, etc., Vol. I, Chapt. III.

residues of the modul  $a$  with respect to the modul  $b$  is infinite. For if  $(a, b) = 0$ , we have  $0 \cdot a$  which is divisible by  $b$ .

We may consequently assume that  $(a, b) = k$ , where  $k$  is a positive integer different from zero.

Let the quantities  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(k)}$  form a complete system of residues of the modul  $a$  with respect to the modul  $b$ . If then  $\alpha$  is an arbitrary number divisible by  $a$ , then are the  $k$  numbers

$$(1) \quad \alpha + \alpha^{(1)}, \alpha + \alpha^{(2)}, \dots, \alpha + \alpha^{(k)}$$

all divisible by  $a$ ; and further the difference of no two of them is divisible by  $b$ , and consequently no two of the series of numbers (1) belong to the same class. It follows that

$$\alpha^{(1)} \equiv \alpha + \alpha^{(r)} \pmod{b},$$

$$\alpha^{(2)} \equiv \alpha + \alpha^{(s)} \pmod{b},$$

.....

where the integers  $r, s, \dots$ , are (neglecting the sequence) to be found among the numbers  $1, 2, \dots, k$ .

Through addition of the  $n$  congruences just written we have

$$\begin{aligned} \alpha^{(1)} + \alpha^{(2)} + \dots + \alpha^{(k)} &\equiv \alpha + \alpha^{(r)} + \alpha + \alpha^{(s)} + \dots \pmod{b} \\ &\equiv k\alpha + \alpha^{(1)} + \alpha^{(2)} + \dots + \alpha^{(k)} \pmod{b}, \end{aligned}$$

or

$$0 \equiv k\alpha \pmod{b}.$$

Since this congruence is true of every number  $\alpha$  that is divisible by  $a$ , it follows that

$$ka > b$$

and consequently also

$$ka > b + a,$$

or

$$ka > b.$$

From the theorem just proved it is seen that if  $(a, b) \neq 0$ , there exists always a positive integer  $k$ , say, that is

different from zero and is such that

$$ka > b.$$

*Inversely* it also follows that if there is a positive integer  $k$  different from zero and such that  $ka > b$ , then also  $(a, b) \neq 0$  so that *the above condition that*  $(a, b)$  *be different from zero is also sufficient.*

ART. 142. THEOREM. *There are only a finite number of moduls which are at the same time multiples of  $a$  and divisors of  $b$ , if  $b > a$  and  $(a, b) \neq 0$ .*

For let  $f$  be a modul such that  $f > a$  and  $b > f$ . Further let  $\alpha$  be a number that is divisible by  $f$ , and consequently all numbers of the complex  $\alpha + b$  are divisible by the modul  $f$  and therefore also by  $a$ . If then  $0, \alpha^{(1)}, \dots, \alpha^{(k-1)}$  are a complete system of residues of the modul  $a$  with respect to the modul  $b$ , then since  $\alpha$  is also divisible by  $a$ , the complex  $\alpha + b$  is identical with one of the complexes

$$(1) \quad 0 + b, \alpha^{(1)} + b, \alpha^{(2)} + b, \dots, \alpha^{(k-1)} + b.$$

Hence there may arise in all only the following possible cases: The modul  $f$  comprises *only* the numbers of the modul  $b$ , or besides, an additional *one* of the complexes (1), or an additional *two* of the complexes (1),  $\dots$ , or *all* of the complexes (1) in addition. Hence for the modul  $f$  there are in all

$$1 + \binom{k-1}{1} + \binom{k-1}{2} + \binom{k-1}{3} + \dots + \binom{k-1}{k-1} = (1+1)^{k-1} = 2^{k-1}$$

cases conceivable.

We have thus proved the theorem and at the same time given a method of finding all moduls which are at the same time multiples of  $a$  and divisors of  $b$ , when  $(a, b) \neq 0$  and  $b > a$ .

EXAMPLE. Prove that the inverse of this theorem is true.

ART. 143. THEOREM. *If  $a$  and  $b$  are two moduli and if  $\rho$  and  $\sigma$  are two given quantities, then the necessary and sufficient condition that the following two congruences*

$$\begin{aligned}\omega &\equiv \rho \pmod{a}, \\ \omega &\equiv \sigma \pmod{b},\end{aligned}$$

*be satisfied by one and the same quantity  $\omega$ , is expressed through the congruence*

$$\rho \equiv \sigma \pmod{a+b}.$$

We shall first show that this condition is necessary. Assume that there is a number  $\tau$  such that

$$\tau \equiv \rho \pmod{a} \quad \text{and} \quad \tau \equiv \sigma \pmod{b};$$

then is also

$$\tau \equiv \rho \pmod{a+b} \quad \text{and} \quad \tau \equiv \sigma \pmod{a+b},$$

and consequently

$$\rho \equiv \sigma \pmod{a+b}.$$

This condition is also sufficient. For assuming that it is seen that

$$\rho \equiv \sigma \pmod{a+b},$$

$$\rho - \sigma = \delta,$$

where  $\delta$  is a number divisible by  $b = a + b$ . It follows that

$$\rho - \sigma = \alpha + \beta, \quad \text{or} \quad \rho - \alpha = \sigma + \beta.$$

If then we put

$$\tau = \rho - \alpha = \sigma + \beta,$$

it is seen that

$$\tau \equiv \rho \pmod{a} \quad \text{and} \quad \tau \equiv \sigma \pmod{b},$$

or  $\tau$  satisfies both congruences.

The most general solution of the two congruences

$$\omega \equiv \rho \pmod{a} \quad \omega \equiv \sigma \pmod{b}$$

may now be derived. This of course depends on the possibility of the solution, and that is, if

$$\rho \equiv \sigma \pmod{a+b}.$$

Let  $\tau$  be a special and  $\omega$  any arbitrary solution of the two

congruences, so that

$$\begin{aligned}\omega &\equiv \rho \pmod{a} & \omega &\equiv \sigma \pmod{b} \\ \tau &\equiv \rho \pmod{a} & \tau &= \sigma \pmod{b},\end{aligned}$$

and consequently

$$\omega \equiv \tau \pmod{a} \quad \omega \equiv \tau \pmod{b}.$$

It follows that

$$\omega \equiv \tau \pmod{m},$$

where  $m = a - b$ . We thus see that

$$\omega = \tau + \mu,$$

where  $\mu$  is some number divisible by the modulus  $m$ .

Reciprocally, if  $\mu$  is some number divisible by  $m$ , then always  $\tau + \mu$  is a solution of the two congruences.

For if

$$\mu \equiv 0 \pmod{m},$$

it is seen that

$$\mu \equiv 0 \pmod{a}, \quad \mu \equiv 0 \pmod{b},$$

and since

$$\tau \equiv \rho \pmod{a}, \quad \tau = \sigma \pmod{b},$$

it follows that

$$\mu + \tau \equiv \rho \pmod{a}, \quad \mu + \tau \equiv \sigma \pmod{b}.$$

Hence if  $\tau$  is a special solution of the two congruences

$$\tau \equiv \rho \pmod{a}, \quad \tau \equiv \sigma \pmod{b},$$

then the most general solution of these two congruences is

$$\tau + \mu,$$

where  $\mu$  goes through all numbers that are divisible by  $m$ .

It is seen that this theorem is the analogue of the corresponding theorem for rational integers.





It is evident that any linear expression,<sup>1</sup> that can be formed of the  $\alpha$ 's may also be formed of the  $\beta$ 's and *vice versa*. The changes that may be made among the basal elements may be illustrated by the following example:

$$\begin{aligned} [87, 36] &= [87 - 2 \cdot 36, 36] = [15, 36] = [15, 36 - 2 \cdot 15] \\ &= [15, 6] = [15 - 2 \cdot 6, 6] = [3, 6] = [3, 6 - 2 \cdot 3] \\ &= [3, 0] = [3] = 3x, \end{aligned}$$

where  $x$  is a rational integer. This process is nothing other than a method of finding the greatest common divisor of two rational integers. It is evident that it may be applied to any number of rational integers. If  $d$  is the greatest common divisor of  $a, b, c$ , then is

$$[a, b, c] = [d],$$

if  $a, b, c$  are rational integers (Art. 113).

ART. 145. The following definitions are offered: If a finite modul has a basis which consists of  $n$  elements, and if it has *no* basis that consists of fewer than  $n$  elements, then  $n$  is called the *rank* or *order* of the finite modul.

If  $\alpha_1, \alpha_2, \dots, \alpha_n$  are  $n$  arbitrary numbers, we say that they are *dependent* or that *they form a reducible system* (Art. 57), if it is possible to determine  $n$  rational integers  $x_1, x_2, \dots, x_n$ , such that

$$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n = 0$$

without all the  $x$ 's being zero. If this is *not* possible, the quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$  are said to be *independent* (linear independent), and form an *irreducible system*. An irreducible system is formed, for example, of the  $m$  elements of the basis of a finite algebraic realm of the  $m$ th degree (Art. 64). In the following investigation we shall *at first* confine ourselves *not* wholly to algebraic

<sup>1</sup> In this connection a paper by Frobenius on "Linear Forms" (*Crelle's Journal*, Vol. 86, p. 146) is of great importance.

See also Stieltjes, *Toulouse Ann.*, Vol. 4, p. 1.



Since  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, it follows that in the above equation each coefficient of the  $\alpha$ 's must of itself be zero. Define  $e_{r,s}$  as a symbol to be interpreted as follows:

$$e_{rs} = 0 \text{ if } r \neq s, \quad e_{rs} = 1 \text{ if } r = s.$$

Then from the above equation it is seen that

$$b_{r1}a_{1s} + b_{r2}a_{2s} + \dots + b_{rn}a_{ns} = e_{rs} \quad (r, s = 1, 2, \dots, n).$$

Due to the theorem for the multiplication of determinants it results that

$$|b_{rs}| \cdot |a_{rs}| = |e_{rs}| = 1;$$

or if we put  $|b_{rs}| = B$  and  $|a_{rs}| = A$ , then

$$AB = 1.$$

But since  $A$  and  $B$  are rational integers, it is evident that

$$A = \pm 1, \quad B = \pm 1.$$

It follows since  $A \neq 0$ , that the quantities  $\beta_1, \beta_2, \dots, \beta_n$  are independent. We shall also make use in the sequel of the other result, namely that  $B = \pm 1$ .

**ART. 147. THEOREM.** *If of the elements of a finite modul  $\mathfrak{a}$  there are  $n$  independent, then (1) the modul  $\mathfrak{a}$  has a basis which consists of  $n$  independent elements; and (2)  $n$  is the order of the modul.*

*The first part of the theorem may be proved as follows:* Suppose that the elements of the modul have been so arranged that the  $n$  independent elements come first so that

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n, \beta, \gamma, \dots],$$

where  $\alpha_1, \alpha_2, \dots, \alpha_n$  are independent, while the elements  $\beta, \gamma, \dots$ , which are of course finite in number, are dependent. It will follow in the process of the proof that the number  $n$  is a perfectly definite number. The numbers  $\alpha_1, \alpha_2, \dots, \alpha_n, \beta$  are not independent, and consequently there is an equation of the form

$$b\beta = b_1\alpha_1 + b_2\alpha_2 + \dots + b_n\alpha_n,$$

where  $b, b_1, b_2, \dots, b_n$  are rational integers with no greatest common divisor other than unity. We must also assume that  $b \neq 0$ , otherwise there would be a linear relation among the  $\alpha$ 's. We may further assume that  $b > 1$ ; for if  $b = 1$ , it is seen that  $\beta$  is linearly expressed in terms of the  $\alpha$ 's and may therefore be dropped from the elements that are to constitute the basis of  $a$ . In a similar manner  $\gamma$  is dependent on the  $\alpha$ 's so that there is an equation of the form

$$c\gamma = c_1\alpha_2 + c_2\alpha_2 + \dots + c_n\alpha_n,$$

where  $c > 1$  and  $c_1, c_2, \dots, c_n$  are rational integers without a greatest common divisor other than unity, etc.

Let  $p$  be a prime number that is a factor of  $b$ , so that

$$b = b'p.$$

It follows that

$$(1) \quad b'p\beta = b_1\alpha_1 + b_2\alpha_2 + \dots + b_n\alpha_n.$$

Further since the numbers  $b_1, b_2, \dots, b_n$  have no common divisor, it is seen that all the numbers  $b_1, b_2, \dots, b_n$  cannot be divisible by  $p$ . If say,  $b_1$  is not divisible by  $p$ , then two integers  $r$  and  $s$  may be determined such that

$$ps - b_1r = 1.$$

If we multiply the equation (1) by  $r$ , we have

$$\begin{aligned} b'p\beta r &= b_1r\alpha_1 + (b_2\alpha_2 + \dots + b_n\alpha_n)r \\ &= (ps - 1)\alpha_1 + (b_2\alpha_2 + \dots + b_n\alpha_n)r, \end{aligned}$$

and consequently

$$\alpha_1 = p(s\alpha_1 - b'\beta r) + (b_2\alpha_2 + \dots + b_n\alpha_n)r.$$

If we put

$$\alpha'_1 = s\alpha_1 - b'\beta r,$$

it follows that

$$(2) \quad \alpha_1 = p\alpha'_1 + b_2r\alpha_2 + \dots + b_nr\alpha_n.$$

Next multiply the equation (1) by  $s$ . It is seen that

$$b'p\beta s = b_1s\alpha_1 + (b_2\alpha_2 + \dots + b_n\alpha_n)s,$$



or

$$b'\beta(1+b_1r) = b_1s\alpha_1 + (b_2\alpha_2 + \dots + b_n\alpha_n)s,$$

so that

$$(3) \quad b'\beta = b_1\alpha'_1 + b_2s\alpha_2 + \dots + b_ns\alpha_n.$$

The new system of the numbers  $\alpha'_1, \alpha_2, \alpha_3, \dots, \alpha_n$  has the same characteristic properties as have the  $n$  numbers  $\alpha_1, \alpha_2, \dots, \alpha_n$ ; in other words, if

$$(4) \quad a = [\alpha_1, \alpha_2, \dots, \alpha_n, \beta, \gamma, \dots],$$

then is also

$$(5) \quad a = [\alpha'_1, \alpha_2, \dots, \alpha_n, \beta, \gamma, \dots].$$

This follows from the fact that the element

$$\alpha'_1 = s\alpha_1 - b'r\beta$$

may be added to (4), giving

$$a = [\alpha_1, \alpha_2, \dots, \alpha_n, \beta, \gamma, \dots, \alpha'_1].$$

When this has been done, it follows from (2) that  $\alpha_1$  may be omitted from the elements, thus producing (5).

Further the elements  $\alpha'_1, \alpha_2, \dots, \alpha_n$  are linearly independent. For if they were dependent, there must be an equation of the form

$$(6) \quad x_1\alpha'_1 + x_2\alpha_2 + \dots + x_n\alpha_n = 0,$$

where the  $x$ 's are rational integers. This equation may be written

$$x_1(s\alpha_1 - b'r\beta) + x_2\alpha_2 + \dots + x_n\alpha_n = 0,$$

or

$$x_1s\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n - x_1b'\frac{\beta p}{p}r = 0;$$

or from (1),

$$x_1s\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n - x_1\frac{r}{p}(b_1\alpha_1 + b_2\alpha_2 + \dots + b_n\alpha_n) = 0.$$

It follows that

$$(x_1ps - x_1rb_1)\alpha_1 + (x_2p - x_1rb_2)\alpha_2 + \dots + (x_np - x_1rb_n)\alpha_n = 0.$$

Since  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, the coefficients in this expression just written must be all zero.

Hence

$$x_1(ps - rb_1) = 0,$$

and since

$$ps - rb_1 = 1,$$

it follows that  $x_1 = 0$  and then from (6)

$$x_2\alpha_2 + x_3\alpha_3 + \dots + x_n\alpha_n = 0.$$

Since  $\alpha_2, \alpha_3, \dots, \alpha_n$  are linearly independent, it follows also that

$$x_2 = 0 = x_3 = \dots = x_n.$$

Finally it is seen that  $\beta, \gamma, \dots$  are expressible linearly with integral or fractional coefficients through  $\alpha'_1, \alpha_2, \dots, \alpha_n$ . The form (3) may be written

$$b'\beta = b_1\alpha'_1 + b'_2\alpha_2 + \dots + b'_n\alpha_n,$$

where  $b'_2, \dots, b'_n$  are rational integers; or,

$$\beta = \frac{b_1\alpha'_1 + b'_2\alpha_2 + \dots + b'_n\alpha_n}{b'}.$$

In this expression of  $\beta$  through  $\alpha'_1, \alpha_2, \dots, \alpha_n$ , the denominator  $b'$  is smaller than  $b$  which is the denominator in the expression of  $\beta$  through  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

On the other hand in the expression of  $\gamma, \delta, \dots$  through  $\alpha'_1, \alpha_2, \dots, \alpha_n$ , the denominators are the same as in the expressions of these quantities through  $\alpha_1, \alpha_2, \dots, \alpha_n$ . For we had above

$$\begin{aligned} c\gamma &= c_1\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n \text{ [which from (2)]} \\ &= c_1(pa'_1 + b_2r\alpha_2 + \dots + b_nr\alpha_n) + c_2\alpha_2 + \dots + c_n\alpha_n \\ &= c'_1\alpha'_1 + c'_2\alpha_2 + \dots + c'_n\alpha_n, \end{aligned}$$

where  $c'_1, c'_2, \dots, c'_n$  are rational integers. It follows that

$$\gamma = \frac{c'_1\alpha'_1 + c'_2\alpha_2 + \dots + c'_n\alpha_n}{c}.$$

Comparing the elements  $\alpha'_1, \alpha_2, \dots, \alpha_n, \beta, \gamma, \dots$  with  $\alpha_1, \alpha_2, \dots, \alpha_n, \beta, \gamma, \dots$ , it is seen that 1°, the number of elements is the same in both systems; 2°, the first  $n$  numbers of both systems are independent; 3°, the elements  $\beta, \gamma, \dots$  may be expressed through the first  $n$  elements of either system with the same denominator.

We note, however, in the expression of  $\beta$  through the two systems, that the denominator  $b'$  occurring in the first system is smaller than the denominator  $b$  which occurs in the second system, since  $b = pb'$  and  $p \neq 1$ . If  $b'$  were equal to unity, we could omit  $\beta$  from the system  $\alpha'_1, \alpha_2, \dots, \alpha_n, \beta, \gamma, \dots$ , due to the fact that  $\beta$  could be then expressed linearly with integral coefficients in terms of the remaining elements. If  $b' \neq 1$ , then is

$$b' = p'b'',$$

where the prime integer  $p'$  is different from 1. Proceeding as above we may form a new system of elements in which the first  $n$  elements are linearly independent and are such that when  $\beta$  is expressed linearly through them, the denominator that appears is  $b''$ , which is less than  $b'$ , while the denominators which occur in the expressions for  $\gamma, \delta, \dots$  have not been changed. Continuing this process we must finally come to a system of elements in which the denominator for the expression for  $\beta$  is unity. When this has been done,  $\beta$  may be dropped from the system. The same process may be then applied to  $\gamma, \delta, \dots$ . We thus come finally to a system of  $n$  independent elements which form a basis of the modul  $a$ .

The *second part* of the theorem may be expressed as follows:

*If the modul  $a$  has a basis consisting of  $n$  independent elements, it can not have a basis consisting of fewer elements. It then follows that  $n$  is the rank or order of the modul  $a$ ,*

and that the number of independent elements of the modul  $\mathfrak{a}$  is its rank or order.

Let  $\mathfrak{a}$  have a basis consisting of the  $n$  linearly independent elements  $\alpha_1, \alpha_2, \dots, \alpha_n$ , so that

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n].$$

Denote the rank or order of  $\mathfrak{a}$  by  $m$ ; it is then asserted that  $m = n$ . Suppose that  $m < n$ , and that  $\mathfrak{a}$  has a basis which consists of less than  $n$  elements, and let these elements be  $\beta_1, \beta_2, \dots, \beta_m$ . Then the  $\alpha$ 's may be expressed through the  $\beta$ 's in the form

$$\alpha_r = c_{r1}\beta_1 + c_{r2}\beta_2 + \dots + c_{rm}\beta_m \quad (r=1, 2, \dots, n),$$

where  $c_{r1}, c_{r2}, \dots, c_{rm}$  are rational integers. It follows also that

$$\sum_{r=1}^n \alpha_r x_r = \beta_1 \sum_{r=1}^n c_{r1} x_r + \beta_2 \sum_{r=1}^n c_{r2} x_r + \dots + \beta_m \sum_{r=1}^n c_{rm} x_r,$$

where  $x_1, x_2, \dots, x_n$  are arbitrary rational numbers. These quantities  $x_1, x_2, \dots, x_n$  may, however, be so determined that the equations

$$\sum_{r=1}^n c_{r1} x_r = 0, \quad \sum_{r=1}^n c_{r2} x_r = 0, \quad \dots, \quad \sum_{r=1}^n c_{rm} x_r = 0$$

are satisfied, there being  $m$  equations and  $n (> m)$  unknown quantities which may be satisfied always by values of  $x$  different from zero. It follows then that

$$\sum_{r=1}^n x_r \alpha_r = 0,$$

where the  $x$ 's are not all zero, and consequently also that  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly dependent. This is contrary to the hypothesis. Hence the rank or order of the modul  $\mathfrak{a}$  must be  $n$ , where  $n$  is equal to the number of independent elements of a basis of  $\mathfrak{a}$ .

Reciprocally, if the order of the modul  $\mathfrak{a}$  is equal to  $n$ , then  $\mathfrak{a}$  has a basis of  $n$  linear independent elements; and

in every arbitrary basis of  $\mathfrak{a}$  there are precisely  $n$  linearly independent elements.

ART. 148. *If  $\mathfrak{a}$  is a finite modul and if the modul  $\mathfrak{b}$  is divisible by  $\mathfrak{a}$ , then  $\mathfrak{b}$  is a finite modul; and the order of  $\mathfrak{b}$  is not greater than the order of  $\mathfrak{a}$ . In other words every multiple of a finite modul is a finite modul.*

Let  $\mathfrak{a}$  be a finite modul of the  $n$ th order, say,

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n].$$

Since  $\mathfrak{b}$  is divisible by  $\mathfrak{a}$ , every number that is divisible by  $\mathfrak{b}$  may be expressed in the form  $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$ , where  $x_1, x_2, \dots, x_n$  are rational integers including zero. However, to have all the numbers of the modul  $\mathfrak{b}$  it is not necessary that *all* rational integral values be ascribed to the variables  $x_1, x_2, \dots, x_n$ .

If there are numbers of the form  $\alpha_1 x_1$  which are divisible by  $\mathfrak{b}$ , we seek that one which for a positive  $x_1$  has the smallest value, and denote it by

$$\beta_1 = a_{11} \alpha_1.$$

If there is *no* number of the form  $\alpha_1 x_1$  that is divisible by  $\mathfrak{b}$ , put  $a_{11} = 0$ . Consider next those numbers of the modul  $\mathfrak{b}$  which may be expressed in the form  $a_1 x_1 + a_2 x_2$ , where  $x_2 \neq 0$ . If such numbers exist, choose that one for which  $a_2$  has the smallest positive value and denote it by

$$\beta_2 = a_{21} \alpha_1 + a_{22} \alpha_2.$$

If there is *no* such number, write  $a_{21} = 0 = a_{22}$ . Continuing this process, consider those numbers that are divisible by  $\mathfrak{b}$  and which have the form

$$a_1 x_1 + a_2 x_2 + \dots + a_r x_r \quad (r=1, 2, \dots, n).$$

If there are numbers of this form, choose that one for which  $a_r$  has the smallest positive value and denote it by

$$\beta_r = a_{r1} \alpha_1 + a_{r2} \alpha_2 + \dots + a_{rr} \alpha_r;$$



but if there is no such number of this form, write

$$a_{r1} = 0 = a_{r2} = \dots = a_{rr}.$$

It is asserted that the quantities  $\beta_1, \beta_2, \dots, \beta_n$  which are thus derived constitute a basis of the modul  $\mathfrak{b}$ , so that

$$\mathfrak{b} = [\beta_1, \beta_2, \dots, \beta_n].$$

When this is established, the first part of the theorem is proved, viz., that  $\mathfrak{b}$  is a modul of finite order.

Take any number  $\beta$  which may be expressed through the first  $r$  elements of the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$  in the form

$$\beta = x_1\alpha_1 + x_2\alpha_2 + \dots + x_r\alpha_r,$$

where  $x_1, x_2, \dots, x_r$  are rational integers. If  $a_{rr} = 0$ , then owing to the method by which  $a_{rr}$  was determined, it follows that  $x_r = 0$ ; but if  $a_{rr} \neq 0$ , then  $x_r$  must be divisible by  $a_{rr}$ , due to the hypothesis that

$$|x_r| \geq a_{rr}.$$

For dividing  $x_r$  by  $a_{rr}$  we have, say,

$$x_r = a_{rr}b_r + a_r,$$

where

$$0 \leq a_r < a_{rr}.$$

It results that

$$\begin{aligned} \beta - b_r\beta_r &= (x_1 - b_r a_{r1})\alpha_1 + (x_2 - b_r a_{r2})\alpha_2 + \dots + (x_r - b_r a_{rr})\alpha_r \\ &= (x_1 - b_r a_{r1})\alpha_1 + (x_2 - b_r a_{r2})\alpha_2 + \dots + a'_r\alpha_r. \end{aligned}$$

It appears that the number  $\beta - b_r\beta_r$  which is also divisible by  $\mathfrak{b}$  is expressible through  $\alpha_1, \alpha_2, \dots, \alpha_r$  and that the coefficient of  $\alpha_r$  is smaller than  $a_{rr}$ , which by hypothesis was the smallest coefficient of  $\alpha_r$  among all the numbers of the form  $x_1\alpha_1 + x_2\alpha_2 + \dots + x_r\alpha_r$  that were divisible by  $\mathfrak{b}$ . It follows therefore that

$$a'_r = 0,$$

and consequently  $x_r$  is divisible by  $a_{rr}$ . Suppose next that  $\beta$  is any arbitrary number that is divisible by  $\mathfrak{b}$  and consequently also by  $\mathfrak{a}$ , since  $\mathfrak{b}$  is divisible by  $\mathfrak{a}$ .

We may therefore write  $\beta$  in the form

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n.$$

If  $r$  is the greatest number for which  $a_r \neq 0$ , then

$$\beta - b_r\beta_r = (a_1 - b_r a_{r1})\alpha_1 + (a_2 - b_r a_{r2})\alpha_2 + \cdots + (a_r - b_r a_{rr})\alpha_r,$$

or since

$$a_r - b_r a_{rr} = 0,$$

we must have

$$\beta - b_r\beta_r = a'_1\alpha_1 + a'_2\alpha_2 + \cdots + a'_s\alpha_s \quad (s < r).$$

It is thus shown that a new number  $\beta - b_r\beta_r$  has been derived which is divisible by  $\mathfrak{b}$  and which may be expressed through fewer than  $r$  of the basal elements of  $\mathfrak{a}$ , viz., through  $\alpha_1, \alpha_2, \cdots, \alpha_s$  (where  $s < r$ ).

By means of the number  $\beta - b_r\beta_r$  and using the same method, we derive another number also divisible by  $\mathfrak{b}$ , viz.,

$$\beta - b_r\beta_r - b_s\beta_s = a''_1\alpha_1 + a''_2\alpha_2 + \cdots + a''_t\alpha_t \quad (\text{where } t < s).$$

Finally we come to a number divisible by  $\mathfrak{b}$  which  $= 0$ , and we then have

$$\beta = b_r\beta_r + b_s\beta_s + b_t\beta_t + \cdots.$$

Thus it has been shown that every number  $\beta$  that is divisible by  $\mathfrak{b}$  may be linearly expressed through the numbers  $\beta_1, \beta_2, \cdots, \beta_n$  with rational integral coefficients. It follows that  $\beta_1, \beta_2, \cdots, \beta_n$  form a basis of  $\mathfrak{b}$  and that  $\mathfrak{b}$  is a finite modul. At the same time it is also seen that the order of  $\mathfrak{a}$  is not smaller than the order of  $\mathfrak{b}$ ; for of the  $n$  elements  $\beta_1, \beta_2, \cdots, \beta_n$  it has been seen that some may be zero, and further there may be linear relations among them. This latter question is again considered.

ART. 149. If  $\mathfrak{a}$  is a finite modul taken with respect to an arbitrary (*not necessarily independent*) basis  $\alpha_1, \alpha_2, \cdots, \alpha_n$ , and if  $\mathfrak{b} > \mathfrak{a}$ , then as shown above we may determine a basis of  $\mathfrak{b}$ , say  $\beta_1, \beta_2, \cdots, \beta_n$  such that

$$\beta_r = a_{r1}\alpha_1 + a_{r2}\alpha_2 + \cdots + a_{rn}\alpha_n \quad (r = 1, 2, \cdots, n),$$

where  $a_{r1}, a_{r2}, \dots, a_{rn}$  are integers or zero. These quantities  $a_{rt}$  are zero if  $t > r$ , while  $a_{11}, a_{12}, \dots, a_{rr} \geq 0$ . The quantities  $a_{rt}$  form therefore a triangular system which may be made rectangular by the addition of zeros as illustrated in the following scheme:

$$\begin{array}{ccccccc}
 a_{11}, & 0, & 0, & 0, & \dots, & 0 \\
 a_{12}, & a_{22}, & 0, & 0, & \dots, & 0 \\
 a_{13}, & a_{23}, & a_{33}, & 0, & \dots, & 0 \\
 \dots & \dots & \dots & \dots & \dots & \dots \\
 a_{1n}, & a_{2n}, & a_{3n}, & a_{4n}, & \dots, & a_{nn}.
 \end{array}$$

**THEOREM.** *The number of incongruent residues of the modul a with respect to the modul b is equal to the product  $a_{11} \cdot a_{22} \cdot \dots \cdot a_{nn}$ ; or*

$$(a, b) = a_{11}a_{22} \cdot \dots \cdot a_{nn}.$$

In the proof of this formula two cases are to be distinguished: namely (1) where the quantities  $a_{11}, a_{22}, \dots, a_{nn}$  are all different from zero; and (2) where some of the quantities  $a_{11}, a_{22}, \dots, a_{nn}$  are zero.

In the second case it is asserted that  $(a, b) = 0$ , an assertion which may be stated as follows: If  $(a, b) \neq 0$ , then none of the quantities  $a_{11}, a_{22}, \dots, a_{nn}$  is zero. This is of course identical with the statement that  $(a, b) = 0$  unless all the quantities  $a_{11}, a_{22}, \dots, a_{nn}$  are different from zero.

Suppose that  $(a, b) = m \neq 0$ . It follows (Art. 141) that

$$ma > b$$

and consequently  $m\alpha_r$  is divisible by  $b$  for  $r = 1, 2, \dots, n$ . Accordingly there is a number divisible by  $b$  which must have the form

$$x_1\alpha_1 + x_2\alpha_2 + \dots + x_r\alpha_r$$

and for which  $x_r \neq 0$ , and consequently  $a_{rr} \neq 0$  ( $r = 1, 2, \dots, n$ ). With this the second case is proved.

Returning to the first case, suppose that each of the

quantities  $a_{11}, a_{22}, \dots, a_{nn}$  is different from zero. It is then asserted that

$$(a, b) = a_{11}a_{22} \cdots a_{nn}.$$

We shall derive a complete system of residues and it will be seen that the system consists of exactly  $a_{11}a_{22} \cdots a_{nn}$  numbers.

Form the expression

$$\zeta = z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n,$$

and in this formula give

to  $z_1$  the values  $0, 1, \dots, a_{11} - 1,$

to  $z_2$  the values  $0, 1, \dots, a_{22} - 1,$

.....

to  $z_n$  the values  $0, 1, \dots, a_{nn} - 1.$

The  $a_{11} \cdot a_{22} \cdots a_{nn}$  values of  $\zeta$  thus derived form a complete system of residues of the modul  $a$  with respect to the modul  $b$ . For they have the following three characteristic properties:

(1) *They are all divisible by  $a$ .*

(2) *The difference of no two of these quantities is divisible by  $b$ .* If for example we had

$$g_1\alpha_1 + g_2\alpha_2 + \cdots + g_n\alpha_n \equiv h_1\alpha_1 + h_2\alpha_2 + \cdots + h_n\alpha_n \pmod{b},$$

then it would follow that

$$(g_1 - h_1)\alpha_1 + (g_2 - h_2)\alpha_2 + \cdots + (g_n - h_n)\alpha_n \equiv 0 \pmod{b},$$

where some of the differences  $g_r - h_r$  ( $r = 1, 2, \dots, n$ ) are not zero. Let  $r$  be the greatest of these integers such that

$$g_r - h_r \neq 0.$$

It results that

$$(g_1 - h_1)\alpha_1 + (g_2 - h_2)\alpha_2 + \cdots + (g_r - h_r)\alpha_r \equiv 0 \pmod{b},$$

and it would follow since  $g_r$  and  $h_r$  are both less than  $a_{rr}$  that

$$|g_r - h_r| < a_{rr},$$

which contradicts the definition of  $a_{rr}$  (Art. 148). Hence

the difference of no two of the above numbers is divisible by  $b$ .

(3) *Every arbitrary number that is divisible by  $a$  is congruent to one of the above numbers (mod.  $b$ ).* For let  $\alpha$  be a number divisible by  $a$  of the form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n,$$

where the  $x$ 's are rational integers. Let  $x_n$  be divided by  $a_{nn}$  giving

$$x_n = a_{nn}y_n + z_n,$$

where  $y_n$  is an integer or zero and  $z_n$  is one of the numbers  $0, 1, 2, \dots, a_{nn}-1$ . The  $\beta$ 's being defined as in the preceding article, form the number

$$\begin{aligned} \alpha - y_n\beta_n &= (x_1 - y_n a_{n1})\alpha_1 + (x_2 - y_n a_{n2})\alpha_2 \\ &\quad + \cdots + (x_n - y_n a_{nn})\alpha_n \\ &= (x_1 - y_n a_{n1})\alpha_1 + (x_2 - y_n a_{n2})\alpha_2 + \cdots + \alpha_n z_n \\ &= \alpha' + z_n\alpha_n, \end{aligned}$$

where  $\alpha'$  is a quantity of the form

$$\alpha' = x'_1\alpha_1 + x'_2\alpha_2 + \cdots + x'_{n-1}\alpha_{n-1}.$$

It follows that

$$\alpha = y_n\beta_n + z_n\alpha_n + \alpha'.$$

Applying the same process to  $\alpha'$  as we have just done to  $\alpha$ , we divide  $x'_{n-1}$  by  $a_{n-1, n-1}$ , which gives

$$x'_{n-1} = a_{n-1, n-1}y_{n-1} + z_{n-1},$$

where  $z_{n-1}$  is of the quantities  $0, 1, 2, \dots, a_{n-1, n-1}-1$ ; then as above we have

$$\alpha' = y_{n-1}\beta_{n-1} + z_{n-1}\alpha_{n-1} + \alpha'',$$

where  $\alpha''$  is linearly expressed through  $\alpha_1, \alpha_2, \dots, \alpha_{n-2}$ .

Continuing this process we have finally

$$\begin{aligned} \alpha &= y_n\beta_n + y_{n-1}\beta_{n-1} + \cdots + y_1\beta_1 \\ &\quad + z_n\alpha_n + z_{n-1}\alpha_{n-1} + \cdots + z_1\alpha_1; \end{aligned}$$

and consequently

$$\alpha \equiv z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n \pmod{b},$$



where  $z_\nu$  are of the numbers  $0, 1, \dots, a_{\nu\nu} - 1$  ( $\nu = 1, 2, \dots, n$ ). Thus it is seen that every number  $\alpha$  of the modul  $a$  is congruent to one of the above  $a_{11} \cdot a_{22} \cdot \dots \cdot a_{nn}$  numbers (mod.  $b$ ), so that these numbers form a complete system of residues of the modul  $a$  with respect to the modul  $b$ .

With this is demonstrated the correctness of the formula

$$(a, b) = a_{11} \cdot a_{22} \cdot a_{33} \cdot \dots \cdot a_{nn}.$$

The following results have been derived:

(1) If  $(a, b) \neq 0$ , none of the quantities  $a_{11}, a_{22}, \dots, a_{nn}$  is zero and  $(a, b) = a_{11} a_{22} \dots a_{nn}$ .

(2) If  $(a, b) = 0$ , at least one of the quantities  $a_{11}, a_{22}, \dots, a_{nn}$  is zero.

(3) If  $a_{11}, a_{22}, \dots, a_{nn}$  are all different from zero, then is  $(a, b) \neq 0$ .

(4) If one of the quantities  $a_{11}, a_{22}, \dots, a_{nn}$  is zero, then also  $(a, b) = 0$ .

These theorems are true only under the condition that  $b > a$ .

As a corollary of this theorem, consider a one-termed modul  $a = [\alpha]$ ; then if  $b > a$ , it follows also that  $b$  is a one-termed modul.

Let  $b = [\beta]$  and consequently

$$\beta = \beta_1 = a_{11}\alpha.$$

Since

$$a_{11} = (a, b),$$

and consequently

$$\beta = (a, b)\alpha,$$

it is evident that

$$b = (a, b)a,$$

or in other words, every multiple of a one-termed modul is a one-termed modul and has the form just written.

ART. 150. Assuming that  $b > a$  suppose next that the basis consists of the independent elements  $\alpha_1, \alpha_2, \dots, \alpha_n$ . The system of the  $n$  quantities  $\beta_1, \beta_2, \dots, \beta_n$  is defined as above, the coefficients  $a_{rt}$  forming a rectangle as given in (Art. 149). It is seen that the determinant  $|a_{rt}|$  is equal  $a_{11} \cdot a_{22} \cdot \dots \cdot a_{nn}$ , so that

$$|a_{rt}| = (a, b).$$

The quantities  $\beta_1, \beta_2, \dots, \beta_n$  as shown in the preceding article form a basis of  $b$  and are linearly independent (Art. 145) if  $|a_{rt}| \neq 0$ . In this case the order of  $b$  is the same as the order of  $a$ . On the other hand  $\beta_1, \beta_2, \dots, \beta_n$  are linearly dependent if  $|a_{rt}| = 0$  and in this case the order of  $b$  is less than the order of  $a$ .

Since  $|a_{rt}| = (a, b)$  the following theorems are thus proved:

(1) *If  $b > a$  and  $(a, b) \neq 0$ , then the basis  $\beta_1, \beta_2, \dots, \beta_n$  of  $b$  consists of  $n$  independent elements and the order of  $b$  is equal to the order of  $a$ .*

(2) *If  $b > a$  and  $(a, b) = 0$ , then the basis  $\beta_1, \beta_2, \dots, \beta_n$  of  $b$  consists of elements that are not linearly independent, and the order of  $b$  is less than the order of  $a$ .*

ART. 151. THEOREM. *If  $(a, b) \neq 0$  and if  $b$  is a finite modul, then  $a$  is also a finite modul and the order of  $a$  is not greater than the order of  $b$ .*

For let  $(a, b) = m \neq 0$ , then (see Art. 141)  $ma > b$  and consequently (Art. 148)  $ma$  is a finite modul, whose order is not greater than the order of  $b$ . Further the rank of  $ma$  is equal to the rank of  $a$ , so that the order of  $a$  is not greater than the order of  $b$ .

From the two theorems given above it follows that if  $b > a$  and  $(a, b) \neq 0$  and if one of the moduls  $a$  or  $b$  is finite, then both  $a$  and  $b$  are finite and of the same order. In this case note that  $ma > b > a$ .

ART. 152. Starting with the formula

$$(a, b) = a_{11}a_{22} \cdots a_{nn},$$

where  $b > a$ , theorems will be introduced which become more and more general until finally a means of determining  $(a, b)$  for every arbitrary case is offered.

Again let  $a$  be a finite modul of order  $n$ , and write

$$a = [\alpha_1, \alpha_2, \cdots, \alpha_n].$$

Further let  $b > a$ , and suppose that  $b$  has a basis consisting of the  $n$  elements  $\gamma_1, \gamma_2, \cdots, \gamma_n$ , which are not necessarily independent, since we have not assumed that  $(a, b) \neq 0$ . Since  $b > a$ , it follows that  $\gamma_1, \gamma_2, \cdots, \gamma_n$  may be expressed through  $\alpha_1, \alpha_2, \cdots, \alpha_n$  in the form

$$\gamma_r = c_{r1}\alpha_1 + c_{r2}\alpha_2 + \cdots + c_{rn}\alpha_n \quad (r = 1, 2, \cdots, n),$$

where  $c_{r1}, c_{r2}, \cdots, c_{rn}$  are rational integers. It is asserted under the conditions just made, viz., if  $b > a$ , that the absolute value of the determinant  $|c_{rs}|$ , that is of  $C$ , say, is equal to  $(a, b)$ . This theorem differs from the preceding one in that it is true for any arbitrary basis  $\gamma_1, \gamma_2, \cdots, \gamma_n$  of  $b$ , while the preceding theorem was true only for the special basis  $\beta_1, \beta_2, \cdots, \beta_n$ .

In the proof two cases are to be distinguished:

- (1) when  $C = 0$       and      (2) when  $C \neq 0$ .

In the *first* case where  $C = 0$ , the basal elements  $\gamma_1, \gamma_2, \cdots, \gamma_n$  are dependent (see preceding article) and consequently the order of  $b$  is less than the order of  $a$ . When this is the case it was shown (Art. 149) that  $(a, b) = 0$ .

In the *second* case where  $C \neq 0$ , the rank of  $b$  is equal  $n$ . Since  $b > a$ , we may introduce the system of  $n$  basal elements of  $b$ ,  $\beta_1, \beta_2, \cdots, \beta_n$  which was given in Art. 149, viz.,

$$\beta_r = a_{r1}\alpha_1 + a_{r2}\alpha_2 + \cdots + a_{rn}\alpha_n \quad (r = 1, 2, \cdots, n),$$

where  $a_{rt} = 0$  for  $t > r$  and where

$$(a, b) = a_{11} \cdot a_{22} \cdot \dots \cdot a_{nn} = |a_{rt}|.$$

Since the quantities  $\beta_1, \beta_2, \dots, \beta_n$  as well as the quantities  $\gamma_1, \gamma_2, \dots, \gamma_n$  form bases of  $\mathfrak{b}$ , they may be linearly expressed through one another with integral coefficients and the determinant of the coefficients is equal  $\pm 1$  (Art. 94).

Write

$$\gamma_r = \sum_{t=1}^{t=n} (b_{rt} \beta_t) \quad (r = 1, 2, \dots, n),$$

where  $b_{rt}$  are rational integers and  $|b_{rt}| = \pm 1$ . Further since

$$\beta_t = \sum_{s=1}^{s=n} (a_{ts} \alpha_s) \quad (t = 1, 2, \dots, n),$$

it is seen that

$$\gamma_r = \sum_{\substack{s=1, 2, \dots, n \\ t=1, 2, \dots, n}} (b_{rt} a_{ts} \alpha_s) \quad (r = 1, 2, \dots, n).$$

On the other hand, since

$$\gamma_r = \sum_{s=1}^{s=n} (c_{rs} \alpha_s),$$

it follows that

$$\sum_{\substack{s=1, 2, \dots, n \\ t=1, 2, \dots, n}} (b_{rt} a_{ts} \alpha_s) = \sum_{s=1}^{s=n} (c_{rs} \alpha_s),$$

As the  $\alpha$ 's are linearly independent, it is seen that

$$c_{rs} = \sum_{t=1}^{t=n} (b_{rt} a_{ts}) = b_{r1} a_{1s} + b_{r2} a_{2s} + \dots + b_{rn} a_{ns} \quad (r, s = 1, 2, \dots, n).$$

It follows from the theorem for the multiplication of determinants that

$$C = |c_{rt}| = |a_{rt}| |b_{rt}|;$$

or, since  $|b_{rt}| = \pm 1$ , it follows that

$$C = \pm |a_{rt}| = \pm (a, b)$$

and consequently  $(a, b)$  is equal to the absolute value of  $C = |c_{rs}|$ .

As an example of this theorem, take the modul of the  $n$ th order

$$a = [\alpha_1, \alpha_2, \dots, \alpha_n]$$

and for the modul  $b$  write

$$b = ka = [k\alpha_1, k\alpha_2, \dots, k\alpha_n],$$

where  $k$  is a rational integer. We then have

$$\gamma_\nu = k\alpha_\nu \quad (\nu = 1, 2, \dots, n)$$

and consequently in the above discussion

$$c_{rr} = k, \quad c_{rt} = 0, \quad (r \neq t) \quad (r, t = 0, 1, \dots, n).$$

Substituting in the determinant  $|c_{rs}|$ , it is seen that

$$(a, ka) = \begin{vmatrix} k, & 0, & 0, & \dots, & 0 \\ 0, & k, & 0, & \dots, & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & 0, & \dots, & k \end{vmatrix} = k^n;$$

or, if  $a$  is a finite modul of order  $n$  and  $k$  is any rational integer, then is

$$(a, ka) = k^n.$$

ART. 153. In the proof of the theorem indicated in the formula

$$(a, b) = \pm |c_{rs}| = |C|$$

it was assumed that  $b > a$  and consequently that the quantities  $c_{rs}$  were rational integers. We now do away with the restriction that  $c_{rs}$  are rational integers in that they are allowed to be any rational numbers, and it is no longer assumed that  $b > a$ . From now on it is assumed that  $a$  and  $b$  are finite moduls and that

$$a = [\alpha_1, \alpha_2, \dots, \alpha_n], \\ b = [\beta_1, \beta_2, \dots, \beta_n].$$

The  $n$  basal elements  $\alpha_1, \alpha_2, \dots, \alpha_n$  are supposed to be linearly independent but this assumption is *not* made for the basal elements  $\beta_1, \beta_2, \dots, \beta_n$  of  $b$ . However, it is assumed that there exist integral or fractional rational



numbers  $c_{rs}$  such that

$$\beta_r = c_{r1}\alpha_1 + c_{r2}\alpha_2 + \cdots + c_{rn}\alpha_n \quad (r = 1, 2, \cdots, n).$$

With these more general assumptions we cannot at first compute the value of  $(a, b)$ , but the value of the quotient  $\frac{(a, b)}{(b, a)}$  may be derived.

It is asserted that, under the assumptions just stated,

$$\frac{(a, b)}{(b, a)} = |C|,$$

where  $|C|$  denotes the absolute value of the determinant  $C = |c_{rs}|$ . Observe that this formula is true for the case that  $C = 0$  (see again Art. 154) since then  $(a, b) = 0$  as already seen in Art. 150, and further it is true for the case  $b > a$ , for in this case  $(b, a) = 1$  (Art. 138) and consequently  $(a, b) = |C|$ , the quantities  $c_{rs}$  being integers.

To prove the more general case let  $k$  be the least common multiple of the denominators of the fractions  $c_{rs}$  so that the product  $kc_{rs}$  is a rational integer. It results that

$$k\beta_r = kc_{r1}\alpha_1 + kc_{r2}\alpha_2 + \cdots + kc_{rn}\alpha_n \quad (r = 1, 2, \cdots, n).$$

It follows that  $k\beta_1, k\beta_2, \cdots, k\beta_n$ , which quantities also form a basis of  $k\mathfrak{b}$ , may be linearly expressed with integral coefficients through  $\alpha_1, \alpha_2, \cdots, \alpha_n$ . It is thus also shown that

$$kb > a$$

and consequently from the preceding theorem,

$$(a, kb) = \pm |kc_{rs}| = \pm k^n |c_{rs}| = \pm k^n C.$$

Next write

$$a + b = \mathfrak{b}.$$

Since  $a > \mathfrak{b}$  and  $kb > a$ , it follows from Art. 139 that

$$(b, kb) = (b, a)(a, kb);$$

and since  $b > \mathfrak{b}$  and  $kb > b$ , it is also seen that

$$(b, kb) = (b, \mathfrak{b})(\mathfrak{b}, kb).$$

Further since

$$\begin{aligned} (\mathfrak{b}, \mathfrak{a}) &= (\mathfrak{b}, \mathfrak{a}) \quad (\text{Art. 137}), & (\mathfrak{a}, k\mathfrak{b}) &= \pm k^n C, \\ (\mathfrak{b}, \mathfrak{b}) &= (\mathfrak{a}, \mathfrak{b}), & (\mathfrak{b}, k\mathfrak{b}) &= k^n, \end{aligned}$$

it follows that

$$\pm (\mathfrak{b}, \mathfrak{a}) k^n C = (\mathfrak{a}, \mathfrak{b}) k^n,$$

or

$$\frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})} = \pm C = |C|,$$

as  $\frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})}$  is a *positive* number.

ART. 154. It may be shown that if  $C = 0$ , then also  $(\mathfrak{a}, \mathfrak{b}) = 0$ . For if  $C = 0$ , then  $\beta_1, \beta_2, \dots, \beta_n$  are linearly dependent, and consequently the order of  $\mathfrak{b}$  is less than the order of  $\mathfrak{a}$ , that is, less than  $n$ . It follows also that the order of the modul  $k\mathfrak{b}$  is less than  $n$ . But since  $k\mathfrak{b} > \mathfrak{a}$ , it follows from Art. 150 that

$$(\mathfrak{a}, k\mathfrak{b}) = 0.$$

Hence in the formula given in the preceding article, viz.,

$$(\mathfrak{b}, \mathfrak{a})(\mathfrak{a}, \mathfrak{f}\mathfrak{b}) = (\mathfrak{b}, \mathfrak{b})(\mathfrak{b}, \mathfrak{f}\mathfrak{b}),$$

it is seen that

$$(\mathfrak{b}, \mathfrak{b})(\mathfrak{b}, \mathfrak{f}\mathfrak{b}) = 0.$$

But since

$$(\mathfrak{b}, k\mathfrak{b}) = k^r,$$

where  $r$  is the order of  $\mathfrak{b}$ , it follows that  $(\mathfrak{b}, \mathfrak{b}) = 0$ , or since  $(\mathfrak{b}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{b})$ ,

$$(\mathfrak{a}, \mathfrak{b}) = 0.$$

ART. 155. LEMMA. Let  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_p$  be two bases of one and the same finite modul  $\mathfrak{a}$  so that

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n] = [\beta_1, \beta_2, \dots, \beta_p];$$

and further assume that  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, so that  $n$  is the rank of  $\mathfrak{a}$  while  $p \geq n$ .

We then have

$$\alpha_r = \sum_{t=1}^{t=p} (a_{rt}\beta_t) \quad (r = 1, 2, \dots, n),$$

$$\beta_t = \sum_{s=1}^{s=n} (b_{st}\alpha_s) \quad (t = 1, 2, \dots, p),$$

where  $a_{tr}$  and  $b_{ts}$  are rational integers. It follows that

$$\alpha_r = \sum_{\substack{t=1, 2, \dots, p \\ s=1, 2, \dots, n}} (a_{rt}b_{ts}\alpha_s).$$

Since  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, it is evident that

$$\sum_{t=1}^{t=p} a_{rt}b_{st} = e_{rs} \quad (r, s = 1, 2, \dots, n),$$

where  $e_{rs} = 0$  for  $r \neq s$  and  $e_{rs} = 1$  for  $r = s$ . This expression may be written

$$a_{r1}b_{s1} + a_{r2}b_{s2} + a_{r3}b_{s3} + \dots + a_{rp}b_{sp} = e_{rs} \quad (r, s = 1, 2, \dots, n).$$

It is then clear that

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{np} \end{vmatrix} \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2p} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{np} \end{vmatrix} = \begin{vmatrix} e_{11} & e_{12} & \dots & e_{1n} \\ e_{21} & e_{22} & \dots & e_{2n} \\ \dots & \dots & \dots & \dots \\ e_{n1} & e_{n2} & \dots & e_{nn} \end{vmatrix} = 1.$$

Denoting any determinant formed by taking  $n$  columns of the system  $a_{tr}$  by  $A$  and any determinant formed by taking  $n$  columns of the system  $b_{st}$  by  $B$ , the expression just written is

$$\sum(A \cdot B) = 1.$$

It follows that all determinants formed by taking  $n$  columns from the system  $a_{tr}$ , in number  $= \binom{p}{n}$ , have no common di-

visor save unity, the same being also true of the determinants formed by taking  $n$  columns from the system  $b_{st}$ .

A special case of this theorem was treated in Art. 94 where  $p = n$ . In this case there was only one determinant formed from the system  $a_{tr}$  and only one from the system  $b_{st}$  and both these determinants had the value  $\pm 1$ .

ART. 156. Let  $\mathfrak{a}$  and  $\mathfrak{b}$  be two moduls of finite order,

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n],$$

$$\mathfrak{b} = [\beta_1, \beta_2, \dots, \beta_p];$$

and let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be linearly independent, the order of  $\mathfrak{a}$  being  $n$ , while  $p \geq n$ . Further assume that there are  $pn$  rational numbers  $c_{ts}$  such that

$$\beta_t = c_{t1}\alpha_1 + c_{t2}\alpha_2 + \dots + c_{tn}\alpha_n \quad (t=1, 2, \dots, p),$$

and that is, the elements  $\beta_1, \beta_2, \dots, \beta_p$  by hypothesis may be expressed linearly with rational coefficients in terms of the  $\alpha$ 's. It is asserted:

*The greatest common divisor of all the determinants of the  $n$ th order which are had from the system  $c_{ts}$  by taking  $n$  columns is in absolute value equal to  $\frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})}$ .*

The special case  $p = n$  was proved in Art. 153.

In the proof of the more general theorem, two cases are to be distinguished; (1) where the determinants of the  $n$ th order formed by taking  $n$  rows of the system  $c_{ts}$  are not all zero. In this case there are among the  $p$  quantities  $\beta_1, \beta_2, \dots, \beta_p$   $n$  independent, and the order of the modul  $\mathfrak{b}$  is  $n$  (Art. 148). Accordingly the modul  $\mathfrak{b}$  has a basis consisting of  $n$  independent elements, say

$$\mathfrak{b} = [\gamma_1, \gamma_2, \dots, \gamma_n].$$

It follows that  $\beta_1, \beta_2, \dots, \beta_p$  may be linearly expressed through the  $\gamma$ 's with integral coefficients in the form

$$(1) \quad \beta_t = \sum_{s=1}^{s=n} a_{ts} \gamma_s \quad (t=1, 2, \dots, p),$$

where the quantities  $a_{ts}$  are rational integers and the greatest common divisor of the determinants of the  $n$ th order formed from the system  $a_{ts}$  is, from the lemma in the preceding article, equal to 1.

The quantities  $\gamma_1, \gamma_2, \dots, \gamma_n$  may be expressed through the  $\beta$ 's and consequently through the  $\alpha$ 's in the form, say

$$(2) \quad \gamma_s = b_{s1}\alpha_1 + b_{s2}\alpha_2 + \dots + b_{sn}\alpha_n = \sum_{\tau=1}^{\tau=n} b_{s\tau}\alpha_\tau \quad (s = 1, 2, \dots, p),$$

where  $b_{sr}$  are rational numbers.

If we put the absolute value of the determinant  $|b_{sr}| = B$ , it follows from Art. 153, that

$$B = \frac{(a, b)}{(b, a)}.$$

It is further seen from (1) and (2) that

$$\beta_t = \sum_{\substack{r=1, 2, \dots, n \\ s=1, 2, \dots, n}} (a_{ts}b_{sr}\alpha_r) \quad (t = 1, 2, \dots, p).$$

On the other hand, since

$$\beta_t = \sum_{r=1, 2, \dots, n} (c_{tr}\alpha_r),$$

it results that

$$(3) \quad c_{tr} = \sum_{s=1, 2, \dots, n} (a_{ts}b_{sr}) \quad (t = 1, 2, \dots, p).$$

Of the  $p$  numbers  $1, 2, \dots, p$  choose  $n$  and denote them by  $t_1, t_2, \dots, t_n$ . It follows at once from (3) that

$$\begin{vmatrix} c_{t_1,1} & c_{t_1,2} & \dots & c_{t_1,n} \\ c_{t_2,1} & c_{t_2,2} & \dots & c_{t_2,n} \\ \dots & \dots & \dots & \dots \\ c_{t_n,1} & c_{t_n,2} & \dots & c_{t_n,n} \end{vmatrix} = \begin{vmatrix} a_{t_1,1} & a_{t_1,2} & \dots & a_{t_1,n} \\ a_{t_2,1} & a_{t_2,2} & \dots & a_{t_2,n} \\ \dots & \dots & \dots & \dots \\ a_{t_n,1} & a_{t_n,2} & \dots & a_{t_n,n} \end{vmatrix} \cdot B.$$

Since the numbers  $t_1, t_2, \dots, t_n$  may be chosen from the numbers  $1, 2, \dots, p$  in  $\binom{p}{n}$  ways, we have  $\binom{p}{n}$  equations like the one just written. These  $\binom{p}{n}$  equations show, since the determinants on the right hand side formed



from the system  $a_{t_s}$  have unity as their greatest common divisor, that the determinants of the  $n$ th order formed by taking  $n$  columns of the system  $c_{t_s}$  have  $B$  for their greatest common divisor, where

$$|B| = \frac{(a, b)}{(b, a)}.$$

(2) In the second case the determinants of the  $n$ th order formed from the system  $c_{t_s}$  are all supposed to be zero. In this case it is asserted that  $(a, b) = 0$ . For of the  $p$  quantities

$$\beta_1, \beta_2, \dots, \beta_p$$

select any  $n$ , say

$$\beta_{t_1}, \beta_{t_2}, \dots, \beta_{t_n}.$$

These quantities are linearly dependent since by hypothesis the determinant formed from the system  $c_{t_s}$  is zero. It follows that the order of  $b$  is less than the order of  $a$ . It was proved in Art. 151 that if  $(a, b) \neq 0$  and if  $b$  is of finite order, then the order of  $b$  is *not* less than the order of  $a$ . It follows that  $(a, b)$  must equal zero.

ART. 157. Let  $a, b$  be two moduls of the rank  $n$ , say

$$\begin{aligned} a &= [\alpha_1, \alpha_2, \dots, \alpha_n], \\ b &= [\beta_1, \beta_2, \dots, \beta_n], \end{aligned}$$

where  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_n$  are linearly independent systems; further suppose that each system of these  $n$  quantities may be linearly expressed in terms of the other with rational coefficients, so that, say

$$\beta_r = \sum_{s=1}^{s=n} c_{rs} \alpha_s \quad (r=1, 2, \dots, n),$$

where  $c_{rs}$  are rational numbers and  $C = |c_{rs}| \neq 0$ .

It was proved above that

$$\pm C = \frac{(a, b)}{(b, a)},$$

and consequently the quotient  $\frac{(a, b)}{(b, a)}$  is known. This formula presents  $(a, b)$  after  $(b, a)$  has been found. To determine  $(b, a)$ , let

$$b = a + b = [\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n].$$

The  $2n$  elements of  $b$  may be expressed linearly with rational coefficients through  $\alpha_1, \alpha_2, \dots, \alpha_n$  in the form

$$\left. \begin{aligned} \beta_r &= c_{r1}\alpha_1 + c_{r2}\alpha_2 + \dots + c_{rn}\alpha_n, \\ \alpha_r &= e_{r1}\alpha_1 + e_{r2}\alpha_2 + \dots + e_{rn}\alpha_n, \end{aligned} \right\} \quad (r = 1, 2, \dots, n),$$

where  $e_{rs} = 0$  for  $r \neq s$  and  $e_{rs} = 1$  for  $r = s$ . If then of the system of coefficients

$$\begin{array}{cccccc} c_{11} & c_{12} & c_{13} & \dots & c_{1n} \\ c_{21} & c_{22} & c_{23} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ c_{n1} & c_{n2} & c_{n3} & \dots & c_{nn} \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1, \end{array}$$

all possible determinants of the  $n$ th order are formed, and if their greatest common divisor  $d$  is determined, then as seen in Art. 156,

$$d = \frac{(a, b)}{(b, a)} = \frac{1}{(b, a)},$$

since  $a > b$ , so that  $(a, b) = 1$  (Art. 138). Hence

$$d = \frac{1}{(b, a)}$$

(Art. 137).

By the use of this formula the number  $(a, b)$  may be determined. The fact that in each of the  $n$  last lines of the above system of coefficients appear only zeros with the exception of a single unit, permits the theorem as expressed in the last formula to be stated as follows:

The number  $(b, a)$  is the common denominator of all the fractions which are had through the formation of all the sub-determinants of every order of the system  $c_{ts}$  ( $t=1, 2, \dots, n$ ;  $s=1, 2, \dots, n$ ).

ART. 158. It is evident from what follows that if  $a$  and  $b$  are finite moduls, then also  $a-b$ ,  $a+b$ ,  $a \cdot b$ ,  $\frac{a}{b}$  are finite moduls.

(1)  $a-b$  is a finite modul, since  $a-b > a$  (Art. 117).

(2)  $a+b$  is a finite modul, since, if

$$a = [\alpha_1, \alpha_2, \dots, \alpha_n], \quad b = [\beta_1, \beta_2, \dots, \beta_m],$$

then

$$a+b = [\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m]$$

is finite.

Through repetitions of (1) and (2) it is seen that if  $a_1, a_2, \dots, a_r$  are finite moduls, then also  $a_1+a_2+a_3+\dots+a_r$  and  $a_1-a_2-a_3-\dots-a_r$  are finite moduls.

(3)  $a \cdot b$  is a finite modul, for

$$a \cdot b = \alpha_1 b + \alpha_2 b + \dots + \alpha_n b,$$

or

$$a \cdot b = [\alpha_1 \beta_1, \alpha_1 \beta_2, \dots, \alpha_1 \beta_m, \alpha_2 \beta_1, \dots, \alpha_n \beta_m]$$

(Art. 122).

(4)  $\frac{a}{b}$  is a finite modul, for

$$\frac{a}{b} = \beta_1^{-1} a - \beta_2^{-1} a - \dots - \beta_m^{-1} a$$

(Art. 130). As a special case of (4)  $\frac{a}{a} = a^0$  is a finite modul; that is, the order-modul of a finite modul is finite (Art. 132).

## CHAPTER VII

### ALGEBRAIC MODULS

**ART. 159. Definitions.** (1) A finite modul  $a$  is called an *algebraic* modul if all the numbers that are divisible by  $a$  are algebraic. (2) An algebraic modul  $a$  is an *integral algebraic* modul if all the quantities that are divisible by  $a$  are algebraic integers. (3) An integral algebraic modul  $a$  is a *unit-modul* if  $1$  is divisible by  $a$ , and that is if the modul  $[1]$  is divisible by the modul  $a$ .

These definitions are limited to finite moduls. To show that a finite modul is algebraic, it is necessary only to show that it has a basis which consists wholly of algebraic numbers; and to show that a finite modul is an integral algebraic modul, it must be proved that the modul has a basis whose elements are all algebraic integers.

In virtue of the above definitions, the following theorems are at once presented:

(1) If  $a$  and  $b$  are algebraic moduls, then  $a - b$ ,  $a + b$ ,  $a \cdot b$  and  $\frac{b}{a}$  are algebraic moduls.

(2) If  $a$  and  $b$  are two integral algebraic moduls then  $a - b$ ,  $a + b$  and  $ab$  are integral algebraic moduls.

(3) If  $a$  and  $b$  are unit-moduls, then also  $a - b$ ,  $a + b$ ,  $ab$  are unit-moduls.

The quotient of two integral algebraic moduls is in general *not* an integral algebraic modul. On the other hand the quotient of two algebraic moduls is always an algebraic modul; and a special case is the theorem:





for

$$\eta a = [\eta, \eta^2, \eta^3, \dots, \eta^n] \\ = [\eta, \eta^2, \dots, \eta^{n-1}, c_1\eta^{n-1} + c_2\eta^{n-2} + \dots + c_n];$$

and it is seen that all the basal elements of this modul are divisible by  $a$ . It therefore follows that

$$\eta a > a.$$

Further if  $\eta a > a$  then  $\eta$  is divisible by  $\frac{a}{a} = a^0$  and *vice versa*.

It is thus shown that  $\eta$  is an algebraic integer *when and only when, it is divisible by the order-modul of a finite modul*. This offers a third and the best definition of an algebraic integer.

**ART. 161. THEOREM.** *If  $a$  is a finite modul and  $b$  a modul which is divisible by  $a$ , then  $\frac{b}{a}$  is an integral algebraic modul.*

For if  $\eta$  is a number that is divisible by  $\frac{b}{a}$ , then in virtue of the definition (Art. 129) of  $\frac{b}{a}$  we have  $\eta a > b$ , and consequently since  $b > a$ , it follows also that  $\eta a > a$ . Hence every number  $\eta$  that is divisible by  $\frac{b}{a}$  is an algebraic integer, so that  $\frac{b}{a}$  is an integral algebraic modul. This may also be proved by means of a determinant as at the beginning of Art. 160.

**ART. 162.** Use may be made of the definitions and theorems given in the preceding articles, to prove the theorems already derived (Art. 88) regarding algebraic integers:

**THEOREM I.** *If  $\alpha$  and  $\beta$  are two algebraic integers, then also  $\alpha + \beta$  and  $\alpha - \beta$  are algebraic integers.*

For if  $\alpha$  and  $\beta$  are two algebraic integers, there are two moduls, say  $a$  and  $b$ , such that

$$\alpha a > a \quad \text{and} \quad \beta b > b;$$

and since

$$b > b \quad \text{and} \quad a > a,$$

it follows that

$$\alpha a b > a b \quad \text{and} \quad \beta a b > a b.$$

If then  $\gamma$  is a number divisible by the modul  $ab$  which stands on the left of the expressions just written, then  $\alpha\gamma$  and  $\beta\gamma$  and consequently  $\alpha\gamma \pm \beta\gamma = (\alpha \pm \beta)\gamma$  is divisible by  $ab$ . Since this is true for every number  $\gamma$  that is divisible by  $ab$ , it follows that

$$(\alpha \pm \beta)ab > ab,$$

and consequently  $\alpha \pm \beta$  is an algebraic integer.

**THEOREM II.** *If  $\alpha$  and  $\beta$  are algebraic integers, then also  $\alpha\beta$  is an algebraic integer.*

For if  $\alpha$  and  $\beta$  are algebraic integers, there are two moduls  $a$  and  $b$  such that

$$\alpha a > a \quad \text{and} \quad \beta b > b,$$

and further

$$\beta b > \beta b \quad \text{and} \quad a > a.$$

It follows that

$$\alpha\beta ab > \beta ab \quad \text{and} \quad \beta ab > ab$$

and consequently  $\alpha\beta ab > ab$ , so that  $\alpha\beta$  is an algebraic integer.

**THEOREM III.** *If  $\omega$  satisfies an algebraic equation in which the highest coefficient = 1 and the other coefficients are algebraic integers, then is  $\omega$  an algebraic integer.*

For suppose that  $\omega$  satisfies the equation

$$\omega^n = \alpha_1 \omega^{n-1} + \alpha_2 \omega^{n-2} + \dots + \alpha_n.$$

Since  $\alpha_1, \alpha_2, \dots, \alpha_n$  are supposedly algebraic integers, there must be  $n$  moduls  $a_1, a_2, \dots, a_n$  such that

$$\alpha_\nu a_\nu > a_\nu \quad (\nu = 1, 2, \dots, n).$$

Note that

$$a_2 a_3 a_4 \cdots a_n > a_2 a_3 \cdots a_n$$

and also that

$$\alpha_1 a_1 > a_1.$$

It follows that

$$\alpha_1 a_1 a_2 \cdots a_n > a_1 a_2 \cdots a_n;$$

or if we put

$$a = a_1 a_2 \cdots a_n,$$

then is

$$\alpha_1 a > a.$$

In a similar manner it is seen that

$$\alpha_\nu a > a \quad (\nu = 1, 2, \dots, n).$$

If  $\alpha$  is a number divisible by the modul  $a$  on the left of this expression, then also the numbers  $\alpha_\nu \alpha$  ( $\nu = 1, 2, \dots, n$ ) are divisible by  $a$ . Next let  $b$  be a finite modul such that

$$b = [1, \omega, \omega^2, \dots, \omega^{n-1}].$$

It is evident that the numbers  $\omega^{n-\nu}$  ( $\nu = 1, 2, \dots, n$ ) are divisible by  $b$  and consequently the numbers  $\alpha_\nu \omega^{n-\nu} \alpha$  are divisible by  $ab$ . It is further seen that  $(\alpha_1 \omega^{n-1} + \alpha_2 \omega^{n-2} + \dots + \alpha_n) \alpha$  or  $\omega^n \alpha$  is divisible by  $ab$ . Since this is true of every number  $\alpha$  that is divisible by  $a$  it follows that

$$\omega^n a > ab.$$

It is evident also that

$$\omega b = [\omega, \omega^2, \dots, \omega^n];$$

and consequently  $\omega b a$  is the greatest common divisor (Art. 119) of  $\omega a, \omega^2 a, \omega^3 a, \dots, \omega^n a$ , or

$$\omega a b = \omega a + \omega^2 a + \dots + \omega^n a.$$

On the other hand since  $\omega, \omega^2, \dots, \omega^{n-1}$  are all divisible by  $b$ , it follows that

$$\omega a > ab, \quad \omega^2 a > ab, \quad \dots, \quad \omega^{n-1} a > ab.$$

Further as we have just seen,  $\omega^n a > ab$ . It results that

$$\omega a + \omega^2 a + \dots + \omega^n a \quad \text{or} \quad \omega a b > ab.$$

On the other hand,  $ab$  being the product of two finite moduls, is a finite modul. Hence  $\omega$  is an algebraic integer.



Since

$$f(t) = (t - \vartheta)(\eta_0 + \eta_1 t + \eta_2 t^2 + \cdots + \eta_{n-1} t^{n-1}),$$

it is seen that

$$(2) \quad a_{n-r} = \eta_{n-r-1} - \vartheta \eta_r.$$

If the quantities  $a_0, a_1, a_2, \dots, a_{n-1}, a_n$  are rational integers, the lemma consists in proving that

$$\eta_0, \eta_1, \dots, \eta_{n-1}, \eta_0 \vartheta, \eta_1 \vartheta, \dots, \eta_{n-1} \vartheta$$

are algebraic integers.

Write

$$c = [1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}].$$

That the quantities

$$\eta_{n-r-1} \vartheta^s \quad \left( \begin{array}{l} r=0, 1, \dots, n-1 \\ s=0, 1, \dots, n \end{array} \right)$$

are divisible by  $c$  is seen by observing that

$$\eta_{n-r-1} \vartheta^s = a_0 \vartheta^{r+s} + a_1 \vartheta^{r+s-1} + \cdots + a_r \vartheta^s.$$

When  $r+s \leq n-1$ , the quantity  $\eta_{n-r-1} \vartheta^s$  is linearly expressed through the basal elements of  $c$ . If, however,  $r+s > n-1$ , the different powers of  $\vartheta$  which appear on the right must be decreased by means of the equation  $f(\vartheta) = 0$ , and thus  $\eta_{n-r-1} \vartheta^s$  is reduced to the form  $b_0 + b_1 \vartheta + \cdots + b_{n-1} \vartheta^{n-1}$ , where the  $b$ 's are rational integers. Hence in all cases  $\eta_{n-r-1} \vartheta^s$  is divisible by the modul  $c$ . We have thus shown that

$$\eta_{n-r-1}, \eta_{n-r-1} \vartheta, \eta_{n-r-1} \vartheta^2, \dots, \eta_{n-r-1} \vartheta^{n-1}, \eta_{n-r-1} \vartheta^n$$

are all divisible by the modul  $c$ . From this it follows that

$$(1) \quad [\eta_{n-r-1}, \eta_{n-r-1} \vartheta, \eta_{n-r-1} \vartheta^2, \dots, \eta_{n-r-1} \vartheta^{n-1}] > c,$$

or

$$\eta_{n-r-1} c > c,$$

and consequently  $\eta_{n-r-1}$  is an algebraic integer. Similarly it is seen that

$$(2) \quad [\eta_{n-r-1} \vartheta, \eta_{n-r-1} \vartheta^2, \dots, \eta_{n-r-1} \vartheta^n] > c,$$

or

$$\eta_{n-r-1} \vartheta c > c,$$

and consequently  $\eta_{n-r-1} \vartheta$  is an algebraic integer.



The Dedekind Theorem may now be proved by the inductive method. Consider first the modul consisting of one basal element.

If  $a = [\alpha]$  is a modul belonging to the realm of rationality  $\Omega$ , then  $b = \left[ \frac{1}{\alpha} \right]$  is also a modul belonging to the same realm and it is seen that

$$ab = \left[ \alpha \cdot \frac{1}{\alpha} \right] = [1],$$

so that the product  $ab$  is a unit-modul.

Consider next the *special* two-termed modul,

$$a = [1, \vartheta],$$

where  $\vartheta$  is any arbitrary algebraic quantity which satisfies, say, the algebraic equation

$$a_0\vartheta^n + a_1\vartheta^{n-1} + \dots + a_{n-1}\vartheta + a_n = 0,$$

in which the  $a$ 's are rational integers without a greatest common divisor other than unity. If the system of quantities  $\eta_0, \eta_1, \eta_2, \dots, \eta_{n-1}$  are defined as at the beginning of this article, and if the modul  $[ \eta_0, \eta_1, \eta_2, \dots, \eta_{n-1} ] = b$ , say, is formed, it is seen that

$$ab = [1, \vartheta][\eta_0, \eta_1, \dots, \eta_{n-1}],$$

and it is asserted that

$$ab = [\eta_0, \eta_1, \eta_2, \dots, \eta_{n-1}, \eta_0\vartheta, \eta_1\vartheta, \dots, \eta_{n-1}\vartheta] = u,$$

where  $u$  is a unit modul. For the elements of  $u$ , that is  $\eta_0, \eta_1, \dots, \eta_{n-1}\vartheta$ , are all algebraic integers in virtue of the lemma just proved, and consequently this modul contains only algebraic integers. Further 1 is divisible by  $u$ , for owing to the formula (2), namely

$$\eta_{r-1} - \vartheta\eta_r = a_{n-r} \quad (r=1, \dots, n),$$

it is seen that  $a_0, a_1, \dots, a_{n-1}$  are all divisible by  $u$  as is also  $a_n$  which, see equation (1), is  $\eta_0\vartheta$ . Since these integers have by hypothesis no common divisor, we may always

determine rational integers  $x_0, x_1, \dots, x_n$  such that

$$a_0x_0 + a_1x_1 + \dots + a_nx_n = 1.$$

It follows that 1 is divisible by  $u$  and that  $ab = u$  is a unit modul.

Consider next the *general* two-termed modul  $a = [\alpha, \beta]$ . In this modul write  $\vartheta = \beta/\alpha$  so that  $a = [\alpha, \alpha\vartheta] = \alpha[1, \vartheta]$ . If again the quantities  $\eta_0, \eta_1, \eta_2, \dots, \eta_{n-1}$  are defined through the system of equations (Art. 163), and if we write

$$b = \left[ \frac{1}{\alpha}\eta_0, \frac{1}{\alpha}\eta_1, \frac{1}{\alpha}\eta_2, \dots, \frac{1}{\alpha}\eta_{n-1} \right] = \frac{1}{\alpha}[\eta_0, \eta_1, \dots, \eta_{n-1}],$$

then

$$ab = [1, \vartheta][\eta_0, \eta_1, \dots, \eta_{n-1}] = u,$$

where  $u$  is, as just shown, a unit modul.

It remains to prove the theorem when  $n \geq 3$ . Assume that the theorem has been proved for moduls of orders 1, 2, 3, 4,  $\dots$ ,  $n-1$ , and then show that it is true for moduls of the  $n$ th order; or better expressed, show that the theorem is also true for moduls whose bases consist of  $n$  elements.

Suppose that the modul  $a$  which belongs to a fixed realm  $\Omega$  has a basis consisting of  $n$  elements. Distribute these  $n$  elements into three groups where in each group there is at least one element and consequently in no two groups combined are there more than  $n-1$  elements. This distribution may be seen in the following modul

$$a = [\alpha, \alpha', \alpha'', \dots, \beta, \beta', \beta'', \dots, \gamma, \gamma', \gamma'', \dots].$$

Write

$$a_1 = [\alpha, \alpha', \alpha'', \dots], \quad a_2 = [\beta, \beta', \beta'', \dots], \\ a_3 = [\gamma, \gamma', \gamma'', \dots]$$

so that

$$a = a_1 + a_2 + a_3.$$

Each of the three moduls  $a_1 + a_2$ ,  $a_1 + a_3$ ,  $a_2 + a_3$  has a basis consisting of at most  $n-1$  elements; hence, in accord

with the above assumption, there are in the realm  $\Omega$  three moduls  $b_1, b_2, b_3$  such that

$$b_1(a_2 + a_3) = u_1, \quad b_2(a_3 + a_1) = u_2, \quad b_3(a_1 + a_2) = u_3,$$

where  $u_1, u_2, u_3$  are unit moduls.

It follows that

$$(a_2 + a_3)(a_3 + a_1)(a_1 + a_2)b_1b_2b_3 = u_1u_2u_3 = u;$$

and since  $u$  is the product of three unit moduls, it is itself a unit modul.

Further note the formula of Art. 127, namely

$$(a_2 + a_3)(a_3 + a_1)(a_1 + a_2) = (a_1 + a_2 + a_3)(a_1a_2 + a_2a_3 + a_3a_1).$$

If we put

$$(a_1a_2 + a_2a_3 + a_3a_1)b_1b_2b_3 = b,$$

it follows that

$$(a_1 + a_2 + a_3)b = ab = u$$

and as  $b$  is a finite modul belonging to the given realm  $\Omega$ , the Dedekind Theorem is proved.

Dedekind gives a somewhat different proof of this theorem in Dirichlet's *Zahlentheorie*, 4<sup>th</sup> edition, p. 528.

If the nomenclature employed in the modul theory is disregarded, the above theorem may be stated as follows: If  $\alpha_1, \alpha_2, \dots, \alpha_n$  are  $n$  numbers of the realm  $\Omega$ , there are in the same realm  $n$  other numbers  $\beta_1, \beta_2, \dots, \beta_n$  such that

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \dots + \alpha_n\beta_n = 1$$

and the quantities  $\alpha_r\beta_s$  ( $r, s = 1, 2, \dots, n$ ) are all integers, although in general  $\beta_1, \beta_2, \dots, \beta_n$  are *not* integers.

#### MODULS OF THE $n$ TH ORDER IN REALMS OF THE $n$ TH DEGREE

ART. 164. An algebraic realm  $\Omega$  of the  $n$ th degree consists of all rational functions of a root of an irreducible algebraic equation of the  $n$ th degree (Art. 44). Let  $m$  be the order of a finite modul whose elements belong to the realm  $\Omega$ . It is evident that  $m$  cannot be greater than  $n$ ;

for if this were the case, there would be  $m(>n)$  linearly independent quantities in  $\Omega$ . This is not possible, since the number of linearly independent quantities in  $\Omega$  is at most  $n$  (Art. 54). Hence the order of a modul whose elements belong to a realm of the  $n$ th degree is  $\leq n$ .

We shall next consider moduls of a realm  $\Omega$  of the  $n$ th degree, whose order is  $n$ . Let  $[\alpha_1, \alpha_2, \dots, \alpha_n]$  be a modul of order  $n$  which belongs to  $\Omega$ . These quantities must therefore be linearly independent and consequently form a basis not only of the modul but also of the realm  $\Omega$  to which the modul belongs. All numbers which are divisible by the modul  $[\alpha_1, \alpha_2, \dots, \alpha_n]$  may be expressed in the form  $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$ , where  $x_1, x_2, \dots, x_n$  are rational integers; while all the quantities belonging to the realm  $\Omega$  may be expressed in the form  $\alpha_1 r_1 + \alpha_2 r_2 + \dots + \alpha_n r_n$ , where  $r_1, r_2, \dots, r_n$  are rational numbers. If then  $\beta$  is an arbitrary number of the realm  $\Omega$ , it may be expressed in the form

$$\beta = \alpha_1 r_1 + \alpha_2 r_2 + \dots + \alpha_n r_n.$$

Let  $r$  be the least common multiple of the denominators of  $r_1, r_2, \dots, r_n$ . We then have

$$\beta r = \alpha_1 r r_1 + \alpha_2 r r_2 + \dots + \alpha_n r r_n,$$

where  $r r_1, r r_2, \dots, r r_n$  are rational integers. It follows that  $\beta r$  is divisible by the modul  $[\alpha_1, \alpha_2, \dots, \alpha_n]$ , which modul may be represented by  $\mathfrak{a}$ . It is thus proved that *every number of the realm  $\Omega$  may through multiplication by a rational integer be transformed into a number that is divisible by  $\mathfrak{a}$ .*

Let  $\mathfrak{b} = [\beta_1, \beta_2, \dots, \beta_n]$  be a second modul of the  $n$ th order in the same realm  $\Omega$  of the  $n$ th degree. Since the quantities  $\beta_1, \beta_2, \dots, \beta_n$  belong to the realm  $\Omega$ , there are  $n$  rational integers  $s_1, s_2, \dots, s_n$  such that

$$s_1 \beta_1, s_2 \beta_2, \dots, s_n \beta_n$$

are divisible by the modul  $a$ . Let  $s$  be the least common multiple of the  $n$  integers  $s_1, s_2, \dots, s_n$ , so that  $\frac{s}{s_1}, \frac{s}{s_2}, \dots, \frac{s}{s_n}$  are integers. It results that

$$\frac{s}{s_1}s_1\beta_1, \quad \frac{s}{s_2}s_2\beta_2, \quad \dots, \quad \frac{s}{s_n}s_n\beta_n,$$

or

$$s\beta_1, s\beta_2, \dots, s\beta_n$$

and consequently also  $sb$  is divisible by  $a$ . The following theorem is thus presented:

*If  $a$  and  $b$  are two moduls of the  $n$ th order in a realm of the  $n$ th degree, there is always an integer  $r$  such that  $rb > a$ , where  $r \neq 0$ .*

From this theorem follows an important consequence, namely, the integer represented by the symbol  $(a, b)$ , for the case that  $a$  and  $b$  are two moduls of the  $n$ th order in a realm of the  $n$ th degree, is different from zero. For on the one hand, in virtue of the theorem just proved,  $ra > b$  and on the other hand, since  $r$  is a rational integer,  $ra > a$ . If we put  $m = a - b$ , then is  $ra > m$ . Further since  $m > a$  and  $ra > m$ , it follows that (Art. 139)

$$(a, m)(m, ra) = (a, ra).$$

On the other hand, since  $(a, m) = (a, b)$  (Art. 137) and  $(a, ra) = r^n$  (Art. 152), it results that

$$(a, b)(m, ra) = r^n;$$

and, since  $r \neq 0$ , we must also have

$$(a, b) \neq 0.$$

**ART. 165. THEOREM.** *If  $a$  and  $b$  are two moduls of the  $n$ th order in a realm  $\Omega$  of the  $n$ th degree, then also (1)  $a - b$ ;*

*(2)  $a + b$ ; (3)  $ab$ ; (4)  $\frac{b}{a}$ ; (5)  $a^0$ , are moduls of the  $n$ th order in  $\Omega$ .*



For the proof of (1), let  $a - b = m$  and let  $m$  be the order of  $m$ . Then from the theorem of the preceding article there is an integer  $r \neq 0$  such that  $ra > b$  and since  $r$  is a rational integer, we also have  $ra > a$  and consequently  $ra > m$ . It follows (Art. 150) that the order of  $ra$  which is the same as the order of  $a$  cannot be greater than  $m$ , so that  $n \leq m$ . On the other hand since  $m > a$ , it is also true that  $m \leq n$  and consequently  $m = n$ .

To prove (2) let  $a = [\alpha_1, \alpha_2, \dots, \alpha_n]$  and  $b = [\beta_1, \beta_2, \dots, \beta_n]$  so that  $\delta = [\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n]$ . All numbers that are divisible by  $\delta$  belong to the realm  $\Omega$ . Consequently the order of  $\delta$  is at most  $= n$ . On the other hand there are at least  $n$  independent basal elements of  $\delta$ , viz.,  $\alpha_1, \alpha_2, \dots, \alpha_n$  or  $\beta_1, \beta_2, \dots, \beta_n$ . It is thus proved that the greatest common divisor of two moduls of the  $n$ th order in a realm of the  $n$ th degree is a modul of the  $n$ th order.

Again for the proof of (3) let  $a = [\alpha_1, \alpha_2, \dots, \alpha_n]$ . We then have

$$ab = \alpha_1 b + \alpha_2 b + \dots + \alpha_n b.$$

Since these moduls are all of the  $n$ th order, by repetition of (2) it is evident that  $ab$  is of the  $n$ th order.

To prove (4) observe that if  $a = [\alpha_1, \alpha_2, \dots, \alpha_n]$ , then

$$\frac{b}{a} = \frac{1}{\alpha_1} b - \frac{1}{\alpha_2} b - \frac{1}{\alpha_3} b - \dots - \frac{1}{\alpha_n} b.$$

Further since  $\frac{1}{\alpha_\nu} b (\nu = 1, 2, \dots, n)$  are all moduls of the

$n$ th order, through repetition of (1) it is seen that also  $\frac{b}{a}$  is of the  $n$ th order. As a special case of the last statement we have: The order-modul  $a^0$ , where  $a$  is of the  $n$ th order in a realm of the  $n$ th degree, is of the  $n$ th order.

ART. 166. A realm of the  $n$ th degree consists of all

rational functions of a root of an irreducible equation of the  $n$ th degree. Let  $\vartheta$  be the root of such an equation  $f(t) = 0$ , which defines  $\Omega = \mathfrak{K}(\vartheta)$ ; and let  $\vartheta', \vartheta'', \dots, \vartheta^{(n)}$  be the  $n$  roots of this equation, one being  $\vartheta$ . Further let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be  $n$  quantities of  $\Omega$  and express  $\alpha_r (r = 1, 2, \dots, n)$  as rational functions of  $\vartheta$ . Then replace  $\vartheta$  by the  $n$  conjugate roots. We thus have the  $n$  quantities  $\alpha'_r, \alpha''_r, \dots, \alpha_r^{(n)} (r = 1, 2, \dots, n)$  that are conjugate with  $\alpha_r$ .

The discriminant of the  $n$  quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$  was defined (Art. 63) through

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \begin{vmatrix} \alpha'_1 & \alpha'_2 & \dots & \alpha'_n \\ \alpha''_1 & \alpha''_2 & \dots & \alpha''_n \\ \dots & \dots & \dots & \dots \\ \alpha^{(n)}_1 & \alpha^{(n)}_2 & \dots & \alpha^{(n)}_n \end{vmatrix}^2$$

It was also seen that this discriminant was zero if  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly dependent. On the other hand this discriminant is *not* zero, if the  $\alpha$ 's are linearly independent. Suppose that  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent and consequently form a basis of  $\Omega$ .

Further let  $\beta_1, \beta_2, \dots, \beta_n$  be  $n$  arbitrary numbers of this realm, so that

$$\beta_r = c_{r1}\alpha_1 + c_{r2}\alpha_2 + \dots + c_{rn}\alpha_n \quad (r = 1, 2, \dots, n),$$

where the  $c$ 's are rational numbers.

In this equation write for  $\alpha_1, \alpha_2, \dots, \alpha_n$  their values in terms of  $\vartheta$  and then for  $\vartheta$  write its conjugate values. We thus have the quantities  $\beta_r^{(s)}, \beta_s^{(r)}, \dots, \beta_n^{(s)} (s = 1, 2, \dots, n)$  which are conjugate with and include  $\beta_1, \beta_2, \dots, \beta_n$ .

Since the quantities

$$c_{r1}, c_{r2}, \dots, c_{rn} \quad (r = 1, 2, \dots, n)$$

have remained unchanged, it is evident that

$$\beta_r^{(s)} = c_{r1}\alpha_1^{(s)} + c_{r2}\alpha_2^{(s)} + \dots + c_{rn}\alpha_n^{(s)} \quad (r, s = 1, 2, \dots, n).$$

It follows from the theorem for the multiplication of determinants that

$$|\beta_r^{(s)}| = |c_{rs}| |a_r^{(s)}|;$$

or, if we represent the determinant  $|c_{rs}|$  by  $C$ , we have

$$|\beta_r^{(s)}| = C |\alpha_r^{(s)}|.$$

Through squaring, it is seen that

$$\Delta(\beta_1, \beta_2, \dots, \beta_n) = C^2 \Delta(\alpha_1, \alpha_2, \dots, \alpha_n).$$

If it is assumed that  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_n$  form bases of *one and the same modul*  $\mathfrak{a}$ , then  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly expressed through the  $\beta$ 's with integral coefficients and *vice versa*. It follows that  $C = \pm 1$  and (see also Art. 94)

$$\Delta(\beta_1, \beta_2, \dots, \beta_n) = \Delta(\alpha_1, \alpha_2, \dots, \alpha_n).$$

It has thus been shown that *the discriminant of the basal elements of a modul*  $\mathfrak{a}$  *is independent of the choice of the elements*. It may therefore be denoted by  $\Delta(\mathfrak{a})$ .

ART. 167. As a second application of the formula

$$\Delta(\beta_1, \beta_2, \dots, \beta_n) = C^2 \Delta(\alpha_1, \alpha_2, \dots, \alpha_n),$$

suppose that both  $\beta_1, \beta_2, \dots, \beta_n$  and  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent so that each of these systems of quantities determines a modul. Denote these moduls respectively by  $\mathfrak{b}$  and  $\mathfrak{a}$ . We saw (Art. 153) that

$$|C| = \frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})}.$$

If this value of  $C$  is written in the above formula, it results that

$$\Delta(\beta_1, \beta_2, \dots, \beta_n) = \frac{(\mathfrak{a}, \mathfrak{b})^2}{(\mathfrak{b}, \mathfrak{a})^2} \Delta(\alpha_1, \alpha_2, \dots, \alpha_n).$$

If the symbol of the preceding article is adopted, this formula becomes

$$(\mathfrak{a}, \mathfrak{b})^2 \Delta(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})^2 \Delta(\mathfrak{b}).$$

Next apply this formula to the special case  $b = \eta a$ , where  $\eta$  is a number of the realm  $\Omega$ . It is seen that

$$(a, \eta a)^2 \Delta(a) = (\eta a, a)^2 \Delta(\eta a).$$

If the quantities that are conjugate with  $\eta$  are denoted by  $\eta', \eta'', \eta''', \dots, \eta^{(n)}$  (including  $\eta$ ), it is clear that

$$\begin{aligned} \Delta(\eta a) &= \Delta(\eta \alpha_1, \eta \alpha_2, \dots, \eta \alpha_n) \\ &= \begin{vmatrix} \eta' \alpha'_1 & \eta' \alpha'_2 & \dots & \eta' \alpha'_n \\ \eta'' \alpha''_1 & \eta'' \alpha''_2 & \dots & \eta'' \alpha''_n \\ \dots & \dots & \dots & \dots \\ \eta^{(n)} \alpha^{(n)}_1 & \eta^{(n)} \alpha^{(n)}_2 & \dots & \eta^{(n)} \alpha^{(n)}_n \end{vmatrix}^2 \\ &= \{\eta' \eta'' \dots \eta^{(n)}\}^2 \Delta(a) = N(\eta)^2 \Delta(a). \end{aligned}$$

It is thus shown that

$$(a, \eta a)^2 \Delta(a) = (\eta a, a)^2 N(\eta)^2 \Delta(a);$$

or, since

$$\begin{aligned} \Delta(a) &\neq 0, \\ (a, \eta a)^2 &= (\eta a, a)^2 N(\eta)^2 \end{aligned}$$

and consequently

$$N(\eta)^2 = \frac{(a, \eta a)^2}{(\eta a, a)^2}.$$

In extracting the root, so choose the sign that  $\frac{(a, \eta a)}{(\eta a, a)}$  is positive, since the numerator and denominator are by definition positive integers. It follows that

$$|N(\eta)| = \frac{(a, \eta a)}{(\eta a, a)};$$

and from this it is seen that the quotient  $\frac{(a, \eta a)}{(\eta a, a)}$  is independent of  $a$ .

ART. 168. It has been proved (Art. 94) that in every algebraic realm of rationality of the  $n$ th degree there are  $n$  algebraic integers  $\omega_1, \omega_2, \dots, \omega_n$  such that all algebraic integers of the realm may be expressed through the linear form

$$x_1 \omega_1 + x_2 \omega_2 + \dots + x_n \omega_n,$$

where the  $x$ 's are rational integers. This theorem may be expressed as follows:

*All the algebraic integers of the realm of the  $n$ th degree form a finite modul of the  $n$ th order.* This modul may be denoted by  $\mathfrak{o}$ . It is clearly an order-modul.

This theorem may be derived directly from the modul-theory. Let  $\beta_1, \beta_2, \dots, \beta_n$  be  $n$  elements of a basis of a realm  $\Omega$  of the  $n$ th degree. That is, suppose that  $\beta_1, \beta_2, \dots, \beta_n$  are  $n$  arbitrary, linearly independent quantities of the realm  $\Omega$ . Since every algebraic number may through multiplication by a rational integer be transformed (Art. 93) into an algebraic integer, it is possible to determine  $n$  rational integers  $s_1, s_2, \dots, s_n$  such that  $s_1\beta_1, s_2\beta_2, \dots, s_n\beta_n$  are algebraic integers. Denote them by  $\alpha_1, \alpha_2, \dots, \alpha_n$ . It is evident that the modul

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n]$$

consists only of algebraic integers of the realm  $\Omega$ . The two following cases are possible: *either* all the algebraic integers of the realm  $\Omega$  are divisible by  $\mathfrak{a}$ , *or* they are *not* all divisible by this modul. For the first case the theorem is of itself proved. For the second case there must exist in  $\Omega$  an algebraic integer  $\beta$  which is not divisible by  $\mathfrak{a}$ . Since  $\alpha_1, \alpha_2, \dots, \alpha_n$  constitute also a basis of  $\Omega$ , it is seen that  $\beta$  may be expressed in the form

$$\beta = \frac{k_1\alpha_1 + k_2\alpha_2 + \dots + k_n\alpha_n}{k},$$

where  $k, k_1, k_2, \dots, k_n$  are rational integers without a common divisor other than unity. It is assumed also that  $k > 1$ ; for if  $k = 1$ , then  $\beta$  would be divisible by  $\mathfrak{a}$ . Let  $\mathfrak{b} = [\beta]$ ,  $\mathfrak{m} = \mathfrak{a} - \mathfrak{b}$ ,  $\mathfrak{d} = \mathfrak{a} + \mathfrak{b}$ . If  $\mu$  is a number divisible by  $\mathfrak{m}$ , then  $\mu$  is divisible by both  $\mathfrak{a}$  and  $\mathfrak{b}$ . Consequently it is seen on the one hand that  $\mu = x \cdot \beta$ , where  $x$  is a rational integer, and if we substitute for  $\beta$  its value from



above

$$\mu = x \frac{k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n}{k} = x \frac{k_1}{k}\alpha_1 + x \frac{k_2}{k}\alpha_2 + \cdots + x \frac{k_n}{k}\alpha_n.$$

On the other hand since  $\mu$  is divisible by  $\mathfrak{a}$ , it follows also that

$$\mu = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n,$$

where the  $x$ 's are rational integers. As the  $\alpha$ 's are linearly independent, it results that

$$x \frac{k_r}{k} = x_r \quad (r = 1, 2, \cdots, n).$$

It follows that  $x \frac{k_1}{k}, x \frac{k_2}{k}, \cdots, x \frac{k_n}{k}$  must be rational integers,

and consequently that  $x$  must be divisible by  $k$ . For if  $x$  were not divisible by  $k$ , there must be a number  $p$  which divides  $k$  and is not a factor of  $x$ . This number must also divide  $k_1, k_2, \cdots, k_n$ , which is contrary to the hypothesis that these integers had no common factor other than unity.

It follows that every number  $\mu$  that is divisible by  $\mathfrak{m}$  is an integral multiple of  $\beta k$ ; for  $\mu = x\beta$  and  $x$  is divisible by  $k$ . Reciprocally, note *first* that every integral multiple of  $\beta k$  is divisible by  $\mathfrak{a}$ , for  $\beta k = k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n$ , and *secondly* since  $\mathfrak{b} = [\beta]$  and  $k$  is a rational integer, it follows that  $\beta k$  and all integral multiples of  $\beta k$  are divisible by  $\mathfrak{b}$ . Consequently as all integral multiples of  $\beta k$  are divisible by both  $\mathfrak{a}$  and  $\mathfrak{b}$ , they are also divisible by  $\mathfrak{m}$ . We thus see that  $[k\beta] > \mathfrak{m}$ .

As just seen every number divisible by  $\mathfrak{m}$  is an integral multiple of  $k\beta$ , and consequently  $\mathfrak{m} > [k\beta]$ . It follows that

$$\mathfrak{m} = [k\beta] \quad \text{or} \quad \mathfrak{m} = k[\beta].$$

Observing that  $\mathfrak{b}$  is a one-termed modul, it is seen

(Art. 149, end) that

$$m = (b, m)b = (b, m)[\beta];$$

and consequently

$$k = (b, m) = (b, a) = (b, a)$$

(Art. 137). Finally from the formula (Art. 167)

$$(a, b)^2 \Delta(a) = (b, a)^2 \Delta(b),$$

it follows that

$$\Delta(a) = k^2 \Delta(b).$$

Since  $k^2 > 1$ , it results that

$$\Delta(b) < \Delta(a).$$

In other words, if there is an algebraic integer in  $\Omega$  which is not divisible by the modul  $a$  (this modul consisting of only algebraic integers), then a modul  $b$  of the  $n$ th order in  $\Omega$  may be determined, which also consists only of algebraic integers and is such that  $\Delta(b) < \Delta(a)$ .

If there are still algebraic integers in  $\Omega$  which are also not divisible by  $b$ , by proceeding in the same way another modul of the  $n$ th order in  $\Omega$  may be derived which consists of only algebraic integers and whose discriminant is also  $< \Delta(b)$ . Continuing we must finally come to a modul of the  $n$ th order in  $\Omega$  consisting of only algebraic integers, whose discriminant is a *minimum*. All the algebraic integers of  $\Omega$  must be divisible by this modul which is denoted by  $\mathfrak{o}$ ; otherwise the discriminant of  $\mathfrak{o}$  would not be the smallest discriminant and consequently, proceeding as above, a modul could be derived with still smaller discriminant which consists only of algebraic integers in  $\Omega$ .

**ART. 169.** It has thus been shown that the algebraic integers of a realm  $\Omega$  of the  $n$ th degree form a finite modul  $\mathfrak{o}$  of the  $n$ th order. The elements of this modul may be denoted by  $\omega_1, \omega_2, \dots, \omega_n$ , so that

$$\mathfrak{o} = [\omega_1, \omega_2, \dots, \omega_n].$$

The discriminant of this modul,  $\Delta(\mathfrak{o})$  is denoted by  $D$  (Art. 94), and is called the *basal invariant* (*Grundzahl*) of the realm  $\Omega$ . Accordingly an integral modul in  $\Omega$  may be defined as follows: *A modul is integral, if it is divisible by  $\mathfrak{o}$ .* Since every realm, excepting the trivial case of the realm which consists only of zero, contains the unit 1, the modul  $\mathfrak{o}$  has the property that 1 is divisible by  $\mathfrak{o}$  and consequently also  $[1] > \mathfrak{o}$ . Since further the product of two integral algebraic moduls is an integral algebraic modul, it follows that (1)  $\mathfrak{o}\mathfrak{o} > \mathfrak{o}$  (Art. 132, Formula X), or  $\mathfrak{o}^2 > \mathfrak{o}$ . Further since  $[1] > \mathfrak{o}$  and  $\mathfrak{o} > \mathfrak{o}$ , we have  $[1]\mathfrak{o} > \mathfrak{o}^2$  or (2)  $\mathfrak{o} > \mathfrak{o}^2$ . From (1) and (2) it results that

$$\mathfrak{o}^2 = \mathfrak{o},$$

and similarly it may be proved that

$$\mathfrak{o}^0 = \frac{\mathfrak{o}}{\mathfrak{o}} = \mathfrak{o}$$

(Art. 132, Formula XI). The modul  $\mathfrak{o}$  is an order-modul of  $\mathfrak{o}$  and indeed it is its own order-modul. It is called the fundamental or principal order-modul. This modul plays the same rôle in  $\Omega = \mathfrak{R}(\vartheta)$  as 1 does in  $\mathfrak{R}(1)$ .

**ART. 170. THEOREM.** *If  $\alpha$  is an arbitrary modul of the  $n$ th order in a realm  $\Omega$  of the  $n$ th degree, then every number  $\beta$  which belongs to  $\Omega$  may through multiplication by a rational integer be transformed into a number that is divisible by  $\alpha$ .*

For let the  $n$  numbers  $\alpha_1, \alpha_2, \dots, \alpha_n$  form a basis of  $\alpha$ . They consequently also form a basis of  $\Omega$ ; and since  $\beta$  is a number belonging to  $\Omega$ , it follows that  $\beta$  may be expressed in the form

$$\beta = \frac{s_1\alpha_1 + s_2\alpha_2 + \dots + s_n\alpha_n}{s},$$

where  $s, s_1, s_2, \dots, s_n$  are rational integers which have no common factor other than unity. We therefore

have

$$s\beta = s_1\alpha_1 + s_2\alpha_2 + \cdots + s_n\alpha_n,$$

so that  $s\beta$  is divisible by  $\alpha$ . Applying this theorem to the case  $\beta = 1$ , it is seen that there is always a rational integer  $s \cdot 1$  or  $s$  which is divisible by  $\alpha$ . It is thus shown that *every finite modul of the  $n$ th order in  $\Omega$  contains rational integers.*

All rational integers which are divisible by a finite modul  $\alpha$  form a finite modul and the order of this last modul is clearly unity since the modul consists entirely of rational integers. The basis of this modul consists therefore of one element, say  $a$ . It follows then that all the rational integers that are divisible by  $\alpha$  are divisible by the modul  $[\alpha]$  and consequently may be expressed through the form  $ax$  where  $x$  is a rational integer. This number is the smallest rational integer that is divisible by  $\alpha$  and all other rational integers that are divisible by  $\alpha$  are integral multiples of  $a$ . For the modul  $\mathfrak{o}$  the number  $a = 1$ , because all rational integers are divisible by  $\mathfrak{o}$ , and  $[1]$  is the modul formed of all rational integers.

#### COMPLEMENTARY BASES AND COMPLEMENTARY MODULS IN A REALM OF THE $n$ TH DEGREE

ART. 171. We come next to the complementary bases and complementary moduls which play an important rôle in the Theory of Abelian Integrals.

Let  $\Omega$  be a realm of rationality of the  $n$ th degree and let  $\alpha_1, \alpha_2, \cdots, \alpha_n$  form a basis of  $\Omega$  constituting therefore a system of linearly independent elements; and further let  $\alpha_r^{(1)}, \alpha_r^{(2)}, \cdots, \alpha_r^{(n)}$  be the  $n$  quantities conjugate with  $\alpha_r$  ( $r = 1, 2, \cdots, n$ ). The following formula was derived in Art. 104,

$$\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = |S(\alpha_r \alpha_s)| \begin{matrix} (r=1, 2, \cdots, n) \\ (s=1, 2, \cdots, n) \end{matrix},$$

where

$$S(\alpha_r \alpha_s) = \alpha_r^{(1)} \alpha_s^{(1)} + \alpha_r^{(2)} \alpha_s^{(2)} + \dots + \alpha_r^{(n)} \alpha_s^{(n)}.$$

Under the assumption that  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, it follows that  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$  and consequently also the determinant of the  $n$ th degree  $|S(\alpha_r \alpha_s)|$  is different from zero (Art. 63).

Next introduce  $n$  new quantities  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  defined as roots of the  $n$  linear equations

$$\alpha_r = S(\alpha_r \alpha_1) \alpha'_1 + S(\alpha_r \alpha_2) \alpha'_2 + \dots + S(\alpha_r \alpha_n) \alpha'_n, \quad (r=1, 2, \dots, n).$$

To be distinguished are the  $\alpha'$ 's from the preceding alphas whose indices are in brackets. Since their determinant is different from zero, these  $n$  equations with rational coefficients may be solved with respect to the unknown quantities  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$ . It is therefore evident that  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  are quantities of the realm  $\Omega$ . It is asserted:

*The  $n$  quantities  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  form a basis of the realm  $\Omega$ .*

For write

$$(1) \quad \alpha_r = \sum_{s=1}^{s=n} \{S(\alpha_r \alpha_s) \alpha'_s\} \quad (r=1, 2, \dots, n).$$

Suppose in (1) that all the quantities are expressed through  $\vartheta$  where  $\vartheta$  is the algebraic quantity defining the realm of the  $n$ th degree  $\Omega = \mathfrak{R}(\vartheta)$ . Further in the resulting expression write for  $\vartheta$  all the conjugate values of  $\vartheta$  and note that  $S(\alpha_r \alpha_s)$  being a rational quantity remains unchanged. It is seen that

$$\alpha_r^{(t)} = \sum_{s=1}^{s=n} \{S(\alpha_r \alpha_s) \alpha_s'^{(t)}\} \quad (r=1, 2, \dots, n; t=1, 2, \dots, n).$$

It follows that

$$|\alpha_r^{(t)}| = |S(\alpha_r \alpha_s)| \cdot |\alpha_s'^{(t)}|;$$

or squaring,

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \Delta^2(\alpha_1, \alpha_2, \dots, \alpha_n) \Delta(\alpha'_1, \alpha'_2, \dots, \alpha'_n).$$



Further since  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, it is seen that  $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$  and consequently

$$(2) \quad \Delta(\alpha_1, \alpha_2, \dots, \alpha_n) \Delta(\alpha'_1, \alpha'_2, \dots, \alpha'_n) = 1.$$

From this relation it is evident that  $\Delta(\alpha'_1, \alpha'_2, \dots, \alpha'_n) \neq 0$ , and consequently  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  form a basis of  $\Omega$ . This basis of numbers  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  defined through the  $n$  equations (1) is called *the complementary basis* of  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

ART. 172. A generalization of equations (1) may be made which will serve as a further definition of the complementary basis.

If  $\alpha$  and  $\beta$  are two arbitrary algebraic numbers and if  $y$  is a rational number, then we have (Arts. 59 and 89)

$$\begin{aligned} S(\alpha \pm \beta) &= S(\alpha) \pm S(\beta), \\ S(y\alpha) &= yS(\alpha). \end{aligned}$$

Any arbitrary number  $\omega$  of the realm  $\Omega$  may be written

$$\omega = \sum_{r=1}^{\tau=n} (y_r \alpha_r),$$

where  $y_1, y_2, \dots, y_n$  are integral (or fractional) rational numbers. From (1) it follows that

$$\begin{aligned} \omega &= \sum_{s=1}^{s=n} \left\{ \sum_{r=1}^{\tau=n} S(y_r \alpha_r \alpha_s) \alpha'_s \right\} = \sum_{s=1}^{s=n} \left\{ \alpha'_s \sum_{r=1}^{\tau=n} S(y_r \alpha_r \alpha_s) \right\} \\ &= \sum_{s=1}^{s=n} \left\{ \alpha'_s S\left(\sum_{r=1}^{\tau=n} [y_r \alpha_r \alpha_s]\right) \right\} = \sum_{s=1}^{s=n} \left\{ \alpha'_s S\left(\alpha_s \sum_{r=1}^{\tau=n} (y_r \alpha_r)\right) \right\}, \end{aligned}$$

or

$$(3) \quad \omega = \sum_{s=1}^{s=n} \left\{ S(\omega \alpha_s) \alpha'_s \right\}.$$

It is clear that the equation (1) is a special case of equation (3). From this it is seen that the coördinates (Art. 62) of any arbitrary number  $\omega$  of the realm  $\Omega$  with respect to the basis  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$ , which is complementary of the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$  are

$$S(\omega \alpha_1), \quad S(\omega \alpha_2), \quad \dots, \quad S(\omega \alpha_n).$$

ART. 173. If in equation (3) as a special case we write

$$\omega = \alpha'_r,$$

there result the  $n$  equations

$$\alpha'_r = \sum_{s=1}^{s=n} \{S(\alpha'_r \alpha_s) \alpha'_s\} \quad (r=1, 2, \dots, n).$$

It was proved above that  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  are linearly independent. Consequently the  $n$  relations just written must be identities. Using the symbol  $e_{rs} = 0$  when  $r \neq s$  and  $e_{rs} = 1$  when  $r = s$ , it is seen that

$$(4) \quad S(\alpha'_r \alpha_s) = e_{rs} \quad (r, s=1, 2, \dots, n).$$

The  $n^2$  equations just written are *characteristic* of the basis  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  that is complementary of  $\alpha_1, \alpha_2, \dots, \alpha_n$ ; and this may be expressed as follows:

**THEOREM.** *If  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_n$  are two systems of  $n$  numbers in the realm  $\Omega$ , among which the  $n^2$  equations*

$$S(\alpha_r \beta_s) = e_{rs} \quad (r, s=1, 2, \dots, n)$$

*exist, then (1)  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, (2)  $\beta_1, \beta_2, \dots, \beta_n$  form the complementary basis of the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$  in the realm  $\Omega$ .*

The proof of (1) is as follows: If  $\alpha_1, \alpha_2, \dots, \alpha_n$  were linearly dependent, it would be possible to determine  $n$  rational integers  $x_1, x_2, \dots, x_n$  such that

$$x_1 \alpha_1 + x_2 \alpha_2 + \dots + x_n \alpha_n = 0,$$

or

$$\sum_{r=1}^{r=n} (x_r \alpha_r) = 0.$$

Form the expression

$$\sum_{r=1}^{r=n} \{x_r S(\alpha_r \beta_s)\} = \sum_{r=1}^{r=n} S(x_r \alpha_r \beta_s) = S\left(\sum_{r=1}^{r=n} (x_r \alpha_r \beta_s)\right).$$

This expression is equal to  $S(\beta_s \sum_{r=1}^{r=n} x_r \alpha_r) = S(\beta_s \cdot 0) = S(0) = 0$ ; and this is true for  $s = 1, 2, \dots, n$ .

On the other hand by hypothesis

$$\sum_{r=1}^{r=n} \{x_r S(\alpha_r \beta_s)\} = \sum_{r=1}^{r=n} (x_r e_{rs}) = x_s e_{ss} = x_s \quad (s = 1, 2, \dots, n).$$

It results that

$$x_s = 0 \quad (s = 1, 2, \dots, n),$$

and consequently the relation  $\sum_{r=1}^{r=n} (x_r a_r) = 0$  can only exist, if  $x_1 = 0 = x_2 = \dots = x_n$ . It is thus seen that the quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$  are linearly independent, and form a basis of the realm  $\Omega$ .

For the second part of the theorem it remains to show that  $\beta_1, \beta_2, \dots, \beta_n$  form the complementary basis to  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

Suppose that the quantities  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  form the complementary basis in  $\Omega$  of  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

We then have by writing  $\omega = \beta_r$  in (3),

$$\begin{aligned} \beta_r &= \sum_{s=1}^{s=n} \{S(\beta_r \alpha_s) \alpha'_s\} = \sum_{s=1}^{s=n} (e_{rs} \alpha_s) \\ &= \alpha_r \quad (r = 1, 2, \dots, n). \end{aligned}$$

It follows that  $\beta_1, \beta_2, \dots, \beta_n$  form the complementary basis in  $\Omega$  of  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

From equation (4) it also follows in virtue of the theorem just proved that *if the quantities  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  form the complementary basis in  $\Omega$  of the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$ , then the quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$  form the complementary basis in  $\Omega$  of  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$ .*

Due to this theorem, the theorem that is expressed through (3) and (4) is also expressed through the two relations

$$(3) \quad \omega = \sum_{s=1}^{s=n} \{S(\omega \alpha_s) \alpha'_s\},$$

$$(3') \quad \omega = \sum_{s=1}^{s=n} \{S(\omega \alpha'_s) \alpha_s\}.$$

In other words, the coördinates of an arbitrary number  $\omega$  with regard to an arbitrary basis  $\alpha_1, \alpha_2, \dots, \alpha_n$  are  $S(\omega\alpha'_1), S(\omega\alpha'_2), \dots, S(\omega\alpha'_n)$ , where  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  form the complementary basis of  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

To the relations

$$(4) \quad S(\alpha_r'\alpha_s) = e_{rs}$$

may be added

$$(4') \quad S(\alpha_r\alpha'_s) = e_{sr} \quad (r, s = 1, 2, \dots, n).$$

ART. 174. If  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_n$  are two bases of  $\Omega$  complementary of each other and if the quantities conjugate with  $\alpha_r$  are  $\alpha_r^{(1)}, \alpha_r^{(2)}, \dots, \alpha_r^{(n)}$  including  $\alpha_r$ , while the quantities conjugate with  $\beta_s$  are  $\beta_s^{(1)}, \beta_s^{(2)}, \dots, \beta_s^{(n)}$  including  $\beta_s$  ( $r, s = 1, 2, \dots, n$ ), then from above

$$S(\alpha_r\beta_s) = \alpha_r^{(1)}\beta_s^{(1)} + \alpha_r^{(2)}\beta_s^{(2)} + \dots + \alpha_r^{(n)}\beta_s^{(n)} = e_{rs} \quad (r = 1, 2, \dots, n; s = 1, 2, \dots, n).$$

Denote by  $A$  and  $B$  the two determinants

$$\begin{vmatrix} \alpha_1^{(1)} & \alpha_1^{(2)} & \dots & \alpha_1^{(n)} \\ \alpha_2^{(1)} & \alpha_2^{(2)} & \dots & \alpha_2^{(n)} \\ \dots & \dots & \dots & \dots \\ \alpha_n^{(1)} & \alpha_n^{(2)} & \dots & \alpha_n^{(n)} \end{vmatrix}, \quad \begin{vmatrix} \beta_1^{(1)} & \beta_1^{(2)} & \dots & \beta_1^{(n)} \\ \beta_2^{(1)} & \beta_2^{(2)} & \dots & \beta_2^{(n)} \\ \dots & \dots & \dots & \dots \\ \beta_n^{(1)} & \beta_n^{(2)} & \dots & \beta_n^{(n)} \end{vmatrix}.$$

It is evident from the  $n^2$  relations written above that if the elements of the  $r$ th row of the first determinant be multiplied by the elements of the  $s$  row of the second determinant, and if the  $n$  products thus had are added, this sum  $= e_{rs}$ , and this is  $= 1$  when  $r = s$ , and  $= 0$  when  $r \neq s$ .

Further it also follows from these  $n^2$  equations due to a well-known theorem in determinants, which fact is also proved below, that the first minor  $A_r^{(s)}$  associated with  $\alpha_r^{(s)}$  of the determinant  $A$ , divided by the determinant  $A$  is equal to  $\beta_r^{(s)}$ ; and consequently the reciprocal system of the system of quantities  $\alpha_r^{(s)}$  ( $r, s = 1, 2, \dots, n$ ) is formed

through the quantities  $\beta_r^{(s)}$  ( $r, s = 1, 2, \dots, n$ ). This is evident from the following two relations:

$$\begin{aligned}\alpha_r^{(1)}A_r^{(1)} + \alpha_r^{(2)}A_r^{(2)} + \dots + \alpha_r^{(n)}A_r^{(n)} &= A, \\ \alpha_r^{(1)}\beta_s^{(1)} + \alpha_r^{(2)}\beta_s^{(2)} + \dots + \alpha_r^{(n)}\beta_s^{(n)} &= e_{rs}.\end{aligned}$$

It is seen that

$$\beta_r^{(1)} = \frac{A_r^{(1)}}{A},$$

etc. It is also known from the theory of determinants that if the above  $n^2$  relations exist among the elements of the lines of the two determinants  $A$  and  $B$ , the same  $n^2$  relations exist among the elements of the columns of these two determinants. We therefore have the additional relations

$$(5) \quad \alpha_1^{(r)}\beta_1^{(s)} + \alpha_2^{(r)}\beta_2^{(s)} + \dots + \alpha_n^{(r)}\beta_n^{(s)} = e_{rs} \quad (r, s = 1, 2, \dots, n)$$

ART. 175. It follows from (5) above, if we put

$$\alpha_t^{(1)} = \alpha_t, \quad \beta_t^{(1)} = \alpha'_t \quad (t = 1, 2, \dots, n),$$

that

$$(6) \quad \begin{cases} \alpha_1\alpha'_1 + \alpha_2\alpha'_2 + \dots + \alpha_n\alpha'_n = 1, \text{ and} \\ \alpha_1^{(r)}\alpha'_1 + \alpha_2^{(r)}\alpha'_2 + \dots + \alpha_n^{(r)}\alpha'_n = 0. \end{cases} \quad (r = 2, 3, \dots, n).$$

By means of these  $n$  linear equations in the  $n$  unknown quantities  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  we may define the basis  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  complementary to the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$ . However this definition is not as good as the definition of the complementary basis as presented through the equations (1). For in the case of the definition as given through the equations (6) it must be shown that the quantities  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  belongs to the same realm of rationality as the quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$ , a fact which is evident in the case of the definition through equations (1).

ART. 176. A further consequence may be drawn from formulas (4):

If  $\alpha_1, \alpha_2, \dots, \alpha_n; \alpha'_1, \alpha'_2, \dots, \alpha'_n$  are two complementary



bases of the realm  $\Omega$ , it follows in virtue of (4) that

$$S(\alpha_r \alpha'_s) = e_{rs} \quad (r=1, 2, \dots, n; s=1, 2, \dots, n).$$

It is evident that

$$S(\eta \alpha_r \cdot \eta^{-1} \alpha'_s) = e_{rs} \quad (r=1, 2, \dots, n; s=1, 2, \dots, n),$$

where  $\eta$  is an arbitrary quantity of the realm  $\Omega$ . From the existence of the  $n^2$  relations just written it follows from the theorems of Art. 173 that

$$\eta \alpha_1, \eta \alpha_2, \dots, \eta \alpha_n \\ \eta^{-1} \alpha'_1, \eta^{-1} \alpha'_2, \dots, \eta^{-1} \alpha'_n$$

are also two complementary bases in the realm  $\Omega$  to which belong the quantities  $\alpha_1, \alpha_2, \dots, \alpha_n$ .

ART. 177. Suppose that  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_n$  are two arbitrary bases of the realm  $\Omega$  of the  $n$ th degree. It follows that  $\beta_1, \beta_2, \dots, \beta_n$  may be expressed in the form

$$\beta_r = c_{r1} \alpha_1 + c_{r2} \alpha_2 + \dots + c_{rn} \alpha_n = \sum_{s=1}^{s=n} c_{rs} \alpha_s \quad (r=1, 2, \dots, n), \quad (i)$$

where the  $c$ 's are rational numbers.

On the other hand it follows from (3'), if we denote the basis complementary to  $\alpha_1, \alpha_2, \dots, \alpha_n$  by  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  and write in (3')  $\omega = \beta_r$  ( $r=1, 2, \dots, n$ ), that

$$\beta_r = \sum_{s=1}^{s=n} (S(\beta_r \alpha'_s) \alpha_s) \quad (r=1, 2, \dots, n).$$

Through subtraction it results that

$$\sum_{s=1}^{s=n} [(c_{rs} - S(\beta_r \alpha'_s)) \alpha_s] = 0 \quad (r=1, 2, \dots, n).$$

Since the  $\alpha$ 's are linearly independent, it follows also that

$$c_{rs} = S(\beta_r \alpha'_s) \quad (r, s=1, 2, \dots, n).$$

If further we denote the complementary basis of  $\beta_1, \beta_2, \dots, \beta_n$  by  $\beta'_1, \beta'_2, \dots, \beta'_n$ , it follows from (3), if we write in those equations  $\omega = \alpha'_r$ , that

$$\alpha'_r = \sum_{s=1}^{s=n} \{S(\alpha'_r \beta_s) \beta'_s\} \quad (r=1, 2, \dots, n),$$

or

$$(7) \quad \alpha'_r = \sum_{s=1}^{s=n} (c_{sr} \beta'_s) \quad (r=1, 2, \dots, n).$$

Compare these equations with those given under (i) and observe in particular the coefficients.

ART. 178. From the formula just derived follow some very important consequences. Suppose that  $\alpha_1, \alpha_2, \dots, \alpha_n$  are the elements of a modul of the  $n$ th order and write

$$a = [\alpha_1, \alpha_2, \dots, \alpha_n] = [\beta_1, \beta_2, \dots, \beta_n].$$

It follows then that

$$\beta_r = \sum_{s=1}^{s=n} (c_{rs} \alpha_s) \quad (r=1, 2, \dots, n),$$

where the  $c$ 's are rational integers. Further since the  $\alpha$ 's are linearly expressible through the  $\beta$ 's with rational integral coefficients, it was proved (Art. 94) that the determinant of the  $n$ th order  $|c_{rs}| = \pm 1$ . As the determinant remains unchanged when the rows and columns are interchanged, it follows also that

$$|c_{sr}| = |c_{rs}| = \pm 1.$$

From (7) it is seen that

$$\alpha'_r = \sum_{s=1}^{s=n} \{c_{sr} \beta'_s\},$$

the  $c$ 's being rational integers with determinant  $= \pm 1$ . It follows that the modul which has the basis  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  is identical with the modul which has the basis  $\beta'_1, \beta'_2, \dots, \beta'_n$ . Denote this modul by  $a'$ , where

$$a' = [\alpha'_1, \alpha'_2, \dots, \alpha'_n] = [\beta'_1, \beta'_2, \dots, \beta'_n].$$

The modul  $a'$  is the *complementary modul* of  $a$ . The following definition is presented:

*A modul  $a'$  is said to be the Complement of a modul  $a$ , if the bases are complements of each other.*

It is thus seen that corresponding to every modul there is a complementary modul *uniquely* defined. For from

whatever basis of  $a$  we start, we always have the same complementary modul  $a'$ , since the modul  $a'$  is independent of the choice of the basis  $\alpha_1, \alpha_2, \dots, \alpha_n$ . In virtue of its definition the modul  $a'$  is like the modul  $a$  a modul of the  $n$ th order in a realm of the  $n$ th degree.

ART. 179. Next do away with the restriction that the determinant  $|c_{rs}| = \pm 1$ , although it is assumed that the  $c$ 's are rational integers with determinant different from zero. Since the  $\alpha$ 's are supposed to be linearly independent, it follows also that the  $\beta$ 's are linearly independent. The two systems  $\alpha_1, \alpha_2, \dots, \alpha_n$  and  $\beta_1, \beta_2, \dots, \beta_n$  form the two moduls of the  $n$ th order in the realm of the  $n$ th degree, say  $a = [\alpha_1, \alpha_2, \dots, \alpha_n]$ ,  $b = [\beta_1, \beta_2, \dots, \beta_n]$ . Further suppose that  $b > a$ , so that

$$\beta_r = \sum_{s=1}^{s=n} (c_{rs}\alpha_s) \quad (r=1, 2, \dots, n),$$

where the  $c$ 's are rational integers.

If the basis complementary to  $\alpha_1, \alpha_2, \dots, \alpha_n$  is denoted by  $\alpha'_1, \alpha'_2, \dots, \alpha'_n$  and the basis complementary to  $\beta_1, \beta_2, \dots, \beta_n$  by  $\beta'_1, \beta'_2, \dots, \beta'_n$ , it results from (7) that

$$\alpha'_r = \sum_{s=1}^{s=n} (c_{sr}\beta'_s) \quad (r=1, 2, \dots, n).$$

If then we put  $a' = [\alpha'_1, \alpha'_2, \dots, \alpha'_n]$  and  $b' = [\beta'_1, \beta'_2, \dots, \beta'_n]$ , we also have

$$a' > b'.$$

In Art. 150 it was proved that

$$|c_{rs}| = (a, b).$$

In virtue of (7) it is seen that

$$|c_{sr}| = (b', a').$$

Further since  $|c_{sr}| = |c_{rs}|$ , it results that

$$(a, b) = (b', a').$$

The following theorem has thus been established:

**THEOREM.** *If  $a$  and  $b$  are two moduls of the  $n$ th order in a realm of the  $n$ th degree and if  $b > a$ ; and if the moduls complementary of  $a$  and  $b$  be denoted by  $a'$  and  $b'$ , then is*

$$(1) \quad a' > b'$$

and also

$$(2) \quad (a, b) = (b', a').$$

**ART. 180.** In the sequel the modul complementary of any modul  $f$  is denoted by  $f'$ . The following consequences arising from the theorem of the preceding article are presented:

*If  $a$  and  $b$  are two arbitrary moduls of the  $n$ th order in the realm  $\Omega$  of the  $n$ th degree, then is*

$$(a + b)' = a' - b';$$

and

$$(a - b)' = a' + b'.$$

To prove these statements, let  $d = a + b$  and  $m = a - b$ . Since  $a > d$  and  $b > d$ , it is evident from the theorem just proved that  $d' > a'$  and  $d' > b'$  and consequently

$$d' = a' - b'.$$

On the other hand every common multiple of  $a'$  and  $b'$  is divisible by  $d'$ . For if  $f$  is a common multiple of  $a'$  and  $b'$ , so that  $f > a'$  and  $f > b'$ , then it follows from above, since  $(a')' = a$  and  $(b')' = b$ , that  $a > f'$  and  $b > f'$ . Hence  $f'$  is a common divisor of  $a$  and  $b$ . But since  $d$  is the greatest common divisor of  $a$  and  $b$ , it follows (Art. 118) that  $d > f'$  and consequently  $f > d'$ . It is thus proved that  $d'$  is the least common multiple of  $a'$  and  $b'$  and that is

$$(a + b)' = a' - b'.$$

From the same formula, it is evident that

$$(a' + b')' = (a')' - (b')' = a - b,$$

and consequently

$$(a - b)' = \{(a' + b')'\}' = a' + b'.$$

Finally the formula

$$(8) \quad (a, b) = (b', a')$$

may be proved for the general case. The proof of this theorem for the special case  $b > a$  was given in Art. 179.

Write  $b = a + b$ . Since  $(a, b) = (b, b)$  (Art. 137) and since  $b > b$ , it follows that  $(b, b) = (b', b')$ . Since  $b' = a' - b'$  it follows that

$$(b, b) = (b', a' - b') = (b', a')$$

(Art. 137).

### EXAMPLES

1. It may be proved that  $(ab)' = \frac{b'}{a} = \frac{a'}{b}$ ; for let  $a = [\alpha_1, \alpha_2, \dots, \alpha_n]$ , so that

$$ab = \alpha_1 b + \alpha_2 b + \dots + \alpha_n b.$$

Hence we have

$$\begin{aligned} [ab]' &= (\alpha_1 b)' - (\alpha_2 b)' - \dots - (\alpha_n b)' \\ &= \frac{b'}{\alpha_1} - \frac{b'}{\alpha_2} - \dots - \frac{b'}{\alpha_n} = \frac{b'}{a}. \end{aligned}$$

2. Prove that  $(\eta a)' = \eta^{-1} a'$ .
3. Prove that  $(a a')' = a^0 = (a')^0$ .



## CHAPTER VIII

### THE MODULAR SYSTEMS OF KRONECKER

ART. 181. We have seen that the aggregate or complex of rational integers of the form  $\dots, a-3m, a-2m, a-m, a, a+m, a+2m, a+3m, \dots$ , may be defined by saying that they are *congruent* to  $a$ , modulo  $m$ . And the series of integers  $a+km$ , where  $a$  and  $m$  are rational integers, while  $k$  takes all positive and negative integral values, is completely determined through two quantities, viz., the fixed modulus  $m$  and any other term of the series.

Kronecker (*Werke* III<sup>1</sup>, p. 148, and *Crelle's Journal*, Vol. 99, pp. 330 et seq.) defined two linear forms of the variables  $x$  and  $x'$ ,

$$a+bx, \quad a'+b'x'$$

as *equivalent* to each other, if the one could be transformed into the other by the integral substitutions

$$x = \alpha x' + \beta, \quad x' = \alpha' x + \beta',$$

where  $a, b, a', b', \alpha, \beta, x$  and  $x'$  have rational integral values.

The necessary and sufficient conditions for this equivalence are therefore

$$b = \pm b', \quad a \equiv a' \pmod{b}.$$

The conception of the *congruence* of the integers  $a \equiv a' \pmod{m}$  is quite the same as the conception of the *equivalence* of the linear forms  $a+mx \sim a'+mx'$ . Clearly any rational integer  $g$  that may be expressed through either of two equivalent forms may be expressed through the other. The natural extension of the conception of

the congruence with regard to one modulus to the more general conception of the congruence with regard to a system of moduli is at once suggested, when instead of the linear forms <sup>1</sup> with one variable, we consider linear forms in any number of variables

$$a + m_1x_1 + m_2x_2 + \dots + m_\mu x_\mu,$$

where all the quantities occurring have rational integral values.

Two linear forms

$$(1) \quad a + \sum_{h=1}^{h=\mu} m_h x_h, \quad a' + \sum_{k=1}^{k=\nu} m'_k x_k$$

are defined as being *equivalent*, when the one can be transformed into the other by the integral substitutions

$$x_h = c_{ho} + \sum_k c_{hk} x'_k, \quad x'_k = c'_{ko} + \sum_h c'_{kh} x_h$$

( $h = 1, 2, \dots, \mu; k = 1, 2, \dots, \nu$ ),

in which the  $c$ 's are rational integers. Hence the necessary and sufficient conditions for the equivalence of the forms (1) are expressed through the equations

$$(A) \quad a = a' + \sum_k c'_{ko} m'_k, \quad a' = a + \sum_h c_{ho} m_h,$$

$$(B) \quad m_h = \sum_k c'_{kh} m'_k, \quad m'_k = \sum_h c_{hk} m_h$$

( $h = 1, 2, \dots, \mu; k = 1, 2, \dots, \nu$ ).

By giving to the coefficients  $c$  and  $c'$  above all possible integral values, it is clear that the aggregate or totality of all the rational integers that may be expressed through the form

$$(2) \quad a + \sum_{h=1}^{h=k} c_{ho} m_h$$

is defined by saying that they are congruent to one another with respect to the *modular system*  $[m_1, m_2, \dots, m_\mu]$ . For brevity this system may be denoted by  $M$ . Any integer  $g$  which may be expressed through the form

<sup>1</sup> *Encyklopaedie der math. Wissenschaften*, Vol. I, pp. 255, 258 et seq.

(2) may be written as the congruence

$$g \equiv a \pmod{m_1, m_2, \dots, m_\mu},$$

or briefly,

$$g \equiv a \pmod{M}.$$

If  $a = 0$  in the form (2), then is  $g$  a linear homogeneous function of the  $m$ 's with integral coefficients and may be written  $g \equiv 0 \pmod{M}$ .

Due to the formulas (A) and (B) the complex of integers that may be expressed through either of the forms (1) is the same, so that the conception of the equivalence of two modular systems  $(m_1, m_2, \dots, m_\mu)$ ,  $(m'_1, m'_2, \dots, m'_\nu)$  is a natural consequence.

The equations (B) are *characteristic* of the equivalence

$$(m_1, m_2, \dots, m_\mu) \sim (m'_1, m'_2, \dots, m'_\nu).$$

In other words, the necessary and sufficient conditions for the equivalence of the linear forms

$$a + \sum_{h=1}^{h=\mu} m_h x_h, \quad a' + \sum_{k=1}^{k=\nu} m'_k x'_k$$

are expressed by the congruence

$$a \equiv a' \pmod{m_1, m_2, \dots, m_\mu},$$

together with the equivalence

$$(m_1, m_2, \dots, m_\mu) \sim (m'_1, m'_2, \dots, m'_\nu).$$

Let  $M'$  denote the modular system  $(m'_1, m'_2, m'_3, \dots, m'_\nu)$  and suppose that each of its elements is congruent to zero  $\pmod{M}$ , and that is

$$(3) \quad m'_r = a_{r1}m_1 + a_{r2}m_2 + \dots + a_{r\mu}m_\mu \quad (r=1, 2, \dots, \nu);$$

then if  $a \equiv a' \pmod{M'}$ , it follows that  $a \equiv a' \pmod{M}$ .

For, due to the first congruence

$$a - a' = g_1 m'_1 + g_2 m'_2 + \dots + g_\nu m'_\nu,$$

where the  $g$ 's are integers. Writing for  $m'_1, m'_2, \dots$ , their values from (3), it follows that

$$a - a' = G_1 m_1 + G_2 m_2 + \dots + G_\mu m_\mu,$$

where  $G_i$  ( $i=1, 2, \dots, \mu$ ) are integers; and that is,  $a \equiv a_1 \pmod{M}$ .

If the equations (3) exist, it is seen that every integer that may be linearly expressed through  $m'_1, \dots, m'_\nu$ , may be also linearly expressed through  $m_1, \dots, m_\mu$ . In this case the modular system  $M'$  is said to be *divisible* by  $M$ .

And following the analogy of the preceding chapter, we shall write

$$M' > M,$$

and say  $M'$  is *divisible* by  $M$ , and therefore  $M'$  is a *multiple* of  $M$ , while  $M$  is a *divisor* of  $M'$ . If further,  $M > M'$ , then is  $M \sim M'$ .

Observe that if  $g \equiv 0 \pmod{\text{modd. } m_1, \dots, m_\mu, m'_1, \dots, m'_\nu}$ , and that is, if  $g \equiv 0 \pmod{\text{modd. } M, M'}$ , and if also the equations (3) exist, then evidently  $M'$  may be omitted from the system, leaving simply

$$g \equiv 0 \pmod{M}.$$

*Any element  $m$  may be added to the modular system  $M = (m_1, \dots, m_\mu, m)$  or omitted from it when  $m$  is a linear function of the remaining elements with rational integral coefficients.*

This offers the suggestions and also a means for the reduction of a system  $M$  to its simplest form. For, suppose that  $m_1 \equiv m_2 \equiv \dots \equiv m_\mu$ , and through division let

$$\frac{m_1}{m_2} = q + \frac{r_1}{m_2},$$

where  $q$  and  $r_1$  are integers. It follows that

$m_1 = qm_2 + r_1$  and  $r_1 = m_1 - qm_2$ . Due to the latter relation,  $r_1$  may be added as an element to  $M$  and the former element  $m_1$  may be omitted, thus rendering

$$(m_1, m_2, \dots, m_\mu) \sim (r_1, m_2, \dots, m_\mu),$$

where  $r_1 < m_1$ .

Continuing this process it is seen that

$$(m_1, m_2, \dots, m_\mu) \sim (d),$$

where  $d$  is the greatest common divisor of the elements  $m_1, \dots, m_\mu$ . (See Art. 14.)

ART. 182. In his *Vorlesungen über Zahlentheorie*, p. 154, Kronecker defines a realm of rationality as follows: Let  $R$  be any prescribed quantity <sup>1</sup> indeterminate in that at any time a definite value may be assigned to it. This quantity connected with itself through the operations of addition, multiplication, subtraction and division produces a realm of quantities which is completely closed in so far that its individual elements reproduce themselves through the operations just mentioned.

For, if  $\Phi(R)$  and  $\Psi(R)$  are any elements of this realm, then to it belong also

$$\Phi + \Psi, \quad \Phi - \Psi, \quad \Phi \cdot \Psi, \quad \frac{\Phi}{\Psi},$$

it being assumed always that in the operation of division,  $\Psi$  is not zero.

Since  $1 = R/R$ , it is seen that all powers  $1, R, R^2, \dots$ , belong to this realm, as do accordingly also all integral functions

$$f(R) = a_0 + a_1R + \dots + a_mR^m,$$

where the  $a$ 's are rational integers; and likewise also all rational functions

$$F(R) = \frac{f(R)}{g(R)} = \frac{a_0 + a_1R + \dots + a_mR^m}{b_0 + b_1R + \dots + b_nR^n},$$

where the  $b$ 's are also rational integers. As 1 is an element of the realm, it follows by definition that all rational numbers are elements of the realm, so that in the above expressions it is not necessary to impose the conditions that the  $a$ 's and  $b$ 's are integers. Kronecker denoted the realm in question by  $(R)$  while the realm of integrity consisting of all integral functions of  $R$ , he

<sup>1</sup> It would be better if the  $R$ 's used here were replaced by  $u$ 's, as was done in Art. 28. However, the notation of Kronecker is followed.



denoted by  $[R]$  (see Art. 28). Thus as seen in Art. 28  $[R]$  constitutes a part of the realm  $(R)$  while  $[1, R]$  constitutes a part of  $[R]$ , in that rational numbers may enter as coefficients in  $(R)$ . Thus Kronecker denoted a realm of rationality by parentheses  $( )$  and the realm of integrity by brackets  $[ ]$ .

No confusion can arise since the word "realm" usually precedes the parentheses or brackets.

In general, denote by  $R', R'', \dots, R^{(n)}$ ,  $n$  arbitrary indeterminates.<sup>1</sup> The complex of all those quantities that can be produced by addition, subtraction, multiplication and division upon the  $R$ 's constitute the realm  $(R^{(1)}, \dots, R^{(n)})$ , while every integral function

$$f(R', \dots, R^{(n)}) = \sum_{k_1, k_2, \dots, k_n} C_{k_1, k_2, \dots, k_n} R'^{k_1} R''^{k_2} \dots R^{(n)k_n},$$

$$(k_1 = 1, 2, \dots; k_2 = 1, 2, \dots; \dots; k_n = 1, 2, \dots),$$

as well as every rational function

$$F(R', \dots, R^{(n)}) = \frac{f(R^{(1)}, \dots, R^{(n)})}{g(R^{(1)}, \dots, R^{(n)})}$$

enter as elements of this realm.

If the operations are restricted to those of addition, subtraction and multiplication, omitting division, the resulting realm is one of integrity and is denoted by  $[R^{(1)}, \dots, R^{(n)}]$ . As above it constitutes a portion of the realm  $(R^{(1)}, \dots, R^{(n)})$ . (See *Report on Algebraic Numbers*, p. 81; and for the literature see the *Report*, pp. 86 et seq.)

ART. 183. In the present discussion rational integers and integral functions of the variable with rational integral coefficients shall constitute the realm<sup>2</sup> of integrity  $[1, x]$ .

<sup>1</sup> These  $R$ 's may be replaced by  $u_1, u_2, \dots, u_n$ .

<sup>2</sup> See Kronecker, *Grundzüge*, etc., pp. 3 et seq.; Molk, *Acta math.*, Vol. 6, p. 20; Hancock, *Quart. Journ.*, Vol. 27 (1894), pp. 152 et seq.; and see in particular the Paris thesis of Hancock printed in the *Ann. de l'École Normale Supérieure*, Vol. XVIII (1901), where algebraic integers are introduced.

The results of Art. 181, practically word for word, may be repeated here.

Let

$$A, M_1, \dots, M_\mu; \quad A', M'_1, \dots, M'_\nu$$

be integral quantities that belong to the prescribed realm of integrity. The equivalence (see two papers by the author in *Crelle's Journal*, Vols. 119 and 122) of two modular systems

$$(M_1, M_2, \dots, M_\mu), \quad (M'_1, M'_2, \dots, M'_\nu),$$

and the congruence of the two quantities  $A$  and  $A'$  with regard to one of these systems may be defined by the equations:

$$(A) \quad A = A' + \sum_{k=1}^{k=\nu} C'_{ko} M'_k, \quad A' = A + \sum_{h=1}^{h=\mu} C_{ho} M_h,$$

$$(B) \quad M_h = \sum_{k=1}^{k=\nu} C'_{kh} M'_k, \quad M'_k = \sum_{h=1}^{h=\mu} C_{hk} M_h,$$

in which the  $C$ 's and  $C$ 's are also integral quantities of the realm of integrity  $[1, x]$ . These same equations serve also to define the equivalence of the linear forms

$$A + \sum_{h=1}^{h=\mu} M_h X_h, \quad A' + \sum_{k=1}^{k=\nu} M'_k X'_k;$$

and the equivalence of these forms is in turn characterized by the congruence

$$A \equiv A' \pmod{M_1, M_2, \dots, M_\mu},$$

together with the equivalence

$$(M_1, M_2, \dots, M_\mu) \sim (M'_1, M'_2, \dots, M'_\nu).$$

Again, if the  $\nu$  congruences

$$M'_k \equiv 0 \pmod{M_1, M_2, \dots, M_\mu} \quad (k=1, 2, \dots, \nu)$$

exist, the system  $(M'_1, M'_2, \dots, M'_\nu)$  is said to be divisible by  $(M_1, M_2, \dots, M_\mu)$ ; and of the two systems, if each is divisible by the other, we have the equivalence

$$(M_1, M_2, \dots, M_\mu) \sim (M'_1, M'_2, \dots, M'_\nu).$$

ART. 184. *It is evident that any system may be transformed into an equivalent system by adding to or subtracting from any element of the system one or more of the other elements, and any element may be added to a modular system or taken away from it, when this element is a linear homogeneous function of the remaining elements of the modular system.*

As an example, it may be proved,  $u$  being any indeterminate, that

$$(21u^3 + 14u^2 + 4u, 7u^2 + 3u) \sim (3u^2 + 5u, 2u^2 - u).$$

For,

$$\begin{aligned} 21u^3 + 14u^2 + 4u &= (3u^2 + 5u)(3u + 1) + (2u^2 - u)(6u + 1), \\ 7u^2 + 3u &= 1(3u^2 + 5u) + 2(2u^2 - u); \end{aligned}$$

while

$$\begin{aligned} 3u^2 + 5u &= 2(21u^3 + 14u^2 + 4u) - (7u^2 + 3u)(6u + 1), \\ 2u^2 - u &= -1 \cdot (21u^3 + 14u^2 + 4u) + (7u^2 + 3u)(3u + 1). \end{aligned}$$

Similarly,

$$(3u^2 + 5u, 2u^2 - u) \sim (2u^2 - u, u^2 + 6u) \sim (u^2 + 6u, 13u).$$

If for brevity we put

$$(M) = (M_1, \dots, M_\mu), \quad (M') = (M'_1, \dots, M'_\nu)$$

and

$$(M'') = (M''_1, \dots, M''_\lambda),$$

and if

$$M' > M'' \quad \text{and if} \quad M'' > M, \quad \text{then is} \quad M' > M.$$

By the *composition* or *multiplication* of any modular system  $(M)$  with any other system  $(N) = (N_1, N_2, \dots, N_\nu)$ , we understand the system which has as its elements the  $\mu \cdot \nu$  elements  $M_h N_k$ ,  $\left( \begin{smallmatrix} h=1, 2, \dots, \mu \\ k=1, 2, \dots, \nu \end{smallmatrix} \right)$ ; and that is  $(M)(N) = (M_1 N_1, M_1 N_2, \dots, M_1 N_\nu, M_2 N_1, \dots, M_\mu N_\nu)$ . If  $(M) \sim (M')$  then is  $(M)(N) \sim (M')(N)$ . If  $(N')$  is any system such that  $(N) \sim (N')$  and if  $(M) \sim (M')$ , then also is  $(M)(N) \sim (M')(N')$ . For  $(M)(N) \sim (M')(N) \sim (M')(N')$ .

ART. 185. The greatest common divisor  $d$  of two rational integers  $m$  and  $n$  is such that both  $m$  and  $n$  are divisible by  $d$  and any other common divisor  $k$  of both  $m$  and  $n$  is a divisor of  $d$ . A similar definition is applicable to modular systems: If the greatest common divisor of two modular systems  $(M)$  and  $(N)$  is denoted by  $D = (D_1, D_2, \dots, D_\delta)$ , it is required that  $(M) > (D)$  and  $(N) > (D)$  with the further characteristic that any divisor  $(K)$  of both  $(M)$  and  $(N)$  be a divisor of  $(D)$ . For it is clear that

$$(D) = (M_1, M_2, \dots, M_\mu, N_1, N_2, \dots, N_\nu),$$

since

$$(M) > (M_1, \dots, M_\mu, N_1, \dots, N_\nu)$$

and

$$(N) > (M_1, \dots, M_\mu, N_1, \dots, N_\nu).$$

Further if  $(M) > (K)$  and  $(N) > (K)$ , then also is

$$(M_1, \dots, M_\mu, N_1, \dots, N_\nu) > K.$$

If the greatest common divisor of two rational integers is denoted by  $(m, n)$ , then is  $\frac{m \cdot n}{(m, n)}$  the least common multiple of  $m$  and  $n$ . And if  $l$  is an integer that is divisible by both  $m$  and  $n$ , then is

$$(m, n)l \equiv 0 \pmod{m \cdot n}.$$

The analogue for modular systems is as follows:

If  $(L) = (L_1, L_2, \dots, L_\lambda)$  is a system that is divisible by both  $(M)$  and  $(N)$ , then is

$$(M_1, M_2, \dots, M_\mu, N_1, N_2, \dots, N_\nu)(L_1, L_2, \dots, L_\lambda) \equiv 0 \pmod{(M)(N)}.$$

ART. 186. Let us consider the modular system  $(f_1(x), f_2(x))$ , where

$$f_1(x) = a_0 + a_1x + \dots + a_mx^m, \quad f_2(x) = b_0 + b_1x + \dots + b_nx^n,$$

are functions in which the  $a$ 's and  $b$ 's are rational integers,

while  $m$  and  $n$  are positive integers such that  $m \equiv n$ . Divide  $f_1(x)$  by  $f_2(x)$  and denote the quotient by  $g(x)$  and the remainder by  $r(x)$ , so that

$$f_1(x) = g(x)f_2(x) + r(x).$$

The coefficients that occur in  $g(x)$  and  $r(x)$  are rational numbers. Let  $n_1$  denote the least common multiple of their denominators and put

$$g(x) = \frac{g_2(x)}{n_1} \quad \text{and} \quad r(x) = \frac{-f_3(x)}{n_1}.$$

We thus have

$$n_1 f_1(x) - g_2(x) f_2(x) + f_3(x) = 0;$$

and consequently, since  $f_3(x)$  is linearly expressed in terms of  $f_1(x)$  and  $f_2(x)$ , it follows that

$$(f_1(x), f_2(x)) \sim (f_1(x), f_2(x), f_3(x)).$$

Continuing, we may divide  $f_2(x)$  by  $f_3(x)$  and thus derive the following system of equations (see Art. 14):

$$(1) \quad \left\{ \begin{array}{l} n_1 f_1 - g_2 f_2 + f_3 = 0, \\ n_2 f_2 - g_3 f_3 + f_4 = 0, \\ \dots\dots\dots \\ \dots\dots\dots \\ n_{\nu-2} f_{\nu-2} - g_{\nu-1} f_{\nu-1} + f_{\nu} = 0, \\ n_{\nu-1} f_{\nu-1} - g_{\nu} f_{\nu} = 0. \end{array} \right.$$

From these relations it is seen that

$$(f_1, f_2) \sim (f_1, f_2, f_3) \sim (f_1, f_2, f_3, f_4) \sim \dots \sim (f_1, f_2, \dots, f_{\nu}).$$

The equations (1) may be written in the form of congruences:

$$(2) \quad \left\{ \begin{array}{l} f_3 \equiv 0 \pmod{f_1, f_2}, \\ f_4 \equiv 0 \pmod{f_2, f_3}, \\ \cdot \\ \cdot \\ f_{\nu} \equiv 0 \pmod{f_{\nu-2}, f_{\nu-1}}; \end{array} \right.$$



and also from equations (1), it is seen that

$$(3) \quad \left\{ \begin{array}{l} n_1 f_1 \equiv 0 \pmod{(f_2, f_3)}, \\ n_2 f_2 \equiv 0 \pmod{(f_3, f_4)}, \\ \vdots \\ n_{\nu-2} f_{\nu-2} \equiv 0 \pmod{(f_{\nu-1}, f_\nu)}, \\ n_{\nu-1} f_{\nu-1} \equiv 0 \pmod{(f_\nu)}. \end{array} \right.$$

From the equations (1) it is further seen that

$$\begin{aligned} f_\nu &= g_{\nu-1} f_{\nu-1} - n_{\nu-2} f_{\nu-2} = g_{\nu-1} (g_{\nu-2} f_{\nu-2} - n_{\nu-3} f_{\nu-3}) - n_{\nu-2} f_{\nu-2} \\ &= c_2 f_{\nu-2} + c_3 f_{\nu-3}, \end{aligned}$$

where  $c_2, c_3$  are quantities of  $[1, x]$ . Hence,

$$(f_\nu, f_{\nu-1}) > (f_{\nu-1}, f_{\nu-2}) > (f_{\nu-2}, f_{\nu-3}) > \cdots > (f_1, f_2).$$

And in particular,  $f_\nu > (f_1, f_2)$ ; or

$$(4) \quad f_\nu \equiv 0 \pmod{(f_1, f_2)}.$$

If we multiply the next to the last of the congruences (3) by  $n_{\nu-1}$  and observe that  $n_{\nu-1} f_{\nu-1} \equiv 0 \pmod{(f_\nu)}$ , it is seen that  $n_{\nu-1} n_{\nu-2} f_{\nu-2} \equiv 0 \pmod{(f_\nu)}$ . And proceeding in the same manner it is seen that

$$(5) \quad \left\{ \begin{array}{l} n_1 n_2 n_3 \cdots n_{\nu-2} n_{\nu-1} f_1 \equiv 0 \pmod{(f_\nu)}, \\ n_2 n_3 \cdots n_{\nu-2} n_{\nu-1} f_2 \equiv 0 \pmod{(f_\nu)}, \\ n_3 \cdots n_{\nu-2} n_{\nu-1} f_3 \equiv 0 \pmod{(f_\nu)}, \\ \vdots \\ n_{\nu-2} n_{\nu-1} f_{\nu-2} \equiv 0 \pmod{(f_\nu)}, \\ n_{\nu-1} f_{\nu-1} \equiv 0 \pmod{(f_\nu)}. \end{array} \right.$$

If we put  $s_1$  equal to the product of the integers  $n_1, n_2, \dots, n_{\nu-1}$ , while  $s_2$  denotes the product  $n_2 \cdot n_3 \cdot \dots \cdot n_{\nu-1}$ , it is seen that

$$(6) \quad s_1 f_1 \equiv 0 \pmod{(f_\nu)} \quad \text{and} \quad s_2 f_2 \equiv 0 \pmod{(f_\nu)}.$$

Observe that the relations (6) and (4) do *not* connote the equivalence

$$(f_1, f_2) \sim f_\nu.$$

The conditions for this equivalence require that  $s_1 = 1 = s_2$ . When these conditions exist and only then is  $f_\nu$  the greatest common divisor of  $f_1$  and  $f_2$  in the realm  $[1, x]$ . For, from (6) it follows that

$$(7) \quad s_1 f_1 = f_\nu \varphi_1, \quad s_2 f_2 = f_\nu \varphi_2,$$

where  $\varphi_1$  and  $\varphi_2$  are quantities of this realm. It is seen that

$$f_1 = f_\nu \frac{\varphi_1}{s_1}, \quad f_2 = f_\nu \frac{\varphi_2}{s_2}$$

and that  $s_1$  does not divide the coefficients of either  $\varphi_1$  or  $\varphi_2$ , since both  $s_1$  and  $s_2$  were taken as the smallest integers which satisfied the congruences in question. Were the realm of rationality  $[1, x]$  extended to  $(1, x)$  and that is, if rational numbers were admitted in the discussion, then  $f_\nu$  would be the greatest common divisor of  $f_1$  and  $f_2$  and we would have the equivalence  $f_\nu \sim (f_1, f_2)$ .

A modular system  $(f_1(x), f_2(x), \dots, f_n(x))$  with an arbitrary number of elements  $f_1(x), \dots, f_k(x)$ , which system is equivalent to a system with only one element, say  $(f(x))$ , was called by Kronecker a modular system of the *first* kind, while all other systems were named modular systems of the *second* kind. Thus the conditions for a modular system of the first kind

$$(f_1(x), \dots, f_k(x)) \sim (f(x))$$

are

$$f(x) \equiv 0 \pmod{f_1(x), \dots, f_k(x)},$$

together with

$$f_i(x) \equiv 0 \pmod{f(x)} \quad (i=1, 2, \dots, k).$$

An example of a system of the first kind is

$$(3x-3, x^2-1, x^2+x-2) \sim (x-1);$$

for observe that

$$\begin{aligned} 3x-3 &\equiv 0 \pmod{(x-1)}, \\ x^2-1 &\equiv 0 \pmod{(x-1)}, \\ x^2+x-2 &\equiv 0 \pmod{(x-1)}; \end{aligned}$$

and

$$(x-1) \equiv 0 \pmod{3x-3, x^2-1, x^2+x-2},$$

since

$$x-1 = (x^2+x-2) - (x^2-1).$$

A system of the second kind is for example

$$(m, x-n).$$

For there is no integer or integral function which divides both elements save unity, and were

$$(m, x-n) \sim 1,$$

it would follow that identically

$$1 = m\varphi(x) + (x-n)\psi(x),$$

where  $\varphi(x)$  and  $\psi(x)$  are quantities of  $[1, x]$ . Writing  $x=n$ , it would follow that  $1 = m\varphi(n)$ , which is impossible since  $\varphi(n)$  is an integral function.<sup>1</sup>

EXAMPLE. Show that 37 may be added as an element of the modular system

$$(x^5+5x^3+5x+1, 2x^3+2x+1).$$

A *pure* modular system of the second kind

$$(f_1, f_2, \dots, f_k)$$

is one whose elements  $f_1, \dots, f_k$  are not all divisible by the same integral function  $f(x)$ . Were these elements all divisible by  $f(x)$ , the system would be a *mixed* system of the second kind which could be written

$$(f_1(x), f_2(x), \dots, f_k(x)) = f(x)(F_1(x), F_2(x), \dots, F_k(x)),$$

where

$$f_i(x) = f(x)F_i(x) \quad (i=1, 2, \dots, k).$$

However,  $f(x)$  cannot at the same time be  $\equiv 0 \pmod{f_1(x), \dots, f_k(x)}$ . For in this case the given system would be equivalent to  $(f(x))$  and would not be a system of the second kind.

<sup>1</sup> In this connection see Smith's *Report*, p. 149, where references are made to Galois, *Liouville's Journ.*, Vol. XI, p. 381; Serret, *Algèbre*, Leçon 25; Dedekind, *Crelle*, Vol. 54, p. 1, etc. Also see Dickson's *History*, Vol. I, pp. 233 et seq.

Thus  $(5, 2x+1)$  is a pure system, while  $(5x, 2x^2+x)$  is a mixed system.

ART. 187. FUNDAMENTAL THEOREM: *A rational integer may always be added as an element of a pure modular system of the second kind.*

This is at once evident, for the elements  $f_1(x), f_2(x), \dots, f_k(x)$  have no common divisor save unity. It is therefore always possible (Art. 17) to determine other integral functions  $g_1(x), \dots, g_k(x)$  with integral coefficients such that

$$m = g_1(x)f_1(x) + \dots + g_k(x)f_k(x)$$

and accordingly,

$$(f_1(x), f_2(x), \dots, f_k(x)) \sim (m, f_1(x), \dots, f_k(x)).$$

Kronecker (*Vorlesungen, loc. cit.*, p. 186) proves the above theorem as follows. Writing for  $f_v(x)$  the function  $\varphi_2(x)$  in formulas (3) and (6) of the preceding article, we have

$$(1) \quad \begin{aligned} \varphi_2(x) &\equiv 0 \pmod{f_1, f_2}, \\ s_1 f_1 &\equiv 0 \equiv s_2 f_2 \pmod{\varphi_2}. \end{aligned}$$

Introducing  $\varphi_2$  as an element in the system, we have

$$(f_1, f_2, \dots, f_k) \sim (f_1, f_2, \varphi_2, \dots, f_k);$$

and proceeding with  $f_3$  and  $\varphi_2$  as was done with  $f_1$  and  $f_2$  in the preceding article, it is seen that there exists a function  $\varphi_3(x)$  such that

$$(2) \quad \varphi_3 \equiv 0 \pmod{\varphi_2, f_3},$$

and

$$s'_2 \varphi_2 \equiv m_3 f_3 \equiv 0 \pmod{\varphi_3}.$$

In virtue of formula (1), it follows that

$$\varphi_3 \equiv 0 \pmod{f_1, f_2, f_3}.$$

If the last two congruences of (1) are multiplied by  $s'_2$ , and if we observe that  $s'_2 \varphi_2$  is divisible by  $\varphi_3$ , it follows

from (1) and (2) that

$$k_1 f_1 \equiv k_2 f_2 \equiv k_3 f_3 \equiv 0 \pmod{\varphi_3},$$

where  $k_1, k_2, k_3$  are definite integers. Next add  $\varphi_3$  as an element to the system and treat  $\varphi_3$  and  $f_4$  in like manner as before and continue the process until the last element  $f_k$  is reached. We have finally an element  $\varphi_k$  for which there exist the following congruences

$$(3) \quad \varphi_k \equiv 0 \pmod{f_1, f_2, \dots, f_k}$$

and

$$l_1 f_1 \equiv l_2 f_2 \equiv \dots \equiv l_k f_k \equiv 0 \pmod{\varphi_k},$$

where  $l_1, l_2, \dots, l_k$  are definite integers. It is clear that  $\varphi_k$  must be an integer,  $m$ , say; for were  $P(x)$  an irreducible factor of  $\varphi_k(x)$ , it would follow from the second congruence in (3) that each of the elements  $f_1, \dots, f_k$  was divisible by  $P(x)$ , contrary to the assumption that these elements had no common divisor. And from the first of the congruences (3) it is seen that  $m$  may be added as an element to the system, so that

$$(f_1(x), \dots, f_k(x)) \sim (m, f_1(x), \dots, f_k(x)).$$

ART. 188. Another important theorem due to Kronecker is the following:

**THEOREM.** *It is always possible to add as an element of a pure modular system of the second kind a function  $f(x)$  in which the coefficient of the highest power of  $x$  is unity.*

*Proof.* Suppose that the elements  $f_1(x), \dots, f_k(x)$  are of degrees  $n_1, \dots, n_k$ , respectively, where

$$n_1 \geq n_2 \geq \dots \geq n_k.$$

Then form the integral function

$$F(x) = f_1(x) + x^{n_1+1} f_2(x) + x^{n_1+n_2+2} f_3(x) \\ + \dots + x_1^{n_1+n_2+\dots+n_k+k-1} f_k(x),$$

a function which evidently may be added as an element to the system. It is also seen that the coefficients of this



function are the same as those that occur in  $f_1(x), \dots, f_k(x)$ , since the coefficients of the latter are in no case mixed in the formation of the coefficients of the function  $F(x)$ . These coefficients accordingly have no common factor, since by hypothesis the functions  $f_1(x), \dots, f_k(x)$  had no common divisor save unity.

Further, as in the preceding article, let  $m$  be an integer that may be added as an element to the modular system and suppose that

$$m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r},$$

where the  $p$ 's are prime integers. Reduce all the coefficients in  $F(x)$ , modulo  $p_i$ , so that

$$F(x) = \Phi_i(x) - p_i \Psi_i(x),$$

and observe that since  $F(x) \equiv 0 \pmod{f_1(x), \dots, f_k(x)}$ , it follows that

$$\Phi_i(x) \equiv p_i \Psi_i(x) \pmod{f_1(x), \dots, f_k(x)};$$

and therefore also

$$(\Phi_i(x))^{h_i} \equiv p_i^{h_i} (\Psi_i(x))^{h_i} \pmod{f_1, \dots, f_k}.$$

This expression multiplied by  $\frac{m}{p_i^{h_i}}$  becomes

$$\frac{m}{p_i^{h_i}} (\Phi_i(x))^{h_i} \equiv m (\Psi_i(x))^{h_i} \pmod{f_1, \dots, f_k}.$$

Since  $m$  is an element of the modular system, it is seen that

$$(1) \quad X_i(x) = \frac{m}{p_i^{h_i}} (\Phi_i(x))^{h_i} \equiv 0 \pmod{f_1, \dots, f_k} \quad (i=1, 2, \dots, k),$$

in which the coefficients of  $\Phi_i(x)$  are less than  $p_i$  and are not all zero. Since  $p_i$  is relatively prime to  $\frac{m}{p_i^{h_i}}$  it is seen that the coefficient, say  $C_i$ , of the highest power of  $x$  in  $X_i(x)$  is relatively prime to  $p_i$ ; however,  $C_i$  contains as

factors all the other prime factors of  $m$  as often as they are found in  $m$ .

We may accordingly determine an integer  $B_i$  such that

$$B_i C_i \equiv 1 \pmod{p_i^{h_i}} \quad (i=1, 2, \dots, n),$$

while at the same time for every other divisor of  $m$ , say  $p_j$ ,

$$B_i C_i \equiv 0 \pmod{p_j^{h_j}}.$$

Form the sum

$$\bar{F}(x) = B_1 x^{\lambda_1} X_1 + B_2 x^{\lambda_2} X_2 + \dots + B_r x^{\lambda_r} X_r,$$

where the integers  $\lambda$  are so chosen that the highest power of  $x$  in each term is, say  $n$ . The coefficient of  $x^n$  is therefore

$$C = B_1 C_1 + B_2 C_2 + \dots + B_r C_r.$$

Further, observe that

$$C \equiv 1 \pmod{p_i^{h_i}} \quad (i=1, 2, \dots, r),$$

and therefore also writing the congruence in the form of an equation, we have

$$C = 1 + \bar{C}m.$$

If finally we put

$$f(x) = \bar{F}(x) - m\bar{C}x^n,$$

it is seen that the coefficient of the highest power of  $f(x)$  is unity.

Since  $X_1, \dots, X_r, m$ , may all be added as elements to the modular system, it is clear that  $f(x)$  is also an element of this system. And with this the theorem in question is proved.

Writing  $(M) = (m, f, f_1, \dots, f_k)$ , it may be noted that there are only a finite number of incongruent  $(\text{mod. } (M))$  quantities of the realm  $[1, x]$ . For, it may be shown that every quantity  $\varphi(x)$  of this realm may be reduced, modulo  $(M)$ , to another whose degree is less than  $n$ , the degree of  $f(x)$ . For, if  $\varphi(x) = cx^{n+\nu} + \dots$ , it is seen that the degree of  $\varphi_1(x) = \varphi(x) - cx^\nu f(x)$  is less than that of

$\varphi(x)$ , while  $\varphi_1(x)$  is congruent to  $\varphi(x) \pmod{(M)}$ . By repeating this process we may derive a function  $\bar{\varphi}(x)$  which is congruent to  $\varphi(x)$  and whose degree is at most  $n-1$ , say

$$\bar{\varphi}(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}.$$

As each of the  $c$ 's may have any of the values  $0, 1, \dots, m-1$ , it follows that there are at most  $m^n$  incongruent functions  $\pmod{(M)}$ ; and that is, every quantity of the realm  $[1, x]$  is congruent  $\pmod{(M)}$  to one of these  $m^n$  quantities. These residues are in general not all incongruent  $\pmod{(M)}$ .

The determination of the number of such incongruent residues for a pure modular system of the second kind, is a problem which, I believe, has not been done.

ART. 189. Any quantity  $R$  of the realm  $[1, x]$  is said to be relatively prime to the modular system

$$(M) = (f_1, \dots, f_k),$$

if

$$(R, f_1, f_2, \dots, f_k) \sim 1.$$

For example, if besides  $m$  there is another integer  $m_1$ , which may also be added as an element to the modular system of the preceding article, and if  $m_1$  is relatively prime to  $m$ , so that two other integers  $g$  and  $g_1$  exist such that

$$m_1g_1 + mg = 1,$$

then is

$$(M) = (f_1, \dots, f_k) = (m, m_1, f_1, \dots, f_k) \sim 1.$$

THEOREM. If  $R$  and  $R'$  are two quantities of  $[1, x]$ , which are relatively prime to  $(M)$ , then also is  $R \cdot R_1$  relatively prime to  $(M)$ .

*Proof.* Since

$$(R, f_1, \dots, f_k) \sim 1 \quad \text{and} \quad (R', f_1, \dots, f_k) \sim 1,$$

it follows that

$$(R, f_1, \dots, f_k)(R', f_1, \dots, f_k) \sim 1;$$

and that is,

$$(RR', Rf_1, \dots, Rf_k, R'f_1, \dots, R'f_k, \dots, f_1f_j, \dots) \sim 1.$$

Observe further that

$$1 \sim (RR', Rf_1, \dots, R'f_1, \dots, f_1f_j, \dots) > (RR', f_1, \dots, f_k),$$

and therefore 1 may be added as an element to the system on the right-hand side, thus proving the theorem.

In the preceding article it was seen that the number of incongruent, modulo  $(M)$ , residues was finite. Select those which have no common divisor with the system  $(M)$ . Such residues are called *units*, modulo  $(M)$ ; and the system having as an element one of these residues is a *unit system*.

Let  $\mu$  be the number of these incongruent units (modulo  $(M)$ ), which denote by

$$R_1, R_2, \dots, R_\mu.$$

If  $R$  is any *unit* (modulo  $(M)$ ), then as just proved,  $RR_1, \dots, RR_\mu$  are units, modulo  $(M)$  and they form a complete system of incongruent units, modulo  $(M)$ . For, were any two of these products, say,  $RR_i$  and  $RR_j$  congruent, modulo  $(M)$ , it would follow that

$$(1) \quad R(R_i - R_j) \equiv 0 \pmod{f_1, \dots, f_k}.$$

Observe however that if the equivalence  $(R, f_1, \dots, f_k) \sim 1$  be multiplied by  $R_i - R_j$ , there would result

$$(2) \quad (R(R_i - R_j), (R_i - R_j)f_1, \dots, (R_i - R_j)f_k) \sim R_i - R_j;$$

and were (1) true, every element of the left-hand side of (2) would be divisible by  $(M)$  and the same would be true of  $R_i - R_j$ . It would follow that

$$R_i \equiv R_j \pmod{(M)},$$

while  $R_i$  and  $R_j$  were assumed to be incongruent (modulo  $(M)$ ). Accordingly, the  $\mu$  products

$$RR_1, RR_2, \dots, RR_\mu$$

form a system of incongruent (modulo  $(M)$ ) units. Hence, if  $S(R_1, \dots, R_\mu)$  is any integral symmetric function of these units, there exists the congruence

$$S(R_1, \dots, R_\mu) \equiv S(RR_1, \dots, RR_\mu) \pmod{f_1, \dots, f_k},$$

and in particular, for any variable  $X$

$$\prod_{h=1}^{h=\mu} (X - R_h) \equiv \prod_{h=1}^{h=\mu} (X - RR_h) \pmod{f_1, \dots, f_k}.$$

By equating the terms that are free of  $X$ , it is seen that

$$\Pi R_h \equiv R^\mu \Pi R_h \pmod{f_1, \dots, f_k}.$$

Writing  $\Pi R_h = Q$ , it follows from above that

$$(Q, f_1, \dots, f_k) \sim 1,$$

and therefore

$$(Q[R^\mu - 1], (R^\mu - 1)f_1, \dots, (R^\mu - 1)f_k) \sim R^\mu - 1;$$

and since

$$Q[R^\mu - 1] \equiv 0 \pmod{f_1, \dots, f_k},$$

every term on the left-hand side and therefore also  $R^\mu - 1 \equiv 0 \pmod{f_1, \dots, f_k}$ .

This is a direct generalization of the Fermat Theorem,<sup>1</sup> which may be formulated as follows:

*The  $\mu$ th power of every quantity in  $[1, x]$  which is relatively prime to  $(M)$  is always congruent, modulo  $(M)$ , to 1, where  $\mu$  is the number of incongruent units (mod.  $(M)$ ).*

An immediate consequence of this theorem is the following:

If  $(M)$  is any pure modular system of the second kind and  $R$  an arbitrary unit (modulo  $(M)$ ), it is always possible to determine a second unit  $R'$  such that

$$RR' \equiv 1 \pmod{(M)}.$$

For this congruence is evidently satisfied by writing

$$R' \equiv R^{\mu-1} \pmod{(M)}.$$

<sup>1</sup> The reader should not neglect to read Smith's "Report on the Theory of Numbers," *Collected Works*, Vol. I, Art. 10, for Fermat's Theorem. And for the Extension of Fermat's Theorem see p. 152 of this report. For the Galois generalization see Dickson, Vol. I, p. 235.



Two such functions  $R$  and  $R'$  are called complementary units.

## EXAMPLES

1. If  $(M) = (2, x^2)$ , show that  $\mu = 2$  and determine the two incongruent (mod.  $(M)$ ) units.

Observe that if  $f(x)$  is any quantity of  $[1, x]$ , so that

$$f(x) = a_0 + a_1x + a_2x^2 + \dots,$$

where  $a_0$  is *not* congruent to zero modulo  $(M)$ , then is

$$f(x)^2 \equiv (a_0 + a_1x)^2 \pmod{x^2} \quad \text{and} \quad \equiv 1 \pmod{2, x^2}.$$

2. Determine  $\mu$  for the system  $(3, x^3)$  and find the incongruent units.

3. If  $R_0$  is *not* a unit, modulo  $(M)$ , where  $(M)$  is any pure modular system of the second kind, determine another quantity  $R'_0$  of  $[1, x]$  such that

$$R_0R'_0 \equiv 0 \pmod{(M)}, \quad \text{where} \quad R'_0 \not\equiv 0 \pmod{(M)}.$$

ART. 190. We come next to the decomposition of modular systems of the second kind into their simplest forms.<sup>1</sup>

Let

$$(M) = (m, f_1(x), \dots, f_k(x));$$

and suppose that  $m = m_1 \cdot m_2$ , where  $m_1$  and  $m_2$  are relatively prime to each other. It is seen from what follows that

$$(m, f_1, \dots, f_k) \sim (m_1, f_1, \dots, f_k)(m_2, f_1, \dots, f_k).$$

In general, let  $f(x)$  be any element of a modular system and suppose that  $f(x)$  is equal to the product of  $f_0f'_0$ , where the factors  $f_0$  and  $f'_0$  are relatively prime, modulo  $(M)$ . It follows that

$$(1) \quad (f_0, f'_0, f_1, \dots, f_k) \sim 1.$$

It will be proved that

$$(2) \quad (f, f_1, \dots, f_k) = (f_0, f_1, \dots, f_k)(f'_0, f_1, \dots, f_k).$$

<sup>1</sup> Macaulay, *Math. Annalen*, Vol. 74, pp. 66-121, has discussed the resolution of a system into "primary systems."

For, multiplying together the two systems on the right-hand side, it is seen that

$$(3) \quad (f_0, f_1, \dots)(f'_0, f_1, \dots) \\ = (f_0f'_0, f_0f_1, \dots, f'_0f_1, \dots, f_1f_1, \dots).$$

Next multiply (1) by the system  $(f_1, \dots, f_k)$ , thus producing the equivalence

$$(4) \quad (f_0f_1, \dots, f'_0f_1, \dots, f_1f_1, \dots) \sim (f_1, \dots, f_k);$$

and substituting the elements on the right-hand side of (4) for the equivalent elements on the right-hand side of (3), it is seen that (3) becomes

$$(f_0, f_1, \dots, f_k)(f'_0, f_1, \dots, f_k) \sim (f_0f'_0, f_1, \dots, f_k).$$

And this verifies the relation (2).

The above includes a proof of the theorem:

*Every pure modular system of the second kind is equivalent to a product of systems*

$$(M_h) = (p^h, f_1(x), \dots, f_k(x)).$$

For the further reduction of modular system two additional observations may be made:

(1) *A system  $(m, f_1, \dots, f_k)$  in the sense of equivalence remains unchanged if any coefficient of any of the elements is increased or diminished by arbitrary multiples of  $m$ .*

For, if

$$f(x) = a_0x^l + a_1x^{l-1} + \dots + a_ix^{l-i} + \dots + a_1$$

is an element of the system, and if

$$\bar{f}(x) = f(x) + ma_ix^{l-i},$$

it is clear that  $\bar{f}$  may be added as an element to the system, and that then  $f(x)$  may be dropped.

(2) *A system  $(m, f_1, \dots, f_k)$  remains unaltered in the sense of equivalence, if any of the elements  $f_1, \dots, f_k$  is multiplied by a unit, mod.  $m$ .*

For, if  $e$  is a unit (mod.  $m$ ) and  $e'$  its complementary unit, such that  $ee' \equiv 1 \pmod{m}$ , or  $ee' = 1 + mg$ , then on the one hand

$(m, f_1, \dots, ee'f_i, \dots, f_k) > (m, f_1, \dots, ef_i, \dots, f_k)$ ,  
and on the other hand

$$(m, f_1, \dots, ef_i, \dots, f_k) > (m, f_1, \dots, f_i, \dots, f_k).$$

And this proves the equivalence

$$(m, f_1, \dots, f_i, \dots, f_k) \sim (m, f_1, \dots, ef_i, \dots, f_k).$$

ART. 191. We may consider next the simplest case where in the preceding article  $h = 1$ , and that is, we shall further reduce the system

$$(M_1) = (p, f_1(x), \dots, f_k(x)).$$

If the coefficient of the highest power of  $x$  in  $f_1(x)$  is  $e$ , it follows from the preceding article that  $f_1(x)$  may be multiplied by  $e'$ , where  $ee' \equiv 1 \pmod{p}$ , and that thereby the equivalence of the system is unaltered. Accordingly, using also the first observation made at the end of the last article, we may assume that the coefficients of the highest powers of  $x$  in each of the elements  $f_1, \dots, f_k$  are unity, while all other coefficients have been reduced, mod.  $p$ . If the degree of  $f_1(x)$  is greater than or equal to that of  $f_2(x)$ , the coefficients of the highest power of  $f_2(x)$  being unity, it is seen through division of  $f_1(x)$  by  $f_2(x)$  that there results the equation

$$f_1(x) - g_2(x)f_2(x) + \bar{f}_1(x) = 0,$$

where all coefficients are integers. And due to this equation  $\bar{f}_1(x)$  may be added as an element of the system and then  $f_1(x)$  dropped. Due to the presence of the element  $p$  in the system, the coefficient of the highest power of  $x$  in  $\bar{f}_1(x)$  may be made unity, and the others reduced, mod.  $p$ .

Continuing this process (see also Art. 186), and dropping out those elements that are divisible, mod.  $p$ , by any other element, we finally reduce the system to one in which besides  $p$ , there is only one element left. Were this element a constant, the system would be equivalent

to unity. Accordingly there results the following important theorem:

*Every pure modular system of the second kind, in which a prime integer enters to the first power as an element, is equivalent to a reduced system  $(p, f(x))$  of two elements. The element  $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$  has coefficients reduced, mod.  $p$ , the coefficient of the highest power of  $x$  being unity.*

ART. 192. Consider next the reduction of the system

$$(M_2) = (p^2, f_1(x), \dots, f_k(x));$$

and to this end form the auxiliary system  $(p, f_1(x), \dots, f_k(x))$ . From the preceding article it is seen that

$$(1) \quad (p, f_1(x), \dots, f_k(x)) \sim (p, \bar{f}(x));$$

and from this we have

$$\bar{f}(x) = pF + \sum_{i=1}^{i=k} f_i g_i,$$

where  $F$  and  $g_i$  ( $i = 1, 2, \dots, k$ ) are quantities of  $[1, x]$ .

Determine a new function  $f(x)$  by the relation

$$(2) \quad f(x) = \bar{f}(x) - pF = \sum_{i=1}^{i=k} f_i g_i;$$

and observe that  $(p, \bar{f}(x)) \sim (p, f(x))$ , so that from (1) it follows that

$$(3) \quad (p, f_1(x), \dots, f_k(x)) \sim (p, f(x)).$$

Due to (2) it is evident that

$$(4) \quad (p^2, f_1, \dots, f_k) \sim (p^2, f_1, \dots, f_k, f).$$

Due to (3) we have

$$f_i = p\psi_i + f\varphi_i \quad (i = 1, 2, \dots, k) \quad \text{or} \quad f_i \equiv p\varphi_i \pmod{f},$$

where all the quantities introduced belong to the realm  $[1, x]$ .

The right-hand side of (4) may accordingly be written

$$(5) \quad (p^2, p\psi_1, p\psi_2, \dots, p\psi_k, f).$$

Since

$(p^2, p\psi_1, \dots, p\psi_k) = p(p, \psi_1, \dots, \psi_k) \sim p(p, g(x))$ ,  
it follows from (5) that

$$(p^2, p\psi_1, \dots, p\psi_k, f) \sim (p^2, pg(x), f(x));$$

and that is

$$(M_2) = (p^2, pg(x), f(x)).$$

In other words: *Every modular system in which a prime integer enters to the second power as an element, may be transformed into an equivalent system in which besides  $p^2$ , there are only two other elements, and one of these has  $p$  as a factor.*

Proceeding in a similar manner for the reduction of the system

$$(M_3) = (p^3, f_1(x), \dots, f_k(x)),$$

form the auxiliary system

$$(1) \quad (p^2, f_1(x), \dots, f_k(x)) \sim (p^2, p\bar{g}(x), \bar{f}(x)).$$

From the latter it is evident that

$$p\bar{g}(x) = p^2F + \sum_{i=1}^{i=k} f_i r_i,$$

and

$$\bar{f}(x) = p^2G + \sum_{i=1}^{i=k} f_i s_i,$$

where all the introduced quantities belong to  $[1, x]$ .

We are thus able to determine two new functions  $g(x)$  and  $f(x)$  through the relations

$$(2) \quad \begin{cases} pg(x) = p\bar{g}(x) - p^2F = \sum_{i=1}^{i=k} f_i r_i, \\ f(x) = \bar{f}(x) - p^2G = \sum_{i=1}^{i=k} f_i s_i. \end{cases}$$

Due to these relations, it follows at once that

$$(3) \quad (p^2, p\bar{g}(x), \bar{f}(x)) \sim (p^2, pg(x), f(x))$$

and therefore also

$$(4) \quad (p^2, f_1, \dots, f_k) \sim (p^2, pg(x), f(x)).$$



Further, and due to (2), the quantities  $pg(x), f(x)$  may be added as elements of  $(M)$ , thus producing the equivalence

$$(p^3, f_1, \dots, f_k) \sim (p^3, f_1, \dots, f_k, pg(x), f(x)).$$

From (4) it is seen that

$$f_i(x) = p^2 X_i + pg \cdot \psi_i + f \cdot \varphi_i,$$

the quantities introduced belonging to  $[1, x]$ ; and accordingly

$$(p^3, f_1, \dots, f_k, pg, f) \sim (p^3, p^2 X_1, \dots, p^2 X_k, pg, f).$$

Putting  $p^2(p, X_1, \dots, X_k) \sim p^2(p, h(x))$ , we have finally

$$(M_3) = (p^3, f_1, \dots, f_k) \sim (p^3, p^2 h(x), pg(x), f(x)).$$

Continuing in the same manner, it is evident that every system  $(M_h) = (p^h, f_1, \dots, f_k)$  may be brought to the form

$$(p^h, p^{h-1} F_1(x), p^{h-2} F_2(x), \dots, p F_{h-1}(x), F_h(x)),$$

where the coefficients of the highest power in each function  $F_i(x)$  [ $i=1, 2, \dots, h$ ] is unity, the others being reduced, mod.  $p$ .

### CANONICAL FORMS FOR THESE SYSTEMS

ART. 193. Let us return to the system in which a prime integer  $p$  enters to the first power. Such a system (see Art. 191) is of the form

$$(p, \theta(x)),$$

where the coefficient of the highest power of  $x$  in  $\theta(x)$  is unity, and the other coefficients have been reduced, mod.  $p$ .

Suppose that the original system  $(p, f_1(x), \dots, f_k(x))$  has been reduced by a different method to the form

$$(p, \theta_1(x)),$$

where the coefficient of the highest power of  $x$  in  $\theta_1(x)$  is unity and the others have been reduced, mod.  $p$ .

The question naturally arises: Is  $\theta_1(x)$  the same function of  $x$  as is  $\theta(x)$ ; and that is: *Is  $(p, \theta(x))$  the unique reduction, or a canonical form of the original system?*

(I) To investigate this question, consider the equivalence

$$(1) \quad (p, \theta(x)) \sim (p, \theta_1(x)).$$

It is seen on the one hand that

$$\theta(x) \equiv \varphi(x)\theta_1(x) \pmod{p}, \quad (i)$$

and on the other,

$$\theta_1(x) \equiv \psi(x)\theta(x) \pmod{p}, \quad (ii)$$

where all quantities or functions introduced are of the realm  $[1, x]$ .

Multiplying both sides of these two congruences together, we have

$$\theta(x)\theta_1(x) \equiv \theta(x)\theta_1(x)\varphi(x)\psi(x) \pmod{p}.$$

Since neither  $\theta(x)$  nor  $\theta_1(x)$  is divisible by  $p$ , we may divide this congruence by  $\theta(x)\theta_1(x)$ , which thereupon becomes

$$1 \equiv \varphi(x)\psi(x) \pmod{p}.$$

If

$$\varphi(x) = ax^k + \dots \quad \text{and} \quad \psi(x) = bx^h + \dots,$$

their product begins with the term  $abx^{hk} + \dots$ ; and as both  $a$  and  $b$  are reduced, mod.  $p$ , this term is not divisible by  $p$ . Hence, in both  $\varphi(x)$  and  $\psi(x)$  there can appear only the terms independent of  $x$ . Writing  $\varphi(x) = c$  and  $\psi(x) = d$ , in (i) and (ii), it is seen that  $c = 1 = d$ , and therefore also

$$\theta(x) \equiv \theta_1(x) \pmod{p}.$$

The coefficients of like powers of  $x$  in these two functions must be equal, since they have been reduced, mod.  $p$ .

We therefore have  $\theta(x) = \theta_1(x)$  and  $(p, \theta(x))$  may be regarded as a canonical form for the unique reduction of the modular system  $(p, f_1(x), f_2(x), \dots, f_k(x))$ .

(II) Take next the system in which  $p$  occurs to the second power, namely,

$$(M_2) = (p^2, pg(x), f(x)).$$

Form the auxiliary system

$$(1) \quad (p, g(x), f(x)) \sim (p, \theta(x)),$$

where the initial coefficient of  $\theta(x)$  is unity and the others are reduced, mod.  $p$ .

From the latter system it is seen that

$$\theta(x) \equiv 0 \pmod{p, g(x), f(x)},$$

or

$$p\theta(x) \equiv 0 \pmod{p^2, pg(x), pf(x)};$$

and also

$$f(x) = \theta(x)\theta'(x) + p\varphi(x),$$

where all quantities introduced belong to  $[1, x]$ .

The system  $(M_2)$  accordingly may be written without changing the equivalence

$$(M_2) = (p^2, pg, p\theta, p\varphi + \theta\theta').$$

From (1) we have

$$g \equiv 0 \pmod{p, \theta},$$

or

$$pg \equiv 0 \pmod{p^2, p\theta}.$$

The element  $pg$  may therefore be omitted from  $(M_2)$ , which becomes

$$(M_2) = (p^2, p\theta, p\varphi + \theta\theta').$$

Owing to the presence of  $p^2$  and  $p\theta$  within this system, the coefficient of the highest power of  $x$  in  $\theta'$  can be made unity, and then the others may be reduced, mod.  $p$ .

For, suppose that

$$\theta'(x) = bx^m + b_1x^{m-1} + \dots,$$

and choose  $\bar{b}$  such that

$$\bar{b}b - p^2g = 1.$$

Then clearly,

$$\Theta(x) = \bar{b}(p\varphi + \theta\theta') - p^2g \cdot \theta \cdot x^m$$

may be added as an element to the system. Since

$$b\Theta(x) = (1 + p^2g)(p\varphi + \theta\theta') - bp^2g \cdot \theta \cdot x^m,$$

it is seen that  $p\varphi + \theta\theta'$  may be expressed linearly through  $\Theta(x)$  and  $p^2$ , and therefore  $\Theta(x)$  may replace  $p\varphi + \theta\theta'$  in the system. Evident substitutions with  $\Theta(x)$  offer the required result.

The degree of  $\varphi(x)$  may be made less than that of  $\theta(x)$ , and its coefficients reduced, mod.  $p$ .

We may therefore assume in the system  $(M_2)$  that

$$(A) \quad \left\{ \begin{array}{l} (a) \text{ initial coefficients of } \theta \text{ and } \theta' \text{ are unity;} \\ (b) \varphi \text{ is of less degree than } \theta; \\ (c) \text{ all the coefficients of the respective functions} \\ \quad \text{are reduced, mod. } p. \end{array} \right.$$

If by any other method of procedure the system  $(M_2)$  in its original form has been reduced to

$$(p^2, p\theta_1, p\varphi_1 + \theta_1\theta'_1),$$

and if the conditions (A) are true of the corresponding elements of this system, then due to the equivalence

$$(1) \quad (p^2, p\theta, p\varphi + \theta\theta') \sim (p^2, p\theta_1, p\varphi_1 + \theta_1\theta'_1),$$

it may be shown that  $\theta = \theta_1$ ,  $\varphi = \varphi_1$ ,  $\theta' = \theta'_1$ .

*Proof.* It follows from the equivalence that

$$p\varphi_1 + \theta_1\theta'_1 \equiv p\theta \cdot f + (p\varphi + \theta\theta')g \pmod{p^2}$$

and therefore

$$\theta_1\theta'_1 \equiv \theta\theta'g \pmod{p}, \tag{i}$$

the coefficient of the highest power of  $x$  in the function  $g$  being unity.

In a similar manner

$$\theta\theta' \equiv \theta_1\theta'_1g_1 \pmod{p}. \tag{ii}$$

If these congruences are multiplied together and the factor  $\theta\theta'\theta_1\theta'_1$  omitted from the resulting congruence, we have

$$1 \equiv g_1g \pmod{p}.$$

If

$$g = cx^k + c_1x^{k-1} + \dots + c_k$$

and

$$g_1 = dx^h + d_1x^{h-1} + \dots + d_h,$$

the first term in the product of these functions is  $cdx^{h+k} + \dots$  and the coefficient  $cd$  is *not* divisible by  $p$ , since neither  $c$  nor  $d$  is divisible by  $p$ . It follows that  $g = c_k$  and  $g_1 = d_h$ ; and these values substituted in (i) and (ii) show that  $g = 1 = g_1$ .

It results that

$$\theta\theta' \equiv \theta_1\theta'_1 \pmod{p}. \tag{iii}$$

From (1) we have

$$p\theta_1 \equiv p\theta \cdot F + (\theta\theta' + p\varphi)G \pmod{p^2}.$$

From this congruence it is seen that  $\theta\theta'G$  and therefore also  $G$  is divisible by  $p$ . Writing  $G = G_1p$ , it follows that

$$\theta_1 \equiv \theta F + (\theta\theta' + p\varphi)G_1 \pmod{p},$$

or

$$\theta_1 \equiv \theta(F + \theta'G_1) \pmod{p}.$$

In the same manner it may be proved that

$$\theta \equiv \theta_1(F_1 + \theta'_1G'_1) \pmod{p}.$$

These two congruences, when multiplied together, offer

$$\theta\theta_1 \equiv \theta\theta_1(F + \theta'G_1)(F_1 + \theta'_1G'_1) \pmod{p}.$$

Hence, as above,  $F + \theta'G_1 = 1 = F_1 + \theta'_1G'_1$ , and therefore

$$\theta \equiv \theta_1 \pmod{p}.$$

Since the coefficients of both  $\theta$  and  $\theta_1$  have been reduced, mod.  $p$ , it follows that  $\theta = \theta_1$ , and therefore from (iii) it also follows that  $\theta' = \theta'_1$ . Writing these equalities in (1), we have

$$\begin{aligned} (p^2, p\theta, p\varphi + \theta\theta') &\sim (p^2, p\theta, p\varphi_1 + \theta\theta', p\varphi + \theta\theta') \\ &\sim (p^2, p\theta, p\varphi + \theta\theta', p(\varphi - \varphi_1)). \end{aligned}$$

And due to this equivalence, it follows that

$$p(\varphi - \varphi_1) \equiv p\theta \cdot B + (p\varphi + \theta\theta')A \pmod{p^2}.$$



It is evident that  $\theta\theta'A$  and therefore  $A$  must be divisible by  $p$ . Writing  $A = pA_1$ , the congruence becomes

$$\varphi - \varphi_1 \equiv \theta(B + A_1\theta') \pmod{p}.$$

Since the degree of  $\theta$  is greater than that of either  $\varphi$  or  $\varphi_1$ , it is seen that

$$B + A_1\theta' \equiv 0 \pmod{p},$$

and therefore also

$$\varphi \equiv \varphi_1 \pmod{p};$$

and the coefficients having been reduced, mod.  $p$ , it follows that  $\varphi = \varphi_1$ .

*We may therefore regard  $(p^2, p\theta, p\varphi + \theta\theta')$  as a canonical form for the unique representation of modular systems which have as an element a prime integer  $p$  raised to the second power.*

(III) The reduced modular system in which  $p^3$  enters as an element was seen to be (Art. 192)

$$(M_3) = (p^3, p^2f(x), pg(x), h(x)).$$

Form the auxiliary system

$$(1) \quad (p^2, pf(x), g(x), h(x)) \sim (p^2, p\theta(x), p\varphi(x) + \theta(x)\theta'(x)),$$

where the conditions (A) above are fulfilled. It is seen that

$$p\theta(x) \equiv pf(x) \cdot F(x) + g(x)G(x) + h(x)H(x) \pmod{p^2},$$

so that

$$p^2\theta(x) \equiv p^2f(x) \cdot F(x) + pg(x)G(x) \pmod{p^3, h(x)};$$

and similarly,

$$p[p\varphi(x) + \theta(x)\theta'(x)]$$

$$\equiv p^2f(x) \cdot \Phi(x) + pg(x)\Psi(x) \pmod{p^3, h(x)}.$$

Accordingly we may add as elements  $p^2\theta(x)$  and  $p^2\varphi(x) + p\theta(x)\theta'(x)$  to  $(M_3)$  without altering its equivalence, thus having

$$(M_3) = (p^3, p^2f(x), p^2\theta(x), pg(x), p^2\varphi(x) + p\theta(x)\theta'(x), h(x)).$$

If  $pf(x)$  and  $g(x)$  are expressed in terms of the elements on the right-hand side of (1), it is seen that  $p^2f(x)$  and  $pg(x)$  may be omitted from the system  $(M_3)$  just written, which becomes

$$(M_3) = (p^3, p^2\theta, p^2\varphi + p\theta\theta', h(x)).$$

Further from (1) we have

$$h(x) = p^2\psi(x) + p\theta\theta^{(2)} + (p\varphi + \theta\theta')\varphi';$$

and this value substituted for  $h(x)$  in  $(M_3)$  offers

$$(M_3) = (p^3, p^2\theta, p^2\varphi + p\theta\theta', p^2\psi + p\theta\theta^{(2)} + p\varphi\varphi' + \theta\theta'\varphi').$$

Owing to the presence of  $p^3, p^2\theta, p^2\varphi + p\theta\theta'$  in this system, we may assume, including conditions (A) already made, that

- (B)  $\left\{ \begin{array}{l} (a) \text{ the initial coefficients of } \theta, \theta' \text{ and } \varphi' \text{ are each} \\ \quad \text{unity;} \\ (b) \varphi \text{ and } \psi \text{ are of lower degree than } \theta; \\ (c) \theta^{(2)} \text{ is of lower degree than } \theta'; \\ (d) \text{ the coefficients of all the elements are reduced,} \\ \quad \text{mod. } p. \end{array} \right.$

Suppose that the original system was reduced by another method to a form corresponding to the one just written, where the corresponding elements conform to the conditions (B), so that

$$\begin{aligned} &(p^3, p^2\theta, p^2\varphi + p\theta\theta', p^2\psi + p\theta\theta^{(2)} + p\varphi\varphi' + \theta\theta'\varphi') \\ &\sim (p^3, p^2\theta_1, p^2\varphi_1 + p\theta_1\theta'_1, p^2\psi_1 + p\theta_1\theta_1^{(2)} + p\varphi_1\varphi'_1 + \theta_1\theta'_1\varphi'_1). \end{aligned}$$

Prove that the corresponding elements are identically equal. See *Crelle's Journal*, Vol. 119, pp. 161 et seq.; see paper also by the author, *Crelle*, Vol. 122, pp. 265 et seq., where Canonical Forms of higher powers of  $p$  are given and the realms extended from  $[1, x]$  to  $[1, x, y]$ , etc.; also see the papers in Vol. 18 (1901), of the *École Normale Supérieure* and of the *Congrès des Mathématiciens*, C. R. (1900).

To determine whether two modular systems in which appears a prime  $p$  to the same power are equivalent, it is only necessary to show that they have the same canonical form.

**ART. 194. Definition.** A function  $f(x)$  is called a *divisor*, modulo  $p$ , of another function  $F(x)$  if there exists a congruence

$$F(x) \equiv f(x)g(x) \pmod{p},$$

in which  $g(x)$  is also an integral function with integral coefficients.

As this congruence may be written in the form of an equation

$$F(x) = f(x)g(x) + ph(x),$$

it is clear that  $f(x)$  is then and only then a divisor of  $F(x)$ , if there exists the equivalence

$$(p, F(x)) \sim (p, f(x)g(x)).$$

In the further discussion we may regard the coefficients of both  $F(x)$  and  $f(x)$  as reduced, modulo  $p$ . The degree of a divisor of  $F(x)$  is at most equal to the degree  $n$  of  $F(x)$ . Such a divisor must accordingly be of the form

$$f(x) = a_0 + a_1x + \cdots + a_\nu x^\nu,$$

where the coefficients of  $a_j$  are integers of the series  $0, 1, \cdots, p-1$ , and where  $\nu \leq n$ . As there can be in all only  $p^{\nu+1}$  such functions, we have the theorem:

*A function  $F(x)$  has only a finite number of divisors, modulo  $p$ .*

Among these divisors there are the units, modulo  $p$ ; and that is, all integers that are not divisible by  $p$ . For, if  $a_0$  is such a unit and if  $a_0 a'_0 \equiv 1 \pmod{p}$ , then is

$$F(x) \equiv a_0 a'_0 F(x) \equiv a'_0 F_0(x) \pmod{p},$$

where  $F_0(x) = a'_0 F(x)$ . Such divisors are excluded in the further discussion.

A function  $\bar{f}(x)$  is called a *common divisor*, modulo  $p$ , of several other functions  $f_1(x), \dots, f_k(x)$ , if, modulo  $p$ , it is a divisor of each of them. And the following statement is true:

All the common divisors  $\bar{f}(x)$  collectively multiplied together form a divisor which accordingly is the greatest common divisor, modulo  $p$ , of  $f_1(x), \dots, f_k(x)$ ; and if  $f(x)$  is this greatest common divisor, then is

$$(p, f_1(x), \dots, f_k(x)) \sim (p, f(x)).$$

It is further seen that  $f(x)$  is the second element of the reduced system that is equivalent to  $(p, f_1(x), \dots, f_k(x))$ . In fact, if  $f(x)$  satisfies the equivalence

$$(1) \quad (p, f_1(x), \dots, f_k(x)) \sim (p, f(x)),$$

then from the equations

$$f_i(x) = f(x)\varphi_i(x) + p\psi_i(x),$$

or

$$f_i(x) \equiv f(x)\varphi_i(x) \pmod{p} \quad (i=1, 2, \dots, k),$$

it is clear that  $f(x)$  is a divisor, modulo  $p$ , of the  $k$  functions  $f_i(x)$ ; and *vice versa*, it follows from (1) that

$$(2) \quad f(x) \equiv f_1(x)g_1(x) + \dots + f_k(x)g_k(x) \pmod{p}.$$

If  $\bar{f}(x)$  were another common divisor, modulo  $p$ , of the  $k$  functions, so that therefore

$$f_i(x) \equiv \bar{f}(x)\bar{\varphi}_i(x) \pmod{p},$$

then  $\bar{f}(x)$  must necessarily be a divisor of  $f(x)$ . For from (2) it follows that

$$f(x) \equiv \bar{f}(x)[\bar{\varphi}_1(x)g_1(x) + \dots + \bar{\varphi}_k(x)g_k(x)] \pmod{p}.$$

And with this the theorem is completely proved.

The  $k$  functions  $f_1(x), \dots, f_k(x)$  are said to be relatively prime, modulo  $p$ , if the associated system

$$(p, f_1(x), \dots, f_k(x)) \sim 1.$$

In this case there are  $k$  functions  $g_1(x), \dots, g_k(x)$  such

that

$$f_1g_1 + f_2g_2 + \cdots + f_kg_k \equiv 1 \pmod{p},$$

where the functions  $g_i(x)$  are determined as in Arts. 191 and 186.

The function  $F(x)$  of the  $n$ th degree has, modulo  $p$ , a finite number of divisors, which are of the form

$$\varphi(x) = x^\nu + a_1x^{\nu-1} + \cdots + a_\nu,$$

whose degree  $\nu \leq n$ , and whose coefficients are reduced, modulo  $p$ . These divisors may be determined through a finite number of operations as follows: Write down all integral functions of the form  $\varphi(x)$  as above indicated and arrange according to their degree. Denote them in this sequence through  $\varphi_0, \varphi_1, \cdots$ , of degrees  $\nu_0, \nu_1, \cdots$ , where  $\nu_0 \leq \nu_1 \leq \cdots \leq \nu_k \leq \cdots$ . Form the modular systems

$$(p, F(x), \varphi_0(x)), (p, F(x), \varphi_1(x)), \cdots$$

Let  $(p, F(x), \varphi_h(x))$  be the first of these systems which is not equivalent to unity. It follows necessarily that

$$(p, F(x), \varphi_h(x)) \sim (p, \varphi_h(x)),$$

where  $\varphi_h(x)$  is the divisor of lowest degree of  $F(x)$ . For were

$$(1) \quad (p, F(x), \varphi_h(x)) \sim (p, \varphi(x)),$$

where  $\varphi(x) \neq \varphi_h(x)$ , then  $\varphi(x)$  would be a common divisor of  $\varphi_h(x)$  and  $F(x)$  and the degree of  $\varphi(x)$  must accordingly be less or at most equal to  $\nu_h$ . This degree cannot be less than  $\nu_h$ ; otherwise  $\varphi(x)$  would have appeared among the previous functions. And were  $\varphi(x)$  and  $\varphi_h(x)$  of the same degree, it would follow necessarily from the equivalence (1) that

$$(2) \quad \varphi_h \equiv g\varphi(x) \pmod{p},$$

where  $g$  is a rational integer. Since the coefficients of the highest powers of  $x$  in the congruence (2) are unity, it follows that  $g = 1$ . This divisor of the lowest degree of



$F(x)$  may be denoted by  $P(x)$ . We may accordingly write

$$(3) \quad F(x) \equiv P(x)F_1(x) \pmod{p},$$

where  $F_1(x)$  is of lower degree than  $F(x)$ .

The divisor  $P(x)$  cannot be further factored, modulo  $p$ . For were

$$P(x) \equiv Q(x)R(x) \pmod{p},$$

where the degrees of both factors are less than that of  $P(x)$ , it would follow from (3) that

$$F(x) \equiv Q(x)R(x)F_1(x) \pmod{p},$$

and that would mean that  $F(x)$  had a factor of lower degree, modulo  $p$ , than the degree of  $P(x)$ , contrary to the assumption.

In the same manner as was done with  $F(x)$  we may proceed with  $F_1(x)$  in the congruence (3) and determine a factor  $P_1(x)$  of lowest degree, so that

$$F_1(x) \equiv P_1(x)F_2(x) \pmod{p},$$

where  $P_1(x)$  is irreducible, modulo  $p$ .

It follows from (3) that

$$F(x) \equiv P(x)P_1(x)F_2(x) \pmod{p};$$

and it is clear that  $P_1(x)$  is also a factor, modulo  $p$ , of  $F(x)$  and is of like or higher degree than  $P(x)$ .

Continuing, we derive a factorization

$$F(x) \equiv P(x)P_1(x) \cdots P_\mu(x) \pmod{p}$$

in like or different irreducible factors, modulo  $p$ . It will be seen in the next article that this factorization is unique.

**ART. 195.** The irreducible, modulo  $p$ , functions  $P(x)$  play the same rôle in  $[1, x]$  as do the prime integers in  $[1]$ . A modular system  $(\Pi) = (p, P(x))$ , whose second element is not factorable, modulo  $p$ , is called a *prime modular system*. There exists the important theorem:

A function  $F(x)$  of  $[1, x]$  is either divisible by a prime modular system  $(\Pi)$ , or it is a unit, modulo  $(\Pi)$ .

For the system  $(p, P(x), F(x))$  can be only equivalent to  $(p, P(x))$  or to 1; otherwise if it reduced to  $(p, \overline{P}(x))$ , then would  $P(x)$  be divisible, modulo  $p$ , by  $\overline{P}(x)$ , which is in contradiction with the assumption made regarding  $P(x)$ .

From this follows immediately a second theorem: A product  $F(x)G(x)$  is then and only then divisible by a prime modular system  $(p, P(x))$ , if at least one of the factors is divisible by this system.

For if the product  $F(x)G(x)$  is divisible by  $(\Pi)$ , there exists the equivalence

$$(p, P(x), F(x)G(x)) \sim (p, P(x));$$

and were we to assume that neither  $F(x)$  nor  $G(x)$  were divisible by  $(\Pi)$ , it would follow necessarily that

$$(p, P(x), F(x)) \sim 1 \quad \text{and} \quad (p, P(x), G(x)) \sim 1.$$

It would then follow through multiplication that

$$(p^2, pP, P^2, pF, pG, PF, PG, FG) \sim 1.$$

This system is clearly divisible by  $(p, P, FG)$  and therefore  $(p, P, FG) \sim 1$ . And this means that  $FG$  is not divisible by  $P$ , modulo  $p$ . The same theorem is evidently true for a product of an arbitrary number of factors.

Finally we have the theorem:

If a quantity  $F(x)$  of  $[1, x]$  is divisible by two prime modular systems  $(p, P(x))$  and  $(p, Q(x))$  which are not equivalent, then is  $F(x)$  divisible by the product  $(p, P(x)) \cdot (p, Q(x))$ .

For if  $P(x)$  and  $Q(x)$  are relatively prime, modulo  $p$ , then is

$$(p, P(x))(p, Q(x)) \sim (p, PQ).$$

And the fact that  $F(x)$  is divisible by  $(p, P(x))$  is nothing other than that  $F(x)$  has  $P(x)$  as a factor, modulo  $p$ .

If the function  $F(x)$ , considered modulo  $p$ , has as divisors both  $P(x)$  and  $Q(x)$ , then, modulo  $p$ , it is divisible by  $P(x)Q(x)$  and therefore also by the system  $(p, PQ)$ .

The above theorems may be used to prove the uniqueness of the decomposition of a function  $F(x)$  into its irreducible factors, modulo  $p$ . For were there two such factorizations, they would be congruent and that is,

$$(1) \quad F(x) \equiv P_1(x)P_2(x) \cdots P_\mu(x) \\ \equiv Q_1(x)Q_2(x) \cdots Q_\nu(x) \pmod{p}.$$

Let  $S(x)$  denote the product of all factors that are identical in both factorizations. The congruence (1) may accordingly be written in the form

$$S(x)[P(x) \cdots P_{\mu_1}(x) - Q(x) \cdots Q_{\nu_1}(x)] \equiv 0 \pmod{p};$$

and since  $S(x)$  is not divisible by  $p$ , this congruence is only satisfied if

$$P(x) \cdots P_{\mu_1}(x) \equiv Q(x) \cdots Q_{\nu_1}(x) \pmod{p},$$

where no factor appears at the same time on either side of the congruence.

Since the product  $Q(x) \cdots Q_{\nu_1}(x) \equiv 0 \pmod{p, P(x)}$ , it follows that one of the factors, say  $Q(x)$  is divisible by  $P(x)$ , modulo  $p$ . The function  $Q(x)$  being irreducible, modulo  $p$ , this is only true if  $P(x) \equiv Q(x) \pmod{p}$ .

It may happen that the function  $F(x)$  has several equal irreducible factors, so that the decomposition will take the form

$$F(x) \equiv P(x)^{h_1}P_1(x)^{h_2} \cdots P_\nu(x)^{h_\nu} \pmod{p},$$

where  $P(x), \cdots P_\nu(x)$  are all irreducible, modulo  $p$ .

ART. 196. We may next consider the more general reduced systems  $(p, f(x))$  and impose the condition that they be further decomposed. A pure modular system of the second kind  $(p, f(x))$  can clearly be decomposed only into factors which are pure systems of the second kind;

and if this is the case the numerical element must be the same in each of the component modular systems, this element being a prime integer, say  $p$ . Every such system may be supposed brought to its reduced form.

We have accordingly to solve the question: Under what condition is the factorization

$$(1) \quad (p, f(x)) \sim (p, f_1(x))(p, f_2(x)) \sim (p^2, pf_1, pf_2, f_1f_2)$$

possible?

Since  $p$  is divisible by the system on the right hand side, it follows that

$$p = p^2F(x) + pf_1(x)G_1(x) + pf_2(x)G_2(x) + f_1(x)f_2(x)H(x).$$

And as all terms contain  $p$  as a factor save the last, it is clear that  $H(x)$  must be divisible by  $p$ , say  $H(x) = pH_1(x)$ . It follows that

$$1 = pF(x) + f_1(x)[G_1(x) + f_2(x)H_1(x)] + f_2(x)G_2(x),$$

and from this it is seen that the necessary condition for the required factorization is

$$1 \sim (p, f_1(x), f_2(x)).$$

And that is, the two factors  $f_1(x)$  and  $f_2(x)$  must be relatively prime, modulo  $p$ .

Reciprocally, if  $(p, f_1, f_2) \sim 1$ , and therefore  $(p^2, pf_1, pf_2) \sim p$ , then is the right hand side of (1) equivalent to  $(p, f_1f_2)$ .

This system is accordingly equivalent to the original system  $(p, f(x))$ , if and only if there exists the congruence

$$(2) \quad f(x) \equiv f_1(x)f_2(x) \pmod{p}$$

together with the equivalence

$$(p, f_1(x), f_2(x)) \sim 1.$$

With this is given at once the complete factorization of a modular system  $(p, f(x))$  into its irreducible factors. For if

$$f(x) \equiv P(x)^h P_1(x)^{h_1} \cdots P_r(x)^{h_r} \pmod{p}$$

is the decomposition of  $f(x)$  into its irreducible factors, modulo  $p$ , then is

$$(p, f(x)) \sim (p, P(x)^h)(p, P_1(x)^{h_1}) \cdots (p, P_\nu(x)^{h_\nu})$$

the complete factorization of the modular system  $(p, f(x))$  into irreducible systems.

*Remark.* Observe that a fundamental difference exists between the factorizations of integers in  $[1]$  and the decomposition of modular systems in  $[1, x]$ . While the divisibility of an integer  $m$  through another integer  $d$  carries with it the decomposition into a product  $dd'$ , in the case of a modular system of the second kind this in general is not the case. For, clearly the modular system  $(p, P(x)^h)$  has as a divisor the system  $(p, P(x))$ , while it is not possible to express  $(p, P(x)^h)$  through the product of two systems of which one is  $(p, P(x))$ . A distinction must accordingly be made between the decomposition of a system and of its property of having a divisor. The property of being irreducible in no wise precludes a system from having a divisor, while on the other hand a system which has no further divisor, clearly cannot be further reduced.

The property that a modular system of the second kind has no further divisor characterizes it as a *prime modular system*, while those systems which can be decomposed no further may be called *irreducible*.

ART. 197. The following theorem offers a resumé of what has been proved in the preceding articles:

THEOREM. *A modular system of the second kind is then and only then a prime modular system, if it is equivalent to a system  $(p, P(x))$ , where  $p$  is a prime integer and where  $P(x)$  is irreducible (mod.  $p$ ).*

For if  $f_0(x)(f_1(x), \dots, f_k(x))$  is a mixed system of the second kind, it cannot be a prime system unless either  $f_0(x)$  or  $(f_1(x), \dots, f_k(x))$  is equivalent to unity. Otherwise there would be more than one divisor of the system. Were the system equivalent to  $f_0(x)$ , it would *not* be of the second kind. Consequently the original system must



be  $(M) \sim (f_1(x), \dots, f_k(x))$ , which is a pure modular system. If, however,  $(M)$  is a pure modular system of the second kind, and if  $m$  is a numerical element in it, and if  $p^h$  is an integer that divides  $m$ , then is  $(p^h, f_1(x), \dots, f_k(x))$  a divisor of  $(M)$ . If, further,  $(M) \sim (p, f_1(x), \dots, f_k(x))$ , where  $p$  is a prime integer,  $(p, f(x))$  being its reduced form, and if  $P(x)$  is a divisor of  $f(x)$ , modulo  $p$ , then  $(p, f(x))$  has as a divisor  $(p, P(x))$ . If, however,  $P(x)$  is irreducible, modulo  $p$ , then is  $(p, P(x))$  a prime modular system.

A prime modular system is never equivalent to unity unless  $P(x)$  is of the zero degree, and therefore a constant.

Suppose that  $(\Pi) = (p, P(x))$  is an arbitrary prime modular system, where

$$P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0$$

is an irreducible function, modulo  $p$ , in which the coefficients may take any of the integral values  $0, 1, \dots, p-1$ .

It is evident that every quantity of  $[1, x]$  is congruent, modulo  $(\Pi)$ , to a function

$$c_0 + c_1x + \dots + c_{n-1}x^{n-1},$$

where the coefficients  $c$  are to be found among the integers  $0, 1, \dots, p-1$ .

These functions are incongruent, modulo  $(\Pi)$ . Accordingly, there exists the theorem:

*The number  $\varphi(\Pi)$  of all incongruent units for a prime modular system  $(\Pi) = (p, P(x))$  is  $p^n - 1$ , where  $n$  is the degree of the function  $P(x)$ .*

Due to the theorem stated at the end of Art. 189 for arbitrary systems, it follows here for every arbitrary quantity  $X$  of  $[1, x]$  which is not divisible by  $(\Pi)$ , that the congruence

$$(1) \quad X^{p^n-1} \equiv 1 \pmod{p, P(x)};$$

or, if a quantity  $X_0 \equiv 0 \pmod{p, P(x)}$  is included, there exists the theorem:

*Every quantity  $X$  of the realm  $[1, x]$  satisfies the congruence*

$$X^{p^n} - X \equiv 0 \pmod{p, P(x)},$$

where  $n$  is the degree of  $P(x)$ .

COROLLARY. Corresponding to every unit  $e$  there exists a complementary unit  $e'$ , such that  $ee' \equiv 1 \pmod{p, P(x)}$ . For in the expression (1) above it is only necessary to put  $e' = e^{p^n-2}$ .

We have proved for a prime modular system  $(\Pi)$  there exists the theorem that a product is only divisible by this system when this is true for one of its factors. It follows that to every theorem regarding a prime integer  $p$  in  $[1]$  there corresponds a completely analogous theorem regarding  $(\Pi)$  in the realm  $[1, x]$ . In particular there exists here the theorem:

*A congruence for a prime modular system*

$$G(Z) = g_k Z^k + g_{k-1} Z^{k-1} + \dots + g_0 \equiv 0 \pmod{p, P(x)},$$

whose coefficients belong to  $[1, x]$ , cannot have more roots within this realm, than the degree of  $G(Z)$ .

Without changing the number of the roots of the congruence, all the coefficients of  $G(Z)$  may be reduced, modulo  $(\Pi)$ , while the coefficient of the highest power may be taken equal to 1. For the function  $G(Z)$  may be multiplied by  $g'_k$ , the complementary unit to  $g_k$ , and the roots of  $g'_k G(Z) \equiv 0$  are the same as those of  $G(Z) \equiv 0$ .

If such a congruence is

$$G(Z) \equiv Z^k + g_{k-1} Z^{k-1} + \dots + g_0 \equiv 0 \pmod{p, P(x)},$$

and if  $X_1$  is one of its roots, it is seen that

$$\begin{aligned} G(Z) \equiv G(Z) - G(X_1) &\equiv (Z^k - X_1^k) + \dots + g_1(Z - X_1) \\ &\equiv (Z - X_1)G_1(Z) \pmod{p, P(x)}, \end{aligned}$$

where  $G_1(Z)$  is a function of the same kind as  $G(Z)$  but of

degree  $k-1$  in  $Z$ . Accordingly if  $X_1$  is any root of the congruence  $G(Z) \equiv 0 \pmod{p, P(x)}$ , then its left hand side is divisible  $\pmod{p, P(x)}$  by the linear factor  $Z - X_1$ . If further  $X_2$  is a second root that is different from  $X_1$ , it follows from the above congruence that for  $Z_2 = X_2$ ,

$$G(X_2) \equiv (X_2 - X_1)G_1(X_2) \equiv 0 \pmod{p, P(x)};$$

and since  $X_2 - X_1$  is relatively prime to  $(\Pi)$ , it is seen that  $X_2$  must be a root of  $G_1(Z) \equiv 0$ . If then the congruence  $G(Z) \equiv 0$  of the  $k$ th degree had more than  $k$  roots, it would follow that the congruence  $G_1(Z) \equiv 0$  of degree  $k-1$  had more than  $k-1$  roots, in fact, all those of  $G(Z) \equiv 0$  with the exception of  $X_1$ . If we assume that the theorem is proved for congruences of the  $k-1$ st degree, it is therefore also true of those of the  $k$ th degree. Since the theorem is evidently true of congruences of the first degree  $Z + g_0 \equiv 0 \pmod{p, P(x)}$ , its validity is proved in general and there exist precisely the same theorems as are the case for the prime integer  $p$  in [1].

In particular if  $X_1, X_2, \dots, X_m$  are  $m$  incongruent roots of our congruence, then is for the variable  $Z$ :

$$G(Z) \equiv (Z - X_1) \cdots (Z - X_m) \bar{G}(Z) \pmod{p, P(x)},$$

where  $\bar{G}(Z)$  denotes an integral function of the  $(k-m)$ th degree.

The congruence  $Z^{p^n} - Z \equiv 0 \pmod{p, P(x)}$  has exactly the same number of roots as is its degree, namely, all of the  $p^n$  incongruent, modulo  $(\Pi)$ , residues:

$$R_0, R_1, \dots, R_{p^n-1}$$

of the realm  $[1, x]$ ; and therefore for a variable  $Z$  there exists the congruence

$$Z^{p^n} - Z \equiv Z \prod_{k=1}^{k=p^n-1} (Z - R_k) \pmod{p, P(x)}.$$

By equating the coefficient of  $Z$  on either side of the

congruence we have the following generalization of the Wilson Theorem

$$-1 \equiv \prod_{k=1}^{k=p^n-1} R_k \equiv \Pi(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \pmod{p, P(x)},$$

where the coefficients  $a_i$  independently of one another go over all integral values from 0 to  $p-1$  and are not all zero at the same time.

ART. 198. Write for  $Z$  any quantity  $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$  of the realm  $[1, x]$  with coefficients reduced, modulo  $p$ ; then as proved in the preceding article, is the difference  $Z^{p^n} - Z$  divisible by every prime modular system  $(p, P_n(x))$  in which the irreducible function  $P_n(x)$  is of the  $n$ th degree. In particular write  $Z = x$  and let us consider the problem of finding every modular system  $(p, P(x))$  which are divisors of the function

$$x^{p^n} - x.$$

The theorem may be proved without difficulty that the above function is also divisible by every prime modular system  $(p, P_\nu(x))$  for which the degree  $\nu$  of  $P_\nu(x)$  is a divisor of  $n$  and including  $n$ . For if  $P_\nu(x)$  is of degree  $\nu$ , then due to the theorem just proved,

$$x^{p^\nu} \equiv x \pmod{p, P_\nu(x)}.$$

Raised to the power  $p^\nu$ , this congruence offers

$$x^{p^{2\nu}} \equiv x \pmod{p, P_\nu(x)},$$

and in general

$$x^{p^{h\nu}} \equiv x \pmod{p, P_\nu(x)}.$$

If then  $n = h\nu$ , and that is, if  $\nu$  is any arbitrary divisor of  $n$ , it is seen that  $x^{p^n} - x$  has the divisor  $(p, P_\nu(x))$ .

It may be further proved that  $x^{p^n} - x$  is only divisible by such prime modular systems  $(p, P_\nu(x))$  for which  $\nu$  is a divisor of  $n$ . For suppose that any system  $(p, P_\nu(x))$  is a

divisor of  $x^{p^n} - x$ . Then there exist the two congruences

$$x^{p^n} \equiv x, \quad x^{p^\nu} \equiv x \pmod{p, P_\nu};$$

and from these we have as before the congruences

$$x^{p^{gn}} \equiv x, \quad x^{p^{\gamma\nu}} \equiv x \pmod{p, P_\nu(x)}.$$

If the first of these congruences is raised to the  $p^{\gamma\nu}$  power, we have with the use of the second,

$$(1) \quad x^{p^{gn+\gamma\nu}} \equiv x \pmod{p, P_\nu}.$$

From this it is seen, if  $g$  and  $\gamma$  are arbitrary positive integers, that  $x^{p^{gn+\gamma\nu}} - x$  is divisible by  $(p, P_\nu)$ .

Let  $d$  be the greatest common divisor of  $n$  and  $\nu$  and let  $g'$  and  $\gamma'$  be two integers such that

$$g'n + \gamma'\nu = d.$$

It follows for every integer  $r$  that

$$(g' + r\nu)n + (\gamma' + rn)\nu = d + 2rn\nu.$$

Let  $r$  be so chosen that  $g' + r\nu$  and  $\gamma' + rn$  are positive integers and writing these values for  $g$  and  $\gamma$  in (1), it follows that  $x^{p^{d+2rn\nu}} \equiv x$ ; or since  $x^{p^{2rn\nu}} \equiv x$ , we have

$$(x^{p^{2rn\nu}})^{p^d} \equiv x^{p^d} \equiv x \pmod{p, P_\nu(x)}.$$

It follows that  $x^{p^d} - x$  and therefore also the modular system  $(p, x^{p^d} - x)$  is divisible by  $(p, P_\nu(x))$ .

Further as will be proved in the next article, every quantity  $F(x)$  of  $[1, x]$  satisfies the congruence

$$F(x)^{p^d} - F(x) \equiv 0 \pmod{p, x^{p^d} - x};$$

and therefore, *a fortiori*,

$$(2) \quad F(x)^{p^d} - F(x) \equiv 0 \pmod{p, P_\nu(x)}.$$

It has been proved (Art. 197) that with respect to the modular system  $(p, P_\nu(x))$  there are exactly  $p^\nu$  incongruent roots. Accordingly, there exist for the congruence (2) exactly  $p^\nu$  incongruent roots. Since a congruence with respect to a prime modular system cannot have more roots than its degree, it is necessary that  $p^\nu \leq p^d$  or



$\nu \leq d$ . On the other hand, since  $d$  is a divisor of  $\nu$ , it is seen that  $d = \nu = (n, \nu)$ ; and that is,  $\nu$  must be a divisor of  $n$ .

We therefore have the theorem: *The function  $x^{p^n} - x$  has as divisors all and only those prime modular systems  $(p, P_d(x))$  for which the degree  $d$  of the function  $P_d(x)$  is a divisor of  $n$ .*

We shall next denote by  $d$  any divisors of  $n$  and by  $P_d(x), P'_d(x), \dots$ , all, modulo  $p$ , irreducible functions of  $x$  of degree  $d$ . Since the function  $x^{p^n} - x$  is divisible by all prime modular systems  $(p, P_d(x)), (p, P'_d(x)), \dots$ , it is also divisible by this product, and since

$$(p, P_d(x))(p, P'_d(x)) = (p, P_d(x)P'_d(x)),$$

it follows from previous considerations that  $x^{p^n} - x$  is divisible by the modular system

$$(p, \Pi P_d(x))$$

and by no other system  $(p, P_\delta(x))$ , where  $\delta$  is not a divisor of  $n$ . The symbol  $d/n$  under a product sign is read " $d$  a divisor of  $n$ ."

There exists accordingly a congruence

$$(3) \quad x^{p^n} - x \equiv \Pi_{d|n} \Pi_k P_d^{(k)}(x)^{h_d^{(k)}} \pmod{p},$$

where the first product means that  $d$  goes over all the divisors of  $n$ , whereas  $k$  in the second product distinguishes the different factors of the same degree, the exponent  $h_d^{(k)}$  denoting a positive integer which is to be determined.

We shall show that the function on the left of (3) has as a divisor each modular system  $(p, P_d(x))$  only once and therefore that the exponent  $h_d^{(k)}$  is equal to unity.

For were this function to have a prime factor, say  $P(x)$ , to the second power, say

$$x^{p^n} - x = P(x)^2 Q(x) + pR(x),$$

where  $Q(x)$  embodies all the remaining factors, modulo  $p$ , it would follow through differentiation that

$$p^n x^{p^n-1} - 1 = 2P(x)P'(x)Q(x) + P(x)^2Q'(x) + pR'(x);$$

or, if both sides are considered, modulis  $p$ ,  $P(x)$ , and all multiples of  $p$  and  $P(x)$  dropped, it would follow that

$$-1 \equiv 0 \pmod{p, P(x)}.$$

And that is,  $-1$  is an element of  $(p, P(x))$ , which modular system would accordingly be a unit system. And this requires that  $P(x)$  be a constant relatively prime to  $p$ .

It follows that the factorization (3) may be written

$$x^{p^n} - x \equiv \prod_{a|n} P_a(x) \pmod{p},$$

where the multiplication extends over all and only those irreducible functions, modulo  $p$ , whose degree is a divisor of  $n$ ; and from this congruence results the following decomposition of the modular system

$$(p, x^{p^n} - x) \sim \prod_{a|n} (p, P_a(x)).$$

This result Kronecker (*Vorlesungen*, p. 225) considered one of the most beautiful and important of the whole theory. See also Dedekind, Dirichlet-Dedekind, *Zahlentheorie*, 4<sup>th</sup> Edition, § 180.

ART. 199. In the present article we shall consider integral functions of any number of variables with integral coefficients and that is, quantities of the realm  $[1, x_1, x_2, \dots, x_k]$ .

Observe that for any prime integer  $p$  there exists the congruence

$$(x_1 + x_2 + \dots + x_k)^p \equiv x_1^p + x_2^p + \dots + x_k^p \pmod{p}.$$

If this process is repeated  $r$  times, the resulting congruence is

$$(x_1 + x_2 + \dots + x_k)^{p^r} \equiv x_1^{p^r} + x_2^{p^r} + \dots + x_k^{p^r} \pmod{p},$$

which may be written

$$\left(\sum_{h=1}^{h=k} x_h\right)^{p^r} \equiv \sum_{h=1}^{h=k} (x_h^{p^r} - x_h) + \sum_{h=1}^{h=k} x_h \pmod{p}.$$

Writing this congruence in the form of a modular system, we have

$$\left(\sum_{h=1}^{h=k} x_h\right)^{p^r} \equiv \sum_{h=1}^{h=k} x_h \pmod{p, \dots, x_h^{p^r} - x_h, \dots}.$$

Next let

$$f(z_1, z_2, \dots, z_\rho) = \sum_{\substack{k_1=1, 2, \dots, \\ \vdots \\ k_\rho=1, 2, \dots}} C_{k_1, k_2, \dots, k_\rho} z_1^{k_1} z_2^{k_2} \dots z_\rho^{k_\rho}$$

be any integral function in  $z_1, \dots, z_\rho$  with integral coefficients, and that is, quantities of the realm  $[1, z_1, \dots, z_\rho]$ .

Write in the above congruences for  $x_h$  each of the individual terms of the function  $f(z_1, \dots, z_\rho)$ , the sequence being arbitrary, so that

$$x_h = C_{k_1, \dots, k_\rho} z_1^{k_1} \dots z_\rho^{k_\rho}.$$

The modular system thereby becomes

$$\begin{aligned} (f(z_1, z_2, \dots, z_\rho))^{p^r} &\equiv f(z_1, z_2, \dots, z_\rho) \\ \pmod{p, \dots, [C_{k_1, \dots, k_\rho} z_1^{k_1}, \dots, z_\rho^{k_\rho}]^{p^r} - C_{k_1, \dots, k_\rho} z_1^{k_1} \dots z_\rho^{k_\rho}, \dots}. \end{aligned}$$

It may be shown as follows that this system is divisible by the simpler system

$$(p, z_1^{p^r} - z_1, \dots, z_k^{p^r} - z_k).$$

For due to the Fermat Theorem

$$C_{k_1, \dots, k_\rho}^{p^r} \equiv C_{k_1, \dots, k_\rho} \pmod{p};$$

and therefore also

$$\begin{aligned} (1) \quad &(p, \dots, [C_{k_1, \dots, k_\rho} z_1^{k_1} \dots z_\rho^{k_\rho}]^{p^r} - C_{k_1, \dots, k_\rho} z_1^{k_1} \dots z_\rho^{k_\rho}, \dots) \\ &\sim (p, \dots, C_{k_1, \dots, k_\rho} [(z_1^{k_1} \dots z_\rho^{k_\rho})^{p^r} - z_1^{k_1} \dots z_\rho^{k_\rho}], \dots). \end{aligned}$$

The latter system is divisible by

$$(p, \dots, z_i^{p^r} - z_i, \dots).$$

For, observe that the difference  $z_i^{k_i p^r} - z_i^{k_i}$  is divisible always

by  $z_i^{p^r} - z_i$ , when  $k_i$  is a positive integer. It follows then that

$$z_i^{k_i p^r} \equiv z_i^{k_i} \pmod{p, \dots, z_i^{p^r} - z_i, \dots};$$

and it is further seen that

$$z_1^{k_1 p^r} \dots z_\rho^{k_\rho p^r} - z_1^{k_1} \dots z_\rho^{k_\rho}$$

is divisible by

$$(p, \dots, z_i^{p^r} - z_i, \dots).$$

Accordingly, it is proved that the system (1) is divisible by the latter system. And with this is derived a generalized Fermat Theorem, which may be expressed as follows:

*Every quantity  $f(z_1, \dots, z_\rho)$  of an arbitrary realm  $[1, z_1, \dots, z_\rho]$  satisfies the congruence*

$$f^{p^r} \equiv f \pmod{p, \dots, z_i^{p^r} - z_i, \dots}$$

where  $p$  is any prime integer, and  $t = 1, 2, \dots, \rho$ .

**ART. 200.** If the realm is limited to  $[1, z]$ , the above congruence takes the form

$$(1) \quad (f(z))^{p^r} \equiv f(z) \pmod{p, z^{p^r} - z},$$

which written as an equation, is

$$f(z)^{p^r} - f(z) = p\varphi(z) + (z^{p^r} - z)\psi(z),$$

where  $\varphi(z)$  and  $\psi(z)$  are quantities of  $[1, z]$ . Observe that this is an identical equation true for every value of  $z$ .

We may so choose  $z$  that  $z^{p^r} - z$  vanishes, and that is, we may take for  $z$  one of the roots of  $z^{p^r} - z = 0$ . Neglecting the root  $z = 0$ , we shall take for  $z$  any of the  $p^r - 1$  roots of unity that satisfy

$$(2) \quad z^{p^r-1} - 1 = 0,$$

with the result that the equation (1) becomes for such roots

$$(3) \quad (f(z))^{p^r} \equiv f(z) \pmod{p}.$$

As examples of the latter congruence, let  $p$  be of the form  $6n + 1$ , say 7, 13, 19, 31, 37, 43,  $\dots$ , and let  $\omega$  be a primi-

tive third root of unity, say

$$\omega = e^{\frac{2\pi i}{3}} = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = \frac{-1 + i\sqrt{3}}{2}.$$

Since  $p-1 (=6n)$  is divisible by 3, it is seen that (2) is satisfied for  $r=1$  and accordingly, from (3)

$$(f(\omega))^p \equiv f(\omega) \pmod{p}.$$

If, however,  $p=6n-1$ , say 5, 11, 17, 23, 29,  $\dots$ , so that  $p-1$  is not divisible by 3, although 3 does divide  $p^2-1$ , then in (2)  $r=2$  and (3) becomes

$$(f(\omega))^{p^2} \equiv f(\omega) \pmod{p}.$$

If  $p$  is of the form  $4n+1$ , say 5, 13, 17, 29, 37,  $\dots$ , and if  $z$  is a fourth root of unity, for example,  $z=i$ , then is

$$f(i)^p \equiv f(i) \pmod{p};$$

however, if  $p$  is of the form  $4n-1$ , say 3, 7, 11, 19, 23,  $\dots$ , then is

$$f(i)^{p^2} \equiv f(i) \pmod{p}.$$

EXAMPLES. Writing  $\rho = e^{\frac{2\pi i}{5}}$ , show that:

$$(f(\rho))^p \equiv f(\rho) \pmod{p}, \text{ if } p=10n+1;$$

$$(f(\rho))^{p^2} \equiv f(\rho) \pmod{p}, \text{ if } p=10n-1;$$

$$(f(\rho))^{p^4} \equiv f(\rho) \pmod{p}, \text{ if } p=5n+2.$$

In general it is seen that if  $\rho = e^{\frac{2\pi i}{n}}$ , and if  $p$  is an arbitrary prime integer which does not divide  $n$ , then from (2) if  $r$  is the smallest exponent for which  $p^r \equiv 1 \pmod{n}$ , we have for every integral function  $f(\rho)$  with integral coefficients, the congruence

$$f(\rho)^{p^r} \equiv f(\rho) \pmod{p}.$$

ART. 201. Returning to the formula of Art. 198

$$x^{p^n} - x \equiv \prod_{d|n} P_d^{(1)} P_d^{(2)} \dots \pmod{p},$$

where the multiplication extended over all the different prime functions  $P_d^{(i)}(x)$ , modulo  $p$ , whose degree  $d$  is



equal to  $n$  or is a divisor of  $n$ , it is seen by equating the highest power of  $x$  on either side of the congruence, that

$$p^n = \sum_{d|n} dN_d,$$

where  $N_d$  denotes the number of different prime functions of the  $d$ th degree. It is clear that

$$nN_a = p^n - \sum p^{\frac{n}{a}} + \sum p^{\frac{n}{ab}} - \dots,$$

where the first summation extends over all the prime factors  $a$  of  $n$ , the second summation extending over all combinations  $a, b$ , of any two such factors, etc.

Employ a notation <sup>1</sup> due to Möbius: for any factor  $d$  occurring more than once as a divisor of  $n$ , let  $e_d = 0$ ; otherwise, when the number of factors constituting  $d$  is odd, let  $e_d = -1$ , while  $e_d = +1$ , when  $d$  consists of an even number of factors of  $n$ , and  $e_1 = 1$ . Accordingly, the above formula may be written

$$N_n = \frac{1}{n} \sum_{d|n} e_d p^{\frac{n}{d}}.$$

If the product of all the prime functions (mod.  $p$ ) of the  $d$ th degree be denoted by  $\Phi_d$  so that

$$P_d^{(1)} P_d^{(2)} \dots = \Phi_d;$$

and if further we put

$$\Psi_n = \prod_{d|n} \Phi_d,$$

so that

$$\log \Psi_n = \sum_{d|n} \log \Phi_d,$$

we have

$$\log \Phi_n = \log \Psi_n - \sum \log \Psi_{\frac{n}{a}} + \sum \log \Psi_{\frac{n}{ab}} - \dots,$$

and that is

$$\Phi_n = \frac{\Psi_n \prod \Psi_{\frac{n}{ab}} \dots}{\prod \Psi_{\frac{n}{a}} \prod \Psi_{\frac{n}{abc}} \dots}.$$

<sup>1</sup> See Dickson, *History*, Vol. I, Chapter XIX.

Observing the formula at the beginning of this article, we may write

$$\Phi_n = \frac{(x^{p^n} - x) \prod (x^{p^{ab}} - x) \dots}{\prod (x^{p^a} - x) \prod (x^{p^{abc}} - x) \dots};$$

or finally

$$\Phi_n(x) = \prod_{d|n} (x^{p^{\frac{n}{d}}} - x)^{e_d}.$$

ART. 202. We shall consider next the modular system  $(p, x^p - x)$ . Observe that any function whatever of  $[1, x]$  may be written in the form

$$F(x) = (x^p - x)\Psi(x) + \Phi(x),$$

where  $\Phi(x)$  is of the  $p-1$ st degree. Due to the Fermat Theorem, every rational integer  $a$  satisfies the congruence  $a^p - a \equiv 0 \pmod{p}$ . If then it is required that  $F(x)$  be divisible by  $p$  for every value of  $x$ , it is necessary and sufficient that  $\Phi(x)$ , which is of the form

$$\Phi(x) = a_0 + a_1x + a_2x^2 + \dots + a_{p-1}x^{p-1}$$

be divisible by  $p$ ; and that is, the congruence

$$\Phi(x) \equiv 0 \pmod{p}$$

must exist identically.

It follows that

$$\Phi(x) = p\Phi_1(x)$$

and with this the theorem: <sup>1</sup>

*In order that a function  $F(x)$  of the realm  $[1, x]$  be divisible by  $p$  for every integral value of  $x$ , it is necessary and sufficient that it be of the form*

$$F(x) = p\Phi(x) + (x^p - x)\Psi(x);$$

*and that is, that it be divisible by the modular system  $(p, x^p - x)$ .*

This theorem admits the following generalization: *The*

<sup>1</sup> See Hensel, *Crelle's Journal*, Vol. 113, p. 144.

necessary and sufficient condition that a function  $F(x, y, z, \dots)$  of the realm  $[1, x, y, z, \dots]$  be divisible by  $p$  for all integral values  $1, x, y, z, \dots$ , is that  $F(x, y, z, \dots)$  be of the form

$$F(x, y, z, \dots) = pG + (x^p - x)\Phi + (y^p - y)\Psi + (z^p - z)\Xi + \dots,$$

where the functions  $G, \Phi, \Psi, \Xi$  belong to  $[1, x, y, z, \dots]$  and that is, that  $F$  be divisible by the modular system  $(p, x^p - x, y^p - y, z^p - z, \dots)$ .

To prove this theorem, consider  $F(x, y, z, \dots)$  as a function of  $x$  and write it in the form

$$(1) \quad F(x, y, z, \dots) = (x^p - x)\Omega(x, y, z, \dots) + Q(x, y, z, \dots),$$

where  $\Omega$  and  $Q$  are functions of  $[1, x, y, z, \dots]$ , and  $Q$  is of degree at most  $p-1$  in  $x$ .

We may accordingly write  $Q$  in the form

$$(2) \quad Q(x, y, z, \dots) = Q_0 + xQ_1 + \dots + x^{p-1}Q_{p-1},$$

where  $Q_0, Q_1, Q_2, \dots, Q_{p-1}$ , are functions of  $[1, y, z, \dots]$ . If next we give to  $y, z, \dots$ , any arbitrary integral values and require that the function  $F(x, y, z, \dots)$  be divisible by  $p$  for every value of  $x$ , it is necessary and sufficient that the congruence

$$Q_0 + xQ_1 + x^2Q_2 + \dots + x^{p-1}Q_{p-1} \equiv 0 \pmod{p}$$

be identically satisfied. The necessary and sufficient condition for this is that each of the functions  $Q_i$  [ $i = 0, 1, \dots, p-1$ ] be divisible by  $p$  for every system of integral values of  $y, z, \dots$ . Observe that each of these functions contains one variable less than the original function  $F(x, y, z, \dots)$ .

Hence, assuming the theorem proved for any number of variables, it is seen that the coefficients  $Q_i$  must be of the form

$$Q_i = pG_i + (y^p - y)\Psi_i + (z^p - z)\Xi_i + \dots,$$

where  $G_i, \Psi_i, \Xi_i, \dots$  are functions of  $[1, y, z, \dots]$ . And

from (2) it follows that  $Q(x, y, z, \dots)$  must have the form

$$(3) \quad Q(x, y, z, \dots) = pG + (y^p - y)\Psi + (z^p - z)\Xi + \dots,$$

where  $G, \Psi, \Xi, \dots$ , are functions of  $[1, x, y, z, \dots]$ , and with this, due to (1), it is seen finally that the function  $F(x, y, z, \dots)$  must have the form asserted in the theorem. Since the theorem has been proved for functions  $F(x)$  of one variable, the inductive method proves its validity for any number of variables.

*Remark.* The discriminant of a modular system may be defined as an "elimination-resultant" of certain systems of equations. See Kronecker, *Ber. Sitzungsber.*, 1888, p. 451; *Werke*, Vol. III<sup>2</sup>, pp. 1 ff.

This discriminant is not to be confused, although it sometimes is, with the discriminant of a curve or surface, which offers a certain multiplicity (*Mannigfaltigkeit*) of the first rank (*Stufe*), while the vanishing of the former indicates a multiplicity of a higher rank. See § 25 of the *Grundzüge*. König, *Einleitung in die allgemeine Theorie der algebraischen Grössen*, seeks to give a systematic development of the Kronecker theory in two directions: the one, an algebra of affine transformations, the other, the general arithmetic of Kronecker as such.

See also Lasker, "Zur Theorie der Moduln und Ideale," *Math. Ann.*, Vol. 60, p. 20. Other references are found in the *Encyclopédie des sciences mathématiques*, Tome 1, Vol. 2, pp. 233 ff.

## CHAPTER IX

### NOTIONS INTRODUCTORY TO THE THEORY OF IDEALS

ART. 203. Before taking up the general theory of ideals, we shall consider their meaning and import in the simpler cases of the quadratic and cubic realms.

It may be well to introduce the conception of the ideal by means of certain well chosen examples. Sommer<sup>1</sup> employed the following example: Consider as the fixed realm of rationality the realm composed only of integers of the form  $4n+1$ , and permit in the discussion only the operations of multiplication and division in their usual sense.

In the series 1, 5, 9, 13, 17, 21, 25, 29,  $\dots$ , 45,  $\dots$ , 117,  $\dots$ , 517,  $\dots$  it is clear that the product of any two integers of the series is an integer of the series, since

$$(4n+1)(4m+1) = 4q+1,$$

where  $n$ ,  $m$ , and  $q$  are integers.

The numbers 5, 9, 13, 17, 21, 29, are irreducible in the realm of integers thus fixed; for example, 21 is *not* equal to the product of two other integers of the series. The number 10857, however, may be factored in the following two different ways  $10857 = 141 \cdot 77 = 21 \cdot 517$ , where 21, 77, 141, and 517 are irreducible in the fixed realm.

It is observed, however, that this factorization becomes unique if the fixed realm of integrity be extended so as to include *all* rational integers.

It is then seen that  $10857 = 3 \cdot 7 \cdot 11 \cdot 47$  is the unique factorization in the extended realm.

<sup>1</sup> Sommer, *Vorlesungen über Zahlentheorie*, p. 38.



Kummer's thought, when applied to the above special case, consists in replacing the factors 3, 7, 11, 47 by what may be called *ideals* in the restricted realm. In this realm observe that the integers 3, 7, 11, 47 as such, do *not* exist.

Denote the greatest common divisor of two integers by  $(a, b)$ , and observe that  $(a, b) = (b, a)$ . The expression  $(a, b)$  is called an *ideal*. It is here nothing other than the greatest common divisor of the integers  $a$  and  $b$  (Art. 113). Note that  $3 = (21, 141)$ .

In the extended realm, 3 may be replaced by the elements 21, 141, which are entities in the restricted realm. Further we may put

$$(7) = (21, 77), \quad (11) = (517, 77), \quad (47) = (517, 141).$$

It is evident that

$$(141) = (141, 21)(141, 517); \quad (77) = (77, 21)(77, 517),$$

and

$$(10857) = (141, 21)(141, 517)(77, 21)(77, 517) = 141 \cdot 77.$$

On the other hand

$$(21) = (21, 141)(21, 77); \quad (517) = (517, 77)(517, 141)$$

and

$$(10857) = (21, 141)(21, 77)(517, 77)(517, 141) = 21 \cdot 517.$$

Similarly it is seen that  $693 = 21 \cdot 33 = 9 \cdot 77$ , where the integers 21, 33, 9, 77, are irreducible in the fixed realm.

Observe that

$$(693) = (21, 9)(21, 77)(33, 9)(33, 77).$$

Again,  $441 = (21)^2 = 9 \cdot 49$ . We may write

$$(441) = (21, 9)(21, 49)(21, 9)(21, 49).$$

Here the *ideal*  $(a, b)$  in the restricted realm is merely the greatest common divisor of  $a, b$  in the extended realm.

In the usual realm of integrity we said (Art. 113) that a number  $k$  is divisible by the ideal  $(a, b)$  when  $k$  can be

expressed in the form  $k = xa + yb$ , where  $x$  and  $y$  are likewise rational integers. But if  $(a, b) = d$ , then also  $k = zd$ , where  $z$  is a rational integer. Corresponding to every pair of integral values  $x, y$  there is an integral value  $z$ , and *vice versa*.

It is clear that  $(a, b) = (a, b, ma + nb)$  where  $m$  and  $n$  are integers.

Any integer  $g$  is said to be *divisible* by the ideal  $(a, b)$  if  $g$  may be written in the form  $xa + yb = g$ , where  $x$  and  $y$  are integers. When  $g$  is divisible by  $(a, b)$ , we may add  $g$  as an element to the ideal, so that  $(a, b) = (a, b, g)$ .

ART. 204. Another illustration due to Hensel<sup>1</sup> is of interest. Let all the rational integers be distributed into two classes. Into the class  $C_0$  let unity and those integers enter which when factored offer an even number of prime factors, while class  $C_1$  is to include all those integers which when factored present an odd number of prime factors. It is seen that

$$C_0 = [1, 4, 6, 9, 10, 14, 15, 16, 21, 22, 24, \dots],$$

$$C_1 = [2, 3, 5, 7, 8, 11, 12, 13, 17, 18, 19, 20, 23, \dots].$$

Let the integers of one class only, say  $C_0$ , form a fixed realm. It is seen that

$$210 = 6 \cdot 35 = 10 \cdot 21 = 14 \cdot 15,$$

which are three products of prime integers in  $C_0$ . Observe, however, that we may write

$$\begin{aligned} 210 &= (6, 10)(6, 21)(35, 10)(35, 21) = 2 \cdot 3 \cdot 5 \cdot 7, \\ &= (6, 14)(6, 15)(35, 14)(35, 15) = 2 \cdot 3 \cdot 7 \cdot 5, \\ &= (10, 14)(10, 15)(21, 14)(21, 15) = 2 \cdot 5 \cdot 7 \cdot 3. \end{aligned}$$

Observe further that the ideals in each of the last three lines are equal; for example,  $(6, 10) = (6, 14) = (10, 14)$ . If then we call the integers of  $C_0$  the real integers and those of  $C_1$  the ideal integers, it is seen that 210 is equal

<sup>1</sup> Hensel, *Festschrift zur Feier des 100 Geburtstages Eduard Kummer*.

to the unique product of the four ideal (Kummer) integers 2, 3, 5, 7. Notice also that the elements of the ideals, say 6, 10 of (6, 10) are numbers of the fixed realm  $C_0$ .

ART. 205. Consider next the factorization of 21 in the realm  $\Re(\sqrt{-5})$ , namely,

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5}).$$

Clearly there is something *common* to 7 and at least to one of the factors  $(1 + 2\sqrt{-5})$ ,  $(1 - 2\sqrt{-5})$ . Take the product of these factors and form the congruence

$$1 - 2^2(-5) \equiv 0 \pmod{7}. \quad (i)$$

Note that  $-5 \equiv 3^2 \pmod{7}$ , so that (i) becomes

$$1 - 2^2 \cdot 3^2 \equiv 0 \pmod{7}.$$

From this it is seen that  $1 + 2 \cdot 3 \equiv 0 \pmod{7}$ . Compare this congruence with the factor  $1 + 2\sqrt{-5}$ . Kummer denoted that which is common to 7 and  $1 + 2\sqrt{-5}$  by the *Kummer factor*  $\{7, 3\} = k_1$ , while the Kummer factor  $k_2 = \{7, -3\}$  denotes what is common to 7 and  $1 - 2\sqrt{-5}$ .

Observing in a similar manner the congruence

$$1 - 2^2(-5) \equiv 0 \pmod{3}, \quad (ii)$$

it is seen that

$$-5 \equiv 2^2 \pmod{3};$$

and writing the congruence (ii) in the form

$$1 - 2^2 \cdot 2^2 \equiv 0 \pmod{3},$$

it is seen that

$$k_3 = \{3, 2\} \quad \text{and} \quad k_4 = \{3, -2\}$$

are the Kummer factors of 3 and  $1 + 2\sqrt{-5}$ ; 3 and  $1 - 2\sqrt{-5}$ , respectively.

Similarly, that which is common to 7 and  $4 + \sqrt{-5}$  is the Kummer factor  $k_1 = \{7, 3\}$  while  $k_2 = \{7, -3\}$  is the factor of 7 and  $4 - \sqrt{-5}$ ; and  $k_3 = \{3, 2\}$  is the Kummer factor of 3 and  $4 + \sqrt{-5}$ ,  $k_4 = \{3, -2\}$  being that of 3 and  $4 - \sqrt{-5}$ .

Hence, associated with the factors

$$(k_1k_2)(k_3k_4) = (k_1k_4)(k_2k_3) = (k_1k_3)(k_2k_4)$$

are the integers

$$7 \cdot 3 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

In the realm of natural numbers the Kummer factors have no objective reality. Hence, the name *ideal*. As such they have no quantitative existence. (Smith's *Report*, p. 110.)

In the more general quadratic realm  $\mathfrak{R}(\sqrt{m})$ ,  $m \not\equiv 1 \pmod{4}$ , we have to do with the factorization of integers  $x + \sqrt{m}y$  (Art. 97). And as above we are led to the consideration of the congruence  $x^2 - my^2 \equiv 0 \pmod{p}$ .

If  $w^2 \equiv m \pmod{p}$  or  $w^2 - pr = m$ , where  $r$  is an integer, we have a Kummer factor  $\{p, w\}$  defined through the congruence

$$x + wy \equiv 0 \pmod{p}.$$

This congruence put in the form of an equation is

$$x = pz - wy.$$

From this it follows that

$$x^2 - my^2 = p(pz^2 - 2wzy + ry^2).$$

Hence, corresponding to the Kummer factor  $\{p, w\}$  of  $p$  and  $x + \sqrt{m}y$ , there is associated a quadratic form  $(p, w, r)$ , and consequently a class of equivalent forms with determinant  $m$  through which  $p$  (connected with  $w$  as above defined) may be expressed. Then and only then when the class to which  $(p, w, r)$  belongs is a principal class  $(1, 0, m)$  can  $p$  be expressed through the form

$$p = x^2 - my^2 = (x + \sqrt{m}y)(x - \sqrt{m}y).$$

In this case and only in this case are the Kummer ideal factors  $\{p, w\}$  and  $\{p, -w\}$  numbers (algebraic) and have a real existence.

This offers the condition under which the rules of

division that exist in the rational realm are also true in the quadratic realms without the necessity of introducing the Kummer factors. This is evidently the case when the number of non-equivalent classes of quadratic forms with determinant  $m$  is unity. When the quadratic form through which the prime ideal  $p$  may be expressed is not equivalent to the principal form it is necessary to introduce the ideal factors to effect factorization of the rational prime integers into irreducible factors uniquely. Thus it is shown that the theory of quadratic forms with determinant  $m$  is exactly correlated with the theory of algebraic numbers of the realm  $\mathfrak{R}(\sqrt{m})$ . (See Art. 272.)

The same is true for the theory of any higher realms. In such realms there occur forms of a higher degree and the distribution of these forms into their linear factors corresponds to the unique factorization of the integers of these realms into their irreducible elements. This will be considered further in the chapter on Kronecker's Linear Forms and in the chapter on Factorable Forms. While this is the kernel of the matter, the method to be pursued in this direction is not so direct as that found in the Dedekind theory.

The Kummer theory may with some modification be so changed that the ideal factors of unreal existence may be replaced by "*ideals*" of a concrete form. For, if a Kummer ideal prime factor  $\{p, w\}$  of  $p$  is defined through the congruence

$$x + wy \equiv 0 \pmod{p},$$

it is seen that the collectivity (complex) of all integers of the form  $x + y\sqrt{m}$  which are divisible by  $\{p, w\}$  with a suitable choice of  $x, y$ , may also be expressed through  $x = pz - wy$ . And that is, the complex of all those algebraic numbers that are divisible by  $\{p, w\}$  is of the



form

$$pz + (\sqrt{m} - w)y.$$

It is thus seen that these numbers are all expressed through the modul

$$a = [p, \sqrt{m} - w].$$

And it is further seen that any number of this modul  $pz + (\sqrt{m} - w)y$  when multiplied by any integer of the realm, say  $x' + y'\sqrt{m}$  is equal to

$$p(zx' - ryy' + wzy') + (\sqrt{m} - w)(yx' + pzy' - wyy'),$$

if we write  $w^2 - m = pr$ .

Observe that this latter expression is of the form

$$pZ + (\sqrt{m} - w)Y,$$

and that is, a number of the modul  $a$  when multiplied by an integer of the realm  $\mathfrak{R}(\sqrt{m})$  is a number of the modul  $a$ . The counterpart of this in the theory of rational integers is: if an integer is divisible by the rational integer  $a$ , then the product of the first integer by any other integer is divisible by  $a$ . This might in a measure be used to define a rational integer  $a$ . It is used by Dedekind to define an ideal  $i = [\alpha, \beta]$ , where the element  $p$  above is replaced by  $\alpha$  and where  $\beta$  stands for  $\sqrt{m} - w$ . Accordingly, the ideal  $i$  is defined as the complex of integers  $\alpha\lambda + \beta\mu$  where  $\lambda$  and  $\mu$  run through all the integers of the given realm, and where  $\alpha$  and  $\beta$  are definite fixed integers of this realm (see Art. 272, end).

### THE IDEALS OF THE QUADRATIC<sup>1</sup> REALMS

**ART. 206. DEFINITION.** *A system of integers  $\alpha, \beta, \gamma, \dots$  of the realm  $\mathfrak{R}(\sqrt{m})$ , say  $i = (\alpha, \beta, \gamma, \dots)$ , such that every linear expression  $\alpha\lambda + \beta\mu + \gamma\nu + \dots$ , where  $\lambda, \mu, \nu, \dots$  are any integers in  $\mathfrak{R}(\sqrt{m})$ , forms an integer that belongs to the system, is called an ideal of the realm.*

<sup>1</sup> Report on Algebraic Numbers, p. 5.

Any integer  $\tau$  that is divisible by the ideal  $i$  may be expressed in the form  $\tau = \alpha\lambda_1 + \beta\mu_1 + \gamma\nu_1 + \dots$ , where  $\lambda_1, \mu_1, \nu_1, \dots$  are definite integers of  $\mathfrak{R}(\sqrt{m})$ . Such an integer  $\tau$  may be added as an element to  $i$  so that  $i = (\alpha, \beta, \gamma, \dots, \tau)$ . Thus any integer  $\tau$  is *divisible* by  $i$  when it may be adjoined or added as an element of  $i$ .

In particular, an ideal is called a *principal* ideal, when the integers that belong to it are multiples of *one* integer, say  $\alpha$ ; for example,  $i = (\alpha, \alpha\lambda, \alpha\mu, \dots)$  or simply  $i = (\alpha)$ .

If the ideal contains 1 or any integer that is a divisor of 1, it is called a *unit ideal*, and written  $i = (1)$ .

The ideals are denoted by German letters  $a, b, \dots, p$ .

DEFINITION. *Two ideals  $(\alpha, \beta, \gamma, \dots)$  and  $(\alpha_1, \beta_1, \gamma_1, \dots)$  of the realm  $\mathfrak{R}(\sqrt{m})$  are equal, and written*

$$(\alpha, \beta, \gamma, \dots) = (\alpha_1, \beta_1, \gamma_1, \dots),$$

*if every integer  $\alpha$  of the first ideal belongs to the second ideal, that is, if  $\alpha = \alpha_1\lambda + \beta_1\mu + \dots$ , and, if, reciprocally, every integer  $\alpha_1$  of the second ideal belongs to the first, so that  $\alpha_1 = \alpha\lambda_1 + \beta\mu_1 + \dots$ , where  $\lambda, \mu, \dots, \lambda_1, \mu_1, \dots$  are integers of the realm, with similar conditions for  $\beta, \beta_1$ , etc.*

For the multiplication of ideals the following may serve as a definition: *If  $a = (\alpha, \beta, \gamma, \dots)$  and  $b = (\alpha_1, \beta_1, \gamma_1, \dots)$  are two ideals of the realm  $\mathfrak{R}(\sqrt{m})$ , then the product of these ideals is had, if every element of  $a$  is multiplied by every element of  $b$ , the terms thus had forming the elements of the ideal  $a \cdot b$ , that is*

$$a \cdot b = (\alpha\alpha_1, \alpha\beta_1, \dots, \beta\alpha_1, \beta\beta_1, \dots, \gamma\alpha_1, \gamma\beta_1, \dots).$$

From this definition it is seen at once that the two factors may be interchanged and that  $ab = ba$ .

*An ideal  $a$  is divisible by an ideal  $b$ , if there is an ideal  $c$  of the realm such that  $ab = c$ .*

Thus while multiplication and division of integers may

be extended to ideals, the conception of addition and subtraction cannot be extended to ideals.

**THEOREM.** *In every ideal of the realm  $\mathfrak{K}(\sqrt{m})$  there may be derived in an infinite number of ways two integers  $\iota_1$  and  $\iota_2$  of the realm such that every number of the ideal may be expressed as a linear combination of these two integers with integral rational coefficients  $l_1$  and  $l_2$  in the form*

$$l_1\iota_1 + l_2\iota_2.$$

Write the ideal  $i$  so that every element is expressed through the basis of the realm in the form (Art. 97)

$$i = (a_1 + b_1\omega, a_2 + b_2\omega, a_3 + b_3\omega, \dots, G_1, G_2, \dots)$$

where  $a_1, b_1, a_2, b_2, \dots, G_1, G_2, \dots$  are rational integers.

It will be proved first that if  $a_1 + b_1\omega$  and  $a_2 + b_2\omega$  are any two numbers of the ideal, there belongs also to the ideal a number  $a' + b'\omega$ , in which  $b'$  is the greatest common divisor of  $b_1$  and  $b_2$ . For there belongs to the ideal the integer  $x(a_1 + b_1\omega) + y(a_2 + b_2\omega)$ , where  $x$  and  $y$  are rational integers which may be so chosen that  $xb_1 + yb_2 = b'$ . By repetition, it is evident that the integer  $g + i_2\omega$  belongs to the ideal, where  $g$  is a rational integer and  $i_2$  the greatest common divisor of  $b, b_1, b_2, \dots$ .

Since  $\frac{b_1}{i_2}$  is a rational integer, it is clear that we may adjoin as an element of the ideal

$$a_1 + b_1\omega - \frac{b_1}{i_2}(g + i_2\omega) = g_1.$$

Having adjoined  $g + i_2\omega$  and  $g_1$  as elements of the ideal, it is seen that  $a_1 + b_1\omega$  may be expressed linearly in terms of these two elements and consequently dropped from the ideal.

Similarly writing

$$a_2 + b_2\omega - \frac{b_2}{i_2}(g + i_2\omega) = g_2,$$

it is clear that if  $g_2$  is adjoined as an element to the ideal, then  $a_2 + b_2\omega$  may be dropped from it. By continuing this process, the ideal  $i$  becomes

$$i = (g + i_2\omega, g_1, g_2, g_3, \dots, G_1, G_2, \dots).$$

If  $i$  is the greatest common divisor of  $g_1, g_2, \dots, G_1, G_2, \dots$ , it is possible to determine rational integers  $a_1, a_2, \dots, A_1, A_2, \dots$ , such that

$$a_1g_1 + a_2g_2 + \dots + A_1G_1 + A_2G_2 + \dots = i.$$

Hence  $i$  may be added as an element to the system; then, since the integers  $g_1, g_2, \dots, G_1, G_2, \dots$  are all divisible by  $i$ , they may be dropped from the ideal, which becomes  $(i, g + i_2\omega)$ .

Suppose further that  $g$  is greater than  $i$  so that  $g = ig' + i_1$  where  $i_1 < i$ . We may then add as an element to the ideal  $g + i_2\omega - g'i = i_1 + i_2\omega$ . When this has been done, it is seen that  $g + i_2\omega$  may be dropped, since this element may be expressed linearly in terms of  $i$  and  $i_1 + i_2\omega$ . Thus the original ideal becomes finally

$$i = (i, i_1 + i_2\omega) = (\iota_1, \iota_2), \quad \text{where } \iota_1 = i, \iota_2 = i_1 + i_2\omega.$$

When an ideal has been reduced to the form  $(i, i_1 + i_2\omega)$ , it is said to be in its *canonical form*. Further note that  $\omega i + (i_1 + i_2\omega)$  is an integer that belongs to the given ideal and consequently the coefficient of  $\omega$  is divisible by  $i_2$ . It follows that  $i + i_2$  is divisible by  $i_2$  and therefore also  $i$  is divisible by  $i_2$ . If  $\omega'$  is the conjugate of  $\omega$ , it is clear also that  $\omega'(i_1 + i_2\omega)$  is an integer of the ideal, and it follows that  $i_1$  is divisible by  $i_2$ .

The quantities  $\iota_1, \iota_2$  form a *basis* of the ideal  $i$ . Any other basis (Art. 94) say

$$\iota_1^* = a_1\iota_1 + b_1\iota_2,$$

$$\iota_2^* = a_2\iota_1 + b_2\iota_2,$$

is had, if the determinant  $a_1b_2 - a_2b_1 = \pm 1$ . In this case  $i = (\iota_1, \iota_2) = (\iota_1^*, \iota_2^*)$ .

ART. 207. **Applications.** We saw (Art. 205) that in the realm  $\mathfrak{R}(\sqrt{-5})$

$$21 = 3 \cdot 7 = (4 - \sqrt{-5})(4 + \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

It may be proved that

$$\begin{aligned} 21 &= (3, 4 - \sqrt{-5})(3, 4 + \sqrt{-5})(7, 4 + \sqrt{-5}) \\ &\qquad \qquad \qquad \times (7, 4 - \sqrt{-5}) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 \\ &= (3, 1 + 2\sqrt{-5})(3, 1 - 2\sqrt{-5})(7, 1 + 2\sqrt{-5}) \\ &\qquad \qquad \qquad \times (7, 1 - 2\sqrt{-5}) = \mathfrak{p}_5 \mathfrak{p}_6 \mathfrak{p}_7 \mathfrak{p}_8 \\ &= (4 - \sqrt{-5}, 1 + 2\sqrt{-5})(4 + \sqrt{-5}, 1 - 2\sqrt{-5}) \\ &\qquad \times (4 + \sqrt{-5}, 1 + 2\sqrt{-5})(4 - \sqrt{-5}, 1 - 2\sqrt{-5}) \\ &\qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad = \mathfrak{p}_9 \mathfrak{p}_{10} \mathfrak{p}_{11} \mathfrak{p}_{12}. \end{aligned}$$

For, writing for brevity  $\mathfrak{p}_1 = (3, 4 - \sqrt{-5})$ ,  $\mathfrak{p}_2 = (3, 4 + \sqrt{-5})$ , etc., in the order indicated, it may be proved first that

$$\mathfrak{p}_1 = \mathfrak{p}_5 = \mathfrak{p}_9; \quad \mathfrak{p}_2 = \mathfrak{p}_6 = \mathfrak{p}_{10}; \quad \mathfrak{p}_3 = \mathfrak{p}_7 = \mathfrak{p}_{11}; \quad \mathfrak{p}_4 = \mathfrak{p}_8 = \mathfrak{p}_{12}.$$

To prove this observe that

$$1 + 2\sqrt{-5} = (4 - \sqrt{-5}) \cdot 1 - 3(1 - \sqrt{-5})$$

and

$$4 - \sqrt{-5} = (1 + 2\sqrt{-5}) \cdot 1 + 3(1 - \sqrt{-5}).$$

Hence,

$$\begin{aligned} \mathfrak{p}_1 &= (3, 4 - \sqrt{-5}) = (3, 4 - \sqrt{-5}, 1 + 2\sqrt{-5}) \\ &= (3, 1 + 2\sqrt{-5}) = \mathfrak{p}_5. \end{aligned}$$

This follows directly; for

$$(3, 4 - \sqrt{-5}) = (3, 3 + 1 + (2 - 3)\sqrt{-5}) = (3, 1 + 2\sqrt{-5}).$$

And similarly

$$\mathfrak{p}_9 = (4 - \sqrt{-5}, 1 + 2\sqrt{-5}, 9, 21, 3) = (3, 4 - \sqrt{-5}) = \mathfrak{p}_1.$$

Secondly, it is seen that

$$\begin{aligned} (3, 4 + \sqrt{-5})(3, 4 - \sqrt{-5}) \\ = (3^2, 3(4 + \sqrt{-5}), 3(4 - \sqrt{-5}), 21, 3) = (3) \end{aligned}$$

while

$$(7, 4 + \sqrt{-5})(7, 4 - \sqrt{-5}) = (7),$$

etc. Then by means of the ideals we have the unique



factorization of (21) as the product  $p_1 p_2 p_3 p_4$ . Further observe that

$$(3, 4 + \sqrt{-5})(7, 4 + \sqrt{-5}) \\ = (21, 3(4 + \sqrt{-5}), 7(4 + \sqrt{-5}), 11 + 8\sqrt{-5});$$

and since the greatest common divisor of 3 and 7 is 1, it is seen that  $4 + \sqrt{-5}$  may be added as an element of the ideal on the right. Since both 21 and  $11 + 8\sqrt{-5}$  are divisible by  $4 + \sqrt{-5}$ , it follows that

$$p_2 p_3 = (3, 4 + \sqrt{-5})(7, 4 + \sqrt{-5}) = (4 + \sqrt{-5}).$$

Similarly we have

$$p_1 p_4 = (3, 4 - \sqrt{-5})(7, 4 - \sqrt{-5}) = (4 - \sqrt{-5}), \\ p_1 p_3 = (3, 4 - \sqrt{-5})(7, 4 + \sqrt{-5}) = (1 + 2\sqrt{-5}), \\ p_2 p_4 = (3, 4 + \sqrt{-5})(7, 4 - \sqrt{-5}) = (1 - 2\sqrt{-5}).$$

In this realm it is seen that

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}),$$

or, since

$$(2, 1 - \sqrt{-5}) = (2, 1 + \sqrt{-5}) = q_5,$$

we have

$$(2) = (2, 1 + \sqrt{-5})^2.$$

Thus in the realm  $\mathfrak{R}(\sqrt{-5})$ , the prime ideal factors of the integers 2, 3, 4, 5, 6, 7, 8, 9, 10 are found among  $p_1, p_2, p_3, p_4, q_1, q_2 = (\sqrt{-5})$ .

As a second example, observe that in the realm  $\mathfrak{R}(\sqrt{10})$  the fundamental units are  $3 \pm \sqrt{10}$  ( $\epsilon$ , or  $\epsilon'$ ) and that

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10}).$$

Form the ideals

$$(2, 4 + \sqrt{10}) = (2, \sqrt{10}) = p_1 = (2, 4 - \sqrt{10}), \\ (3, 4 + \sqrt{10}) = (3, 1 + \sqrt{10}) = p_2, \\ (3, 4 - \sqrt{10}) = (3, 1 - \sqrt{10}) = p_3.$$

It is evident that

$$(6) = (2, \sqrt{10})^2 (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}) = p_1^2 p_2 p_3;$$

for

$$(2, \sqrt{10})^2 = (4, 2\sqrt{10}, 10) = (2)$$

and

$$(3, 1 + \sqrt{10})(3, 1 - \sqrt{10}) = (9, 3 + 3\sqrt{10}, 3 - 3\sqrt{10}, 6) = (3).$$

Similarly it is seen that

$$\begin{aligned} (2, \sqrt{10})(3, 1 + \sqrt{10}) &= (6, 2 + 2\sqrt{10}, 3\sqrt{10}, 10 + \sqrt{10}) \\ &= (6, 2 + 2\sqrt{10}, 3\sqrt{10}, 10 + \sqrt{10}, 4 + \sqrt{10}) = (4 + \sqrt{10}) \end{aligned}$$

and

$$(2, \sqrt{10})(3, 1 - \sqrt{10}) = (4 - \sqrt{10}).$$

In this realm show that

$$\begin{aligned} (5) &= (5, \sqrt{10})(5, \sqrt{10}), \\ (13) &= (13, 6 + \sqrt{10})(13, 6 - \sqrt{10}). \end{aligned}$$

As a third example consider the integers of the realm  $\Re(\sqrt{-15})$ . Since  $-15 \equiv +1 \pmod{4}$ , the basis of this realm is  $\left(1, \omega = \frac{1 + \sqrt{-15}}{2}\right)$ , and the integers of the realm are  $a + b\omega$ , where  $a$  and  $b$  are rational integers. It is seen that

$$\begin{aligned} (2) &= (2, \omega)(2, \omega') \\ (3) &= (3, \sqrt{-15})^2 = (3, -1 + 2\omega)^2 \\ &= (3, -1 + 2\omega, 3\omega - (-1 + 2\omega))^2 \\ &= (3, 1 + \omega)^2 \end{aligned}$$

(canonical form). It is also seen that

$$(5) = (5, \sqrt{-15})^2 = (5, -1 + 2\omega)^2 = (5, 2 + \omega)^2$$

(canonical form).

$$(17) = (17, 5 + \omega)(17, 5 + \omega').$$

In this realm note that 3 is divisible by the second power of an ideal, as is also 5; further observe that both 3 and 5 are divisors of the discriminant of this realm.

**ART. 208. Realms in Which There Exist Only Principal Ideals.** Such realms are clearly those in which Euclid's Algorithm for division is applicable. For if  $\tau$  is the

greatest common divisor of the algebraic numbers  $\alpha, \beta, \gamma, \dots$ , then is  $(\alpha, \beta, \gamma, \dots) = (\alpha, \beta, \gamma, \dots, \tau) = (\tau)$ .

**ART. 209. Congruences with Respect to Ideals. The Norm of an Ideal.** We say that  $\alpha$  is congruent to zero with respect to the ideal  $\mathfrak{a}$ , and write  $\alpha \equiv 0 \pmod{\mathfrak{a}}$ , when  $\alpha$  is one of the numbers that belong to the ideal  $\mathfrak{a}$ ; and that is  $\alpha = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots$ , where  $\lambda_1, \lambda_2, \dots$  are definite algebraic integers in the realm to which  $\mathfrak{a} = (\alpha_1, \alpha_2, \dots)$  belongs. Similarly  $\alpha \equiv \beta \pmod{\mathfrak{a}}$ , when  $\alpha - \beta$  can be written in the above linear form.

If an ideal  $\mathfrak{a}$  is given, all the integers of the realm in which  $\mathfrak{a}$  is defined may be distributed into classes, such that the integers of every class are congruent to one another with respect to the ideal; and no integer of one class is congruent to an integer of another class with respect to this ideal. Any integer of a class being congruent  $\pmod{\mathfrak{a}}$  to any other integer of the same class may be chosen as a *representative* of this class. The number of representatives is equal to the number of classes and no representative is congruent  $\pmod{\mathfrak{a}}$  to any other representative. Such a system of representatives constitute a *complete system of incongruent residues* with respect to  $\mathfrak{a}$ . *The number of representatives constituting such a system of incongruent residues with respect to the ideal  $\mathfrak{a} = (i, i_1 + i_2\omega)$  is  $|i \cdot i_2|$ .* This number is called the *norm* of  $\mathfrak{a}$  and is written  $N(\mathfrak{a})$ . It is the number of classes into which the integers of the realm may be distributed with respect to the modulus  $\mathfrak{a}$ . Consider any integer  $a + b\omega$  with respect to  $\mathfrak{a}$ .

It is seen that  $a$  can have any of the values

$$(I) \begin{cases} a = 0, 1, 2, \dots, i-1 \text{ and that } b \text{ can take values} \\ b = 0, 1, 2, \dots, i_2-1 \text{ where } i, i_2 \text{ may be taken positive.} \end{cases}$$

The system (I) forms a system of  $i \cdot i_2$  numbers which satisfy the two following conditions:

1st. No two numbers are congruent with respect to  $\mathfrak{a}$ .  
For if

$$a_k + b_k\omega - (a_l + b_l\omega) \equiv 0 \pmod{\mathfrak{a}},$$

then is  $a_k - a_l + (b_k - b_l)\omega$  a number of the ideal  $\mathfrak{a}$  and consequently  $(b_k - b_l)$  is divisible by  $i_2$ . This can be true only if  $b_k = b_l$  since both of these numbers are less than  $i_2$ , and then  $a_k - a_l$  must be divisible by  $i$ . It follows that  $a_k = a_l$ , for both  $a_k$  and  $a_l$  are less than  $i$ .

2nd. Any number  $A + B\omega$  of the realm is congruent to one and only one of the number  $a + b\omega$  with respect to  $\mathfrak{a}$ , where  $a$  and  $b$  take values as indicated in (I). For writing

$$A + B\omega - (a + b\omega) = l_1i + l_2(i_1 + i_2\omega),$$

we may so determine  $b (< i_2)$  that

$$B - b = l_2i_2,$$

where  $l_2$  is a definite integer, and then  $a (< i)$  may be so determined that

$$A - a - l_2i_1 = l_1i,$$

where  $l_1$  is a definite integer.

It may be next shown that if  $i_1^*$  and  $i_2^*$  constitute an arbitrary basis of the ideal  $\mathfrak{a} = (i, i_1 + i_2\omega)$ , and if  $i_1^* = a_1 + b_1\omega$  and  $i_2^* = a_2 + b_2\omega$ , then is

$$N(\mathfrak{a}) = \begin{vmatrix} a_1, & b_1 \\ a_2, & b_2 \end{vmatrix} = i \cdot i_2.$$

For the basal elements  $i_1^*$  and  $i_2^*$  may be written

$$i_1^* = ri + s(i_1 + i_2\omega),$$

$$i_2^* = ti + u(i_1 + i_2\omega),$$

where

$$\begin{vmatrix} r, & s \\ t, & u \end{vmatrix} = \pm 1$$

(Art. 94). It follows that

$$a_1 = ri + si_1, \quad b_1 = si_2,$$

$$a_2 = ti + ui_1, \quad b_2 = ui_2,$$

and consequently:

$$\left| \begin{array}{cc} a_1 & b_1 \\ a_2 & b_2 \end{array} \right| = i i_2 \left| \begin{array}{cc} r & t \\ s & u \end{array} \right| = i i_2,$$

where the *positive* sign is to be taken, since the norm is always a positive integer.

It is thus seen that the *norm of an ideal is independent of its basis*.

*The norm of an ideal is the product of conjugate ideals.* If in the ideal  $\mathfrak{a} = (\alpha, \beta, \gamma, \dots)$  we write the conjugates of  $\alpha, \beta, \dots$ , we derive another ideal, say,  $\mathfrak{a}' = (\alpha', \beta', \gamma', \dots)$  which is called the *conjugate* of  $\mathfrak{a}$ .

**THEOREM.** *The product of an ideal and its conjugate is a rational principal ideal, and in fact*

$$|\mathfrak{a} \cdot \mathfrak{a}'| = i \cdot i_2 = N(\mathfrak{a}).$$

For let

$$\mathfrak{a} = (i, i_1 + i_2 \omega), \quad \mathfrak{a}' = (i, i_1 + i_2 \omega').$$

It was seen in Art. 206 that  $i$  and  $i_1$  are multiples of  $i_2$ . Write  $i = a i_2$  and  $i_1 = a_1 i_2$ , where  $a$  and  $a_1$  are integers. It follows that

$$\mathfrak{a} = (i_2)(a, a_1 + \omega), \quad \mathfrak{a}' = (i_2)(a, a_1 + \omega')$$

and consequently  $\mathfrak{a} \mathfrak{a}' = (i_2)^2 (a, a_1 + \omega) (a, a_1 + \omega')$ .

Further note that

$$(a_1 + \omega)(a_1 + \omega') \equiv 0 \pmod{a};$$

for  $a$  is a divisor of every rational integer of the ideal  $(a, a_1 + \omega)$ . Through multiplication we have

$$\mathfrak{a} \cdot \mathfrak{a}' = (i_2)^2 (a^2, a(a_1 + \omega), a(a_1 + \omega'), (a_1 + \omega)(a_1 + \omega')).$$

**CASE I.** When  $m \equiv 3 \pmod{4}$ ,  $\omega = \sqrt{m}$ ,  $\omega' = -\sqrt{m}$ , observe that

$$\begin{aligned} \mathfrak{a} \cdot \mathfrak{a}' &= (i_2)^2 (a) \left( a, a_1 + \omega, a_1 + \omega', \frac{a_1^2 - m}{a} \right) \\ &= (i_2)^2 (a) \left( a, a_1 + \sqrt{m}, a_1 - \sqrt{m}, 2a_1, 2m, \frac{a_1^2 - m}{a} \right). \end{aligned}$$



Further it may be shown that the greatest common divisor of  $a, 2m, \frac{a_1^2 - m}{a}$  is 1. For suppose that these three integers have as a divisor the prime number  $q > 2$ . It is clear that if we put  $a = qb$ , then  $\frac{a_1^2 - m}{q^2 b}$  must be an integer, and since  $a_1^2 - m$  is divisible by  $q$  as is  $2m$  by hypothesis, it follows that  $a_1^2$  is divisible by  $q$  and consequently  $a_1$  is divisible by  $q$ . Further since  $a_1^2 - m$  is divisible by  $q^2$ , then necessarily  $m$  is divisible by  $q^2$ , which is contrary to the assumption that  $m$  must not contain an integer squared as a factor. (Art. 97.)

If 2 were a divisor of  $a, 2m, \frac{a_1^2 - m}{a}$ , then  $a_1^2 - m$  must be divisible by 4. Since however  $m \equiv 3 \pmod{4}$  or  $m = 4k + 3$ ,  $a_1$  must be an odd integer  $= 2g + 1$ , say. We must then have  $(2g + 1)^2 - 4k - 3$  divisible by 4, which is not true.

It follows that

$$\begin{aligned} aa' &= (i_2)^2(a) \left( a, a_1 + \sqrt{m}, a_1 - \sqrt{m}, 2a_1, 2m, \frac{a_1^2 - m}{a}, 1 \right) \\ &= (i_2)^2(a) = (ii_2). \end{aligned}$$

CASE II. When  $m \equiv 2 \pmod{4}$ ,  $\omega = \sqrt{m}$ ,  $\omega' = -\sqrt{m}$ . We then have as in the first case

$$\begin{aligned} (a, a_1 + \omega)(a, a_1 + \omega') &= a \left( a, a_1 + \omega', a_1 + \omega, \frac{a_1^2 - m}{a} \right) \\ &= a \left( a, 2m, \frac{a_1^2 - m}{a}, a_1 + \omega', a_1 + \omega \right). \end{aligned}$$

As above it is seen that  $a, 2m, \frac{a_1^2 - m}{a}$  have no common

divisor  $q > 2$ . If  $a, 2m, \frac{a_1^2 - m}{a}$  had 2 as a common factor,

then writing  $a = 2k$  ( $k$  an integer), it is seen that  $\frac{a_1^2 - m}{4k}$  must be integral. But as  $m$  is divisible by 2, it follows also that  $a_1^2$  must be divisible by 2, and therefore also by 4. We must then have  $m$  divisible by 4, which is *not* true. Hence, as above, it is seen that

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a).$$

CASE III. When

$$m \equiv 1 \pmod{4}, \quad \text{we have} \quad \omega = \frac{1 + \sqrt{m}}{2}, \quad \omega' = \frac{1 - \sqrt{m}}{2}.$$

In this case

$$\begin{aligned} &(a, a_1 + \omega)(a, a_1 + \omega') \\ &= \left( a^2, a(a_1 + \omega), a(a_1 + \omega'), \left( a_1 + \frac{1}{2} \right)^2 - \frac{m}{4} \right) \\ &= a \left( a, \frac{\left( a_1 + \frac{1}{2} \right)^2 - \frac{m}{4}}{a}, a_1 + \omega, a_1 + \omega', 2a_1 + 1, \sqrt{m}, m \right). \end{aligned}$$

Now if  $a, m, 2a_1 + 1$  contain a prime factor  $q$ , then is

$$\frac{\left( a_1 + \frac{1}{2} \right)^2 - \frac{m}{4}}{a} \text{ prime to } q, \text{ for since } \left( a_1 + \frac{1}{2} \right)^2 \text{ contains } q \text{ as}$$

a factor, and consequently  $q^2$ , we would necessarily have  $m$  divisible by  $q^2$ . It follows as in the two preceding cases that

$$(a, a_1 + \omega)(a, a_1 + \omega') = (a).$$

Note that the norm  $N(a) = i_2$  belongs to the rational integers of  $a$ . Further note that the norm of a product of ideals is equal to the product of their norms, for

$$\begin{aligned} N(a \cdot b \cdot c \cdots) &= a \cdot b \cdot c \cdots a' \cdot b' \cdot c' \cdots \\ &= N(a)N(b)N(c) \cdots \end{aligned}$$

ART. 210. THEOREM. *If  $\alpha$  is an arbitrary integer of  $\mathfrak{R}(\sqrt{m})$ , the complete system of representatives (Art. 209)*

with respect to  $\alpha$ , consists of  $|N(\alpha)|$  integers. For this number is the same as the number of representatives which constitute a complete system of residues taken with respect to the principal ideal  $(\alpha) = \mathfrak{a}$ , say. As basis of  $\mathfrak{a}$ , we may take  $\iota_1^* = \alpha$ , and  $\iota_2^* = \alpha\omega$ . Further writing  $\alpha = a + b\omega$ , it is seen when  $m \equiv 1 \pmod{4}$ , that

$$\iota_1^* = a + b\omega,$$

$$\iota_2^* = \frac{bm-1}{4} + (a+b)\omega, \quad \text{since} \quad \omega^2 = \frac{m-1}{4} + \omega.$$

It follows (Art. 209) that

$$N(\mathfrak{a}) = \left| a^2 + ab - \frac{m-1}{4}b^2 \right| = |N(\alpha)|.$$

In the second case, when  $m \not\equiv 1 \pmod{4}$ ,

$$\iota_1^* = a + b\omega,$$

$$\iota_2^* = bm + a\omega,$$

and as above, we have

$$N(\mathfrak{a}) = |a^2 - b^2m| = |N(\alpha)|.$$

### EXAMPLES

1. Let  $\alpha = x + iy$  be an integer of  $\mathfrak{R}(i)$  so that  $N(\alpha) = x^2 + y^2$ . Since in this realm Euclid's Algorithm for finding the greatest common divisor is applicable, all ideals are principal ideals. If  $\bar{\omega} = x + iy$  is a prime integer of  $\mathfrak{R}(i)$  that is *not* rational, then is  $N(\bar{\omega}) = x^2 + y^2 = \bar{\omega}\bar{\omega}'$  a rational prime integer in  $\mathfrak{R}$ , say  $p$  (Art. 240), and consequently the system of residues of  $\mathfrak{R}(i)$  with respect to  $\bar{\omega}$  consists of  $p$  integers. If, however, a rational prime integer in  $\mathfrak{R}(1)$ ,  $q$  say, is also prime in  $\mathfrak{R}(\sqrt{m})$ , then is  $N(q) = q \cdot q = q^2$ .

As an illustration take  $5 = (2+i)(2-i) = \bar{\omega} \cdot \bar{\omega}'$ , where  $\bar{\omega} = 2+i$ . The five representatives of the complete system of residues, mod.  $\bar{\omega}$ , are 0, 1, 2,  $i$ ,  $1+i$ . Every other integer of  $\mathfrak{R}(i)$  is congruent (mod.  $\alpha$ ) to one of these five integers, for example

$$2 \equiv -\sqrt{-1} \pmod{\bar{\omega}},$$

$$3 \equiv 1 \pmod{\bar{\omega}},$$

$$4 \equiv +1+i \pmod{\bar{\omega}},$$

etc. Similarly, since 3 is irreducible in  $\mathfrak{R}(i)$ , the nine integers 0, 1, 2,  $i$ ,  $2i$ ,  $1+i$ ,  $1+2i$ ,  $2+i$ ,  $2+2i$  constitute a complete system of incongruent residues (mod. 3). Show that this number is 13 in the case of  $2+3i$ .

2. In the realm  $\mathfrak{R}(\sqrt{-5})$ , it is seen that  $(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$  and the integers 0, 1, 2, constitute a complete system of residues with respect to the ideal  $(3, 1 + \sqrt{-5})$ . On the other hand 11 is irreducible in  $\mathfrak{R}(\sqrt{-5})$  and the integers  $a+ib$  consisting of the 121 combinations  $a=0, 1, 2, \dots, 10$ ;  $b=0, 1, 2, \dots, 10$  constitute a complete system of residues taken with respect to  $p = (11, 11\sqrt{-5})$ ,  $N(p)$  being 121.

ART. 211. THEOREM. *An ideal may have as factors only a finite number of ideals.* For let  $i = a \cdot b \cdot c \dots$ , then is  $N(i) = N(a)N(b)N(c) \dots$ , and the rational integer  $N(i)$  is divisible only by a finite number of rational integers. Of course, unit ideals are not counted.

It follows also that *there are only a finite number of ideals whose norms are less than a fixed rational integer.*<sup>1</sup> And this is equivalent to saying that there are only a finite number of different ideals<sup>2</sup> which contain as an element a given finite integer  $\alpha$ .

If an ideal is a divisor of a rational prime integer  $p$ , then  $p$  is a number belonging to this ideal and can be expressed therefore through the canonic form

$$(i, i_1 + i_2\omega).$$

Consequently since  $p$  may be added as an element of this ideal, it is evident that  $i = p$ , otherwise  $(i, p) = 1$  and the ideal reduces to a unit ideal.<sup>3</sup> Since  $i_2$  is a divisor of  $i$ ,

<sup>1</sup> When this ideal is in its canonical form, its norm  $= i_1 i_2$  and this product being less than a given integer restricts  $i_1$  and  $i_2$  and therefore the number of ideals in which these integers occur.

<sup>2</sup> For, observe that the norm of an element  $\alpha$  of an ideal is a rational integer that may be added as an element and therefore is divisible by  $i$ .

<sup>3</sup> If an element  $\alpha$  of an ideal divides 1, and is therefore a unit of the realm, then  $N(\alpha) = 1$  is an element of the ideal, which may accordingly be called a unit ideal. Further observe that the unit ideal (1) consists of all the integers of the fixed realm.

it is in this case either  $p$  or unity. In the latter case the ideal is of the form  $(p, i_1 + \omega)$  where  $i_1 < p$  but otherwise undetermined; in the first case the ideal is of the form  $(p, p\omega)$ , for  $i_1$  is divisible by  $i_2$  and may be neglected.

To the two cases  $(p, i_1 + \omega)$ ,  $(p, p\omega)$  correspond the norms  $p$  and  $p^2$ . In the first case the ideal is said to be one of the *first degree*, and in the second case it is said to be of the *second degree*. We thus have the theorem:

**THEOREM.** *The norm of an ideal, which is a divisor of a rational prime integer  $p$  is either  $p$  or  $p^2$ .*

#### EXAMPLES

1.  $\Re(\sqrt{-5})$ . Let  $i = (2, 1 + \sqrt{-5})$ ,  $i' = (2, 1 - \sqrt{-5})$ . Note that  $i = 2$ ,  $i_2 = 1$ , so that  $N(i) = 2$ . It is seen that

$$\begin{aligned} ii' &= (4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6) \\ &= (4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6, 2) = (2). \end{aligned}$$

If  $i = (3, 1 + \sqrt{-5})$ ,  $i' = (3, 1 - \sqrt{-5})$ , then is  $N(i) = 3 = ii'$ . If  $i = (21, 10 + \sqrt{-5})$ ,  $i' = (21, 10 - \sqrt{-5})$ , then  $N(i) = 21 = ii'$ .

2.  $\Re(\sqrt{-15})$ ,  $\omega = \frac{1 + \sqrt{-15}}{2}$ . Let  $i = (2, \omega)$ ,  $i' = (2, \omega')$ . It follows that  $N(i) = 2$ . It is further seen that

$$\begin{aligned} ii' &= \left(2, \frac{1 + \sqrt{-15}}{2}\right) \left(2, \frac{1 - \sqrt{-15}}{2}\right) \\ &= (4, 1 + \sqrt{-15}, 1 - \sqrt{-15}, 4) \\ &= (4, 1 + \sqrt{-15}, 1 - \sqrt{-15}, 4, 2) = (2), \end{aligned}$$

since  $\frac{1 \pm \sqrt{-15}}{2}$  are integers in this realm. If  $i = (17, 5 + \omega)$ , it is seen that  $N(i) = 17 = ii'$ .

3. Derive the complete system of incongruent residues of the preceding ideals.

#### THE UNIQUE FACTORIZATION OF IDEALS

**ART. 212.** If we define *prime ideals* as such that are different from unit ideals and which are divisible only





ART. 213. THEOREM. *If a product of two ideals  $a$  and  $b$  is divisible by a prime ideal  $\mathfrak{p}$ , and if  $b$  is not divisible by  $\mathfrak{p}$ , then  $a$  is divisible by  $\mathfrak{p}$ ; or if the product  $ab$  is divisible by  $\mathfrak{p}$ , then at least one of the factors  $a$  or  $b$  is divisible by  $\mathfrak{p}$ .* For write  $a$  and  $b$  as above, and put  $\mathfrak{p} = (\bar{\omega}_1, \bar{\omega}_2, \dots)$ . Since by hypothesis  $b$  is not divisible by  $\mathfrak{p}$ , the ideal  $(1) = (\beta_1, \beta_2, \dots, \bar{\omega}_1, \bar{\omega}_2, \dots)$  is a unit ideal, and it is possible to find a number  $\beta$  in  $b$  and a number  $\bar{\omega}$  in  $\mathfrak{p}$  such that  $1 = \beta + \bar{\omega}$ . It is also seen since  $ab \equiv 0 \pmod{\mathfrak{p}}$  that  $\mathfrak{p} = (\bar{\omega}_1, \bar{\omega}_2, \dots, ab)$  and therefore also  $\alpha_1\beta \equiv 0 \pmod{\mathfrak{p}}$ ,  $\alpha_2\beta \equiv 0 \pmod{\mathfrak{p}}$ ,  $\dots$ . Since  $\bar{\omega}$  is divisible by  $\mathfrak{p}$ , it follows that  $\alpha_1(\beta + \bar{\omega}) \equiv 0 \pmod{\mathfrak{p}}$ ,  $\alpha_2(\beta + \bar{\omega}) \equiv 0 \pmod{\mathfrak{p}}$ ,  $\dots$ ; or since  $\beta + \bar{\omega} = 1$ , it is evident that  $\alpha_1 \equiv 0 \pmod{\mathfrak{p}}$ ,  $\alpha_2 \equiv 0 \pmod{\mathfrak{p}}$ ,  $\dots$ , and consequently  $a$  is divisible by  $\mathfrak{p}$ .

ART. 214. THEOREM. *The factorization of ideals into their prime factors is unique.* Let  $\mathfrak{i}$  be a given ideal and suppose that  $\mathfrak{i} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_n$ , where  $\mathfrak{p}_1, \dots$  are prime ideals. If further  $\mathfrak{i} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \dots \cdot \mathfrak{q}_m$ , where  $\mathfrak{q}_1, \dots$  are prime ideals, it must follow that  $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_n = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \dots \cdot \mathfrak{q}_m$ . Of course, in this expression some of the  $\mathfrak{p}$ 's as well as of the  $\mathfrak{q}$ 's may be repeated. It is evident that  $\mathfrak{p}_1$  must divide the product on the right and is therefore either a divisor of  $\mathfrak{q}_1$  and is equal to  $\mathfrak{q}_1$ , or it is prime to  $\mathfrak{q}_1$  and then  $\mathfrak{p}_1$  must divide the product  $\mathfrak{q}_2 \cdot \dots \cdot \mathfrak{q}_m$ . In this case  $\mathfrak{p}_1$  must equal  $\mathfrak{q}_2$  or it must be a divisor of  $\mathfrak{q}_3 \cdot \dots \cdot \mathfrak{q}_m$ . Through repetition of this process it is seen that  $\mathfrak{p}_1$  must be equal to at least one of the quantities  $\mathfrak{q}$ . By dividing this common factor out, and by continuing the method of procedure, the theorem is proved. (Sommer, *loc. cit.*, p. 56.)

ART. 215. The following theorem offers a practical application of determining whether ideals are prime or not.

THEOREM. *Every prime ideal of the realm  $\mathfrak{R}(\sqrt{m})$  is*

always a factor of a rational prime integer  $p$ , or more exactly, of a rational principal ideal  $(p)$ . For if  $\mathfrak{p}$  is a prime ideal, then  $N(\mathfrak{p}) = \mathfrak{p} \cdot \mathfrak{p}' = g$ , where  $g$  is a rational integer. Denoting the prime factors of  $g$  by  $p_1, p_2, \dots$ , it is evident from the theorem above, since  $\mathfrak{p} \cdot \mathfrak{p}' = p_1 \cdot p_2 \cdot \dots$  that one of the factors  $p_1, p_2, \dots$  is divisible by  $\mathfrak{p}$ . Further, no two of these factors are divisible by  $\mathfrak{p}$ , for see Art. 211. In that case the two prime integers would occur as elements in the prime ideal  $\mathfrak{p}$ , and as their greatest common divisor is 1, the ideal would reduce to a unit ideal. If  $p$  is divisible by  $\mathfrak{p}$ , it follows also that  $p$  is divisible by  $\mathfrak{p}'$  and that  $\mathfrak{p}\mathfrak{p}' = p$ . It may be observed further that only those algebraic integers are divisible by  $\mathfrak{p}$  whose norms are divisible by  $p$ . For if  $\alpha$  is divisible by  $\mathfrak{p}$ , then  $\alpha$  may be adjoined as an element of  $\mathfrak{p}$ , as also the norm of  $\alpha$ . Since  $p$  is an element of this ideal, it is evident that unless  $N(\alpha)$  is divisible by  $p$ , the greatest common divisor of  $N(\alpha)$  and  $p$  would be unity, and the ideal  $\mathfrak{p}$  would become a unit ideal.

To determine the ideal prime factors of any ideal  $\mathfrak{a}$ , first form  $N(\mathfrak{a}) = g$ , say. Then distribute  $g$  into its rational integral prime factors, and finally those prime integers into their ideal prime factors. The fact that the norm of every element of an ideal is an element of the ideal and hence divisible by  $p$  must not be lost sight of. In the distribution of the rational prime integer  $p$  into its prime ideal factors, note that every principal ideal may be expressed through *one* number  $\alpha$ , say, in the form  $(\alpha)$ . And every ideal which is *not* a principal ideal may be expressed through two integers in the form  $(\alpha, \beta)$  where  $\alpha$  and  $\beta$  do *not* necessarily form a basis of the ideal. This is proved below in the form of a theorem.

LEMMA. *If  $\mathfrak{a}$  and  $\mathfrak{b}$  are two ideals that are different,*

there exists an integer  $\alpha$  of  $\mathfrak{a}$  such that the quotient  $\frac{(\alpha)}{\mathfrak{a}}$  is prime to  $\mathfrak{b}$ .<sup>1</sup>

If  $\mathfrak{b} = \mathfrak{p}$  is a prime ideal, the lemma is at once evident. For were  $\frac{(\alpha)}{\mathfrak{a}}$  divisible by  $\mathfrak{p}$  for every integer  $\alpha$  of  $\mathfrak{a}$ , it would follow that  $\mathfrak{a}$  was divisible by  $\mathfrak{a}\mathfrak{p}$ , which is *not* true.

For the general case let  $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$  be the different prime ideal factors of  $\mathfrak{b}$ , and form the ideals

$$\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r, \quad \mathfrak{a}_2 = \mathfrak{a}\mathfrak{p}_1\mathfrak{p}_3 \cdots \mathfrak{p}_r, \quad \dots, \quad \mathfrak{a}_r = \mathfrak{a}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{r-1}$$

and let respectively  $\alpha_i$  be integers of  $\mathfrak{a}_i$  such that  $\frac{(\alpha_i)}{\mathfrak{a}_i}$  are relatively prime to  $\mathfrak{p}_i (i=1, 2, \dots, r)$ . It follows that  $\alpha = \alpha_1 + \alpha_2 + \dots + \alpha_r$  is an integer as is required in the lemma.

**THEOREM.** *Every ideal  $\mathfrak{i}$  may be expressed in the form  $(\alpha, \beta)$ , where  $\mathfrak{i}$  is the greatest common ideal divisor of the integers  $\alpha$  and  $\beta$ . For choose any two integers  $\alpha$  and  $\beta$  of the ideal such that  $\frac{(\alpha)}{\mathfrak{i}}$  is relatively prime to  $\frac{(\beta)}{\mathfrak{i}}$ .*

Writing  $\left(\frac{(\alpha)}{\mathfrak{i}}, \frac{(\beta)}{\mathfrak{i}}\right) = 1$ , it follows that  $\mathfrak{i} = (\alpha, \beta)$ . In the factorization of  $p$  into ideal factors, since  $p$  occurs itself as one element in each such ideal factor, it is only necessary to determine the second element.

#### THE IDEAL FACTORS OF THE RATIONAL PRIME INTEGERS IN THE REALM $\mathfrak{R}(\sqrt{m})^2$

**ART. 216.** We saw (Art. 211) that a prime ideal which is a factor of a rational prime integer must have one or the other of the forms

$$(1) \quad \mathfrak{p} = (p, a + \omega),$$

<sup>1</sup> See Reid, *The Elements of the Theory of Algebraic Numbers*, p. 318.

<sup>2</sup> See Sommer, *Vorlesungen über Zahlentheorie*, p. 59.

or

$$(2) \quad \mathfrak{p} = (p, p\omega) = (p)(1, \omega) = (p).$$

In the first case  $(p) = \mathfrak{p}\mathfrak{p}'$  and consequently  $(p)$  may be factored into a product of two prime ideals; in the second case  $\mathfrak{p} = (p)$  and here  $p$  is not reducible.

A simple criterion may be derived by means of which it may be determined whether a prime integer is reducible into a product of two prime ideals as follows:

CASE I.  $m \equiv 3 \pmod{4}$ , discriminant  $d = 4m$ . Let  $p > 2$  be an arbitrary prime number, which is *not* a divisor of the discriminant  $d = 4m$ .

If  $p$  is factorable  $= (\mathfrak{p}\mathfrak{p}')$  in the realm  $\Re(\sqrt{m})$ , then is

$$\mathfrak{p} = (p, a + \sqrt{m}) = (p, a + \sqrt{m}, a^2 - m).$$

It follows that

$$a^2 - m \equiv 0 \pmod{p},$$

otherwise the ideal would be a unit ideal.

Reciprocally, if the congruence

$$x^2 - m \equiv 0 \pmod{p}$$

admits an integral rational solution  $x = a$ , then is  $p$  reducible, being the product of two prime ideals that are different from each other. For if  $x = a$  is a solution of this congruence but not of the congruence  $x^2 - m \equiv 0 \pmod{p^2}$ , then are  $\mathfrak{p} = (p, a + \sqrt{m})$  and  $\mathfrak{p}' = (p, a - \sqrt{m})$  two prime ideals that are divisors of  $p$ . These two ideals are different, since their greatest common divisor is

$$(p, a + \sqrt{m}, a - \sqrt{m}) = (p, a + \sqrt{m}, a - \sqrt{m}, 2a);$$

and as  $p$  and  $2a$  are relatively prime, this ideal reduces to a unit ideal.

The fact that  $x^2 - m \equiv 0 \pmod{p}$  has a solution  $x = a$ , which is *not* a solution of  $x^2 - m \equiv 0 \pmod{p^2}$ , is denoted in the theory of quadratic residues by the Legendre



symbol

$$\left(\frac{m}{p}\right) = 1.$$

If  $p > 2$ , the congruence  $x^2 - m \equiv 0 \pmod{p}$  admits a solution if  $y^2 - 4m \equiv 0 \pmod{p}$ , that is, if  $y^2 - d \equiv 0 \pmod{p}$ . For among the solutions of the latter congruence is evidently an even integer and consequently  $x = \frac{1}{2}y$  is a solution of the former congruence. Hence instead of writing  $\left(\frac{m}{p}\right) = 1$ , we may put  $\left(\frac{d}{p}\right) = 1$  as the condition that  $p$  be factorable. (See Sommer, *Vorlesungen*, p. 60.)

If  $x^2 - m \equiv 0 \pmod{p}$ , or, what is the same thing, if  $y^2 - d \equiv 0 \pmod{p}$  does *not* admit of an integral solution, then  $p$  is irreducible in the realm  $\Re(\sqrt{m})$  and  $(p)$  is itself a prime ideal. The fact that the congruence  $x^2 - d \equiv 0 \pmod{p}$  cannot be solved is represented through the symbol

$$\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1.$$

We must next consider the prime integers that are factors of the discriminant  $d = 4m$ , namely 2, and the odd simple factors of  $m$ . The congruence  $x^2 - m \equiv 0 \pmod{2}$  is satisfied by  $x = 1$  or  $x = -1$ , two solutions which are  $\pmod{2}$  equal. Hence as prime ideals we have

$$\mathfrak{p} = (2, 1 + \sqrt{m}) = \mathfrak{p}' = (2, 1 - \sqrt{m}).$$

Finally let  $p$  be an odd prime factor of  $m$ , which can be only of the first power, since  $m$  by hypothesis does *not* contain squared factors.

In this case the congruence

$$x^2 - m \equiv 0 \pmod{p}$$

admits the solution  $x = 0$  and  $p$  is divisible by

$$\mathfrak{p} = (p, \sqrt{m}) = \mathfrak{p}' = (p, -\sqrt{m}),$$

which ideals are different from unity and from  $p$ . We thus have

$$(p) = \mathfrak{p}^2.$$

It is seen that every prime integer that is a divisor of the discriminant  $d$ , is factorable, being the square of a prime ideal.

If  $p$  is a rational prime integer that is a divisor of  $d$ ; and that is, if the congruence  $y^2 - d \equiv 0 \pmod{p}$  has the solution  $y \equiv 0 \pmod{p}$  which is counted twice, then this fact is expressed through the symbol

$$\left(\frac{d}{p}\right) = 0.$$

EXAMPLES

1. Realm  $\mathfrak{R}(\sqrt{-5})$ ,  $2m = -5$ ,  $d = -20$ . It is seen that 2 and 5 are the only prime factors of 20, and consequently are factorable into the squares of prime ideals. In fact

$$(2) = (2, 1 + \sqrt{-5})^2, \quad (5) = (\sqrt{-5})^2.$$

The congruence  $x^2 + 5 \equiv 0 \pmod{p}$  admits solution for  $p = 3, 7, 23, \dots$ , but cannot be solved for  $p = 11, 13, 17, 19, \dots$ .

We thus have

$$\begin{aligned} (3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}), \\ (7) &= (7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5}), \\ (23) &= (23, 8 + \sqrt{-5})(23, 8 - \sqrt{-5}), \end{aligned}$$

while (11), (13), (17),  $\dots$  are prime ideals.

2. Realm  $\mathfrak{R}(\sqrt{35})$ ,  $m = 35$ ,  $d = 140$ . The prime integers which divide 140 are 2, 5, 7, and therefore

$$(2) = (2, 1 + \sqrt{35})^2, \quad (5) = (5, \sqrt{35})^2, \quad (7) = (7, \sqrt{35})^2.$$

The congruence  $x^2 - 35 \equiv 0 \pmod{p}$  admits solution for  $p = 13, 17, 19, \dots$ , but cannot be solved for  $p = 3, 11, \dots$ .

We therefore have

$$\begin{aligned} (13) &= (13, 3 + \sqrt{35})(13, 3 - \sqrt{35}), \\ (17) &= (17, 1 + \sqrt{35})(17, 1 - \sqrt{35}), \\ (19) &= (19, 4 + \sqrt{35})(19, 4 - \sqrt{35}), \end{aligned}$$

while (3), (11),  $\dots$  are prime ideals.

CASE II.  $m \equiv 2 \pmod{4}$ , discriminant  $d = 4m$ . It is seen here as in the first case that if  $p$  is a prime rational integer which is not a divisor of  $d$ , then  $p$  is reducible or irreducible in  $\Re(\sqrt{m})$  according as

$$\left(\frac{d}{p}\right) = 1 \quad \text{or} \quad \left(\frac{d}{p}\right) = -1.$$

If  $p = 2$ , then is

$$(2) = (2, \sqrt{m})^2 = \mathfrak{p}^2;$$

and for an odd prime integer that divides  $d$  or  $m$  it is also seen that

$$(p) = (p, \sqrt{m})^2 = \mathfrak{p}^2.$$

In both of these cases the congruence

$$x^2 - d \equiv 0 \pmod{p}$$

has the root  $x = 0$ , which is to be counted twice and as above we must write

$$\left(\frac{d}{p}\right) = 0.$$

EXAMPLE.  $\Re(\sqrt{10})$ ,  $4m = d = 40$ . The prime divisors of 40 are 2 and 5. It is seen that

$$\begin{aligned} (2) &= (2, \sqrt{10})^2, & (5) &= (5, \sqrt{10})^2, \\ (13) &= (13, 6 + \sqrt{10})(13, 6 - \sqrt{10}), \\ (7) &= (7), & (11) &= (11), \end{aligned}$$

etc.

CASE III.  $m \equiv 1 \pmod{4}$ ;  $d = m$ . Suppose first that  $p$  is an odd prime integer, such that  $(m, p) = 1$ . If  $p$  is reducible, it must have as a prime factor  $\mathfrak{p} = (p, a + \omega)$ ; and consequently

$$(a + \omega)(a + \omega') = \frac{(2a + 1)^2 - m}{4}$$

must be divisible by  $p$ , and therefore  $(2a + 1)^2 - m \equiv 0 \pmod{p}$  or  $x^2 - d \equiv 0 \pmod{p}$  must admit a solution.

We thus have as above  $\left(\frac{d}{p}\right) = 1$ .

It may be shown that  $\mathfrak{p} = (p, a + \omega)$  and  $\mathfrak{p}' = (p, a + \omega')$  are different, for it is seen that their greatest common divisor  $(p, a + \omega, a + \omega') = 1$ . It is further seen that  $\mathfrak{p}$  is not a unit ideal, nor is it equal to  $(p)$ .

Suppose next that  $p = 2$ . If 2 is divisible by the prime ideal  $\mathfrak{p} = (2, a + \omega)$ , then from above  $\frac{(2a+1)^2 - m}{4}$  must be an even integer and consequently  $(2a+1)^2 - m$  is divisible by 8. Hence if 2 is factorable, the congruence

$$(1) \quad x^2 - d \equiv 0 \pmod{8}$$

admits solution. This congruence may be solved if  $d \equiv 1 \pmod{8}$ , but cannot be solved if  $d \equiv 5 \pmod{8}$ .

And that is  $\left(\frac{d}{2}\right) = +1$ , if  $m \equiv 1 \pmod{8}$ ; and  $\left(\frac{d}{2}\right) = -1$ , if  $m \equiv 5 \pmod{8}$ .

When (1) admits a solution, it is seen that  $\mathfrak{p} = (2, a + \omega)$  and  $\mathfrak{p}' = (2, a + \omega')$  are different, and that neither of them is a unit ideal or  $= (2)$ .

Finally suppose that  $p$  is an odd prime integer which is a factor of  $m$ . Then as above  $\frac{(2a+1)^2 - m}{4}$  must be an integer that is divisible by  $p$  and therefore  $2a+1 \equiv 0 \pmod{p}$ . Since  $x^2 \equiv d \pmod{p}$  admits the double root  $x \equiv 0 \pmod{p}$ , we may again write  $\left(\frac{d}{p}\right) = 0$ . It is clear that  $\mathfrak{p} = (p, \sqrt{m})$ , and  $\mathfrak{p}' = (p, -\sqrt{m}) = \mathfrak{p}$  are two ideals such that  $\mathfrak{p} = \mathfrak{p}^2$ . If we put  $2a+1 = p$ , it is seen that

$$\mathfrak{p} = (p, a + \omega) = \left(p, \frac{p-1}{2} + \omega\right) = \mathfrak{p}'.$$

Observe that

$$\frac{p+1}{2} (2a+2\omega) - p(a+\omega) = a+\omega.$$

Hence,

$$(p, a + \omega) = \left( p, \frac{p+1}{2} (2a+2\omega) \right) = (p, 2a+2\omega),$$

since  $p$  and  $\frac{p+1}{2}$  are relatively prime. Since  $2a+1 \equiv 0 \pmod{p}$ , it follows that  $(p, 2a+2\omega) = (p, \sqrt{m})$ .

The three different cases considered above when expressed in compact form give expression to the following theorem:

**THEOREM.** *A rational prime integer  $p$  is reducible or irreducible in the realm  $\mathfrak{R}(\sqrt{m})$ , whose discriminant is  $d$ , being the product of two different prime ideals, the product of two equal prime ideals, or finally irreducible, according as*

$$\left(\frac{d}{p}\right) = 1, \quad \left(\frac{d}{p}\right) = 0, \quad \text{or} \quad \left(\frac{d}{p}\right) = -1.$$

It is thus seen that the problem of the resolution of a prime integer into its prime ideal factors in the realm  $\mathfrak{R}(\sqrt{m})$  reverts into the fundamental problem of quadratic residues, and that is, whether or not the congruence  $x^2 + m \equiv 0 \pmod{p}$ , or more generally whether the congruence  $x^2 + ax + b \equiv 0 \pmod{p}$  admits solution.<sup>1</sup>

### EXAMPLES

1. Find the three prime factors of the norm of  $(10 + \sqrt{-5})$  and therefrom the prime ideal factors of this number.

Find the product of  $\sqrt{-5}$ ,  $(3, 1 + \sqrt{-5})$ ,  $(7, 3 + \sqrt{-5})$ .

2. Prove that  $(3, 1 + \sqrt{-5})$  has four prime ideal factors and determine the product of  $(2, 1 + \sqrt{-5})$ ,  $(3, 1 + \sqrt{-5})$ ,  $(7, 3 + \sqrt{-5})$ ,  $(23, 8 + \sqrt{-5})$ .

### EQUIVALENCE OF IDEALS. CLASSES OF IDEALS

**ART. 217. DEFINITION.** *Two ideals  $a$  and  $b$  of the realm  $\mathfrak{R}(\sqrt{m})$  are said to be equivalent and written  $a \sim b$  if*

<sup>1</sup> It is of interest to read in this connection the article *Elementary Theorems Relating to Ideal Factors*. See Smith's Report, p. 108. See also *Report on Algebraic Numbers*, p. 17, by Dickson, etc.



their quotient is equal to a number of the realm; or if there are two integers  $\alpha, \beta$  in  $\mathfrak{R}(\sqrt{m})$  such that

$$\frac{a}{b} = \frac{\alpha}{\beta} \quad \text{or} \quad (\beta)a = (\alpha)b.$$

If  $a$  is a principal ideal, then this fact may be denoted by writing  $a \sim (1)$ .

From this definition follow at once the following theorems for equivalences:

THEOREM 1. If  $a \sim b$  and  $b \sim c$ , then is  $a \sim c$ .

THEOREM 2. If  $a \sim b$  and  $c \sim d$ , then is  $ac \sim bd$ .

THEOREM 3. If  $a$  and  $b$  are equivalent ideals and if  $c$  is a third ideal such that  $ac$  is a principal ideal, and that is,  $ac \sim (1)$ , then is also  $bc \sim (1)$ .

Kummer used this as the definition of *equivalence*. It has the same meaning as the definition first given, for if

$$ac \sim bc \sim (1),$$

then is

$$aN(c) \sim bN(c)$$

and therefore  $a \sim b$ .

THEOREM 4. If  $ac \sim bd$ , and if  $a \sim b$ , then is  $c \sim d$ ; for  $ac \sim bc \sim bd$ , and therefore  $c \sim d$ .

COROLLARY. If  $a \sim b$  then is also  $a' \sim b'$ ; for  $aa' \sim (1)$  and  $bb' \sim (1)$  and therefore  $aa' \sim bb'$  and  $a' \sim b'$ .

From this conception of equivalence follows the next definition.

DEFINITION. All ideals which are equivalent to one and the same ideal, form an ideal-class or class of ideals.

Accordingly every ideal determines an ideal-class, which class contains an indefinite number of ideals. All principal ideals are equivalent to the ideal  $(1)$  and taken collectively form the *principal class*  $K = 1$ .

The classes of a realm may be denoted by  $K, K_1, K_2,$

...

If the ideal  $a_i$  belongs to the class  $K_i$  and  $a_j$  to the class  $K_j$ , and if  $b = a_i a_j$  belongs to the class  $K_n$ , then  $K_n$  is called the *product of the classes*  $K_i$  and  $K_j$  and is symbolically written  $K_n = K_i K_j$ .

We may accordingly multiply the classes by one another, noting always the identity  $K_i = 1 \cdot K_i$ . Since to every ideal  $a_i$  there may be found a corresponding ideal  $\bar{a}_i$ , such that  $a_i \bar{a}_i$  is a principal ideal, *there is associated* with every class  $K_i$  always one and only one class  $\bar{K}_i$  such that  $K_i \bar{K}_i = 1 = K$ .

Two classes which stand in such a relation are called *reciprocal* and may be written  $K_i = \bar{K}_i^{-1}$  or  $\bar{K}_i = K_i^{-1}$ .

We may also introduce the *notion of division* into the process of computation of ideal-classes: An ideal-class  $K_n$  of the realm  $\mathfrak{R}(\sqrt{m})$  is said to be *divisible* by an ideal-class  $K_j$  of the same realm, if there is an ideal-class  $K_i$  in  $\mathfrak{R}(\sqrt{m})$  such that  $K_n = K_i K_j$ .

The exposition of ideal-classes thus defined renders possible the following:

**ART. 218. FUNDAMENTAL THEOREM.** *The number of ideal-classes of a quadratic realm is always finite.<sup>1</sup> There is in every ideal-class at least one ideal whose norm is less than  $|\sqrt{D}|$ ,  $D$  being the discriminant of the realm.*

The proof of this theorem depends upon the following lemma:

**LEMMA.** *In every ideal  $a$  of the realm  $\mathfrak{R}(\sqrt{m})$ , whose discriminant is  $D$ , there is always a number  $\alpha$  whose norm in absolute value  $\leq |N(\alpha)\sqrt{D}|$ .*

For suppose the ideal written in its canonical form  $a = (i, i_1 + i_2\omega)$ ; and in the case of a real realm write

$$\begin{aligned} f_1 &= ix \pm (i_1 + i_2\omega)y, \\ f_2 &= ix \pm (i_1 + i_2\omega')y. \end{aligned}$$

<sup>1</sup> See Smith's Report, p. 112.

In the case of an imaginary realm put

$$f_1 = \frac{1}{\sqrt{2}} \{2ix + (2i_1 + i_2[\omega + \omega'])y\},$$

$\omega + \omega'$  being real, and

$$f_2 = \frac{1}{\sqrt{-2}} \{0 \cdot x \pm i_2(\omega - \omega')y\},$$

which is a real quantity. Regarding the sign  $\pm$ , that sign is to be taken which gives the *positive* sign to

$$\Delta = ii_2 |\sqrt{D}| = |N(\alpha) \sqrt{D}|.$$

Further in the case of a real realm let  $k_1$  and  $k_2$  be any two real quantities such that  $k_1 k_2 = \Delta = |N(\alpha) \sqrt{D}|$ ; and in the case of an imaginary realm impose the additional condition that  $k_1 = k_2 = k$ .

It follows from the Minkowski Theorem that two rational integers  $x$  and  $y$  that are different from zero may be found such that  $|f_1| \leq k_1$ ,  $|f_2| \leq k_2$  (Art. 26).

In the case of the real realms, it is seen that  $\alpha = f_1$  is an integer of  $\mathfrak{a}$  such that

$$\begin{aligned} |\alpha| = |f_1| &= |ix \pm (i_1 + i_2 \omega)y| \leq k_1, \\ |\alpha'| = |f_2| &= |ix \pm (i_1 + i_2 \omega')y| \leq k_2. \end{aligned}$$

It follows that

$$|\alpha \alpha'| = |N(\alpha)| \leq k_1 k_2 \leq |N(\alpha) \sqrt{D}|.$$

In the case of imaginary realms, it is seen, if

$$\alpha = \frac{f_1 \pm \sqrt{-1} f_2}{\sqrt{2}} \quad \text{and} \quad \alpha' = \frac{f_1 \mp \sqrt{-1} f_2}{\sqrt{2}},$$

that

$$|N(\alpha)| = \frac{1}{2} |f_1^2 + f_2^2| \leq \frac{1}{2} (k_1^2 + k_2^2) \leq k^2 \leq |N(\alpha) \sqrt{D}|.$$

*Important Remark.* The theorem is also true for principal ideals  $\mathfrak{a} = (\alpha)$ . (See Art. 206.) As every number of this ideal is of the form  $\lambda \alpha$ , where  $\lambda$  is an integer in  $\mathfrak{R}(\sqrt{m})$ , it follows from the above theorem that there is an integer  $\lambda \alpha$ , say, such that

$$N(\lambda \alpha) \leq |N(\alpha) \sqrt{D}|;$$

and, since for principal ideals (Art. 210)  $N(\alpha) = N(a)$ , it is seen that there is always an integer of the realm,  $\lambda$ , say, such that

$$N(\lambda) \leq |\sqrt{D}|.$$

*Proof of the Fundamental Theorem.* Let  $a$  be an ideal of the class  $A$ , and let  $\alpha$  be a number of this ideal such that  $|N(\alpha)| \leq |N(a)\sqrt{D}|$ . Further there is in  $B$ , the reciprocal class of  $A$ , an ideal  $b$  such that  $a \cdot b = (\alpha)$ ; and consequently  $N(a)N(b) = N(\alpha) \leq |N(a)\sqrt{D}|$ . It follows that  $N(b) \leq |\sqrt{D}|$ . Thus it is seen that the class  $B$  contains an ideal  $b$  whose norm  $\leq |\sqrt{D}|$ . By interchanging the class  $B$  with the class  $A$ , it is seen that in the class  $A$  there is an ideal whose norm  $\leq |\sqrt{D}|$ .

Since  $|\sqrt{D}|$  is a finite number, and as there are only a finite number of ideals whose norm is less than a fixed number, it follows that the number of ideal-classes is finite. Cayley, *Works*, V, p. 141. See H. J. S. Smith, *Collected Works*, Vol. I, pp. 191 et seq.

This number of classes, which will be denoted by  $h$ , is one of the most important constants that occurs in the discussion of the realm  $\mathfrak{R}(\sqrt{m})$ .

ART. 219. The Theorem 3 of Art. 217 may be used to determine whether or not two ideals are equivalent.

#### EXAMPLES FOR THE EXAMINATION OF THE EQUIVALENCE OF IDEALS

1. In the realm  $\mathfrak{R}(\sqrt{-5})$  it is seen that

$$(2, 1 + \sqrt{-5}) \sim (3, 1 + \sqrt{-5}) \propto (1)$$

for multiplying by  $(3, 1 - \sqrt{-5})$ , we have

$$(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (3) \sim (1)$$

and

$$(2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (1 + \sqrt{-5}) \sim (1).$$

It is also seen that

$$(3, 1 + \sqrt{-5}) \sim (3, 1 - \sqrt{-5}) \quad \text{for} \quad (3, 1 + \sqrt{-5})^2 \sim (2 - \sqrt{-5}) \sim (1).$$

Observe that

$$(1 - \sqrt{-5})(3, 1 + \sqrt{-5}) = (1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

2. In the realm  $\mathfrak{R}(\sqrt{-23})$ ,  $\omega = \frac{1 + \sqrt{-23}}{2}$ ,  $(2, \omega) \asymp (2, \omega')$  for

$$(2, \omega)^2 = \left(4, 2\omega, \frac{-22 + 2\sqrt{-23}}{4}\right) = (4, 2\omega, -6 + \omega) = (4, 2 - \omega) \asymp (1),$$

while  $(2, \omega)(2, \omega') = (2) \sim 1$ . Observe that  $(3, \omega) \sim (2, \omega')$ . For  $(3, \omega)(2, \omega) = (6, 2\omega, 3\omega, \omega^2, \omega) = (6, \omega) = (\omega)$ , since  $\frac{6}{\omega} = \omega'$ .

3. In the realm  $\mathfrak{R}(\sqrt{31})$  it is seen that

$$(3, 1 + \sqrt{31}) \asymp (3, 1 - \sqrt{31});$$

for

$$(3, 1 + \sqrt{31})^2 = (9, 2 - \sqrt{31}) \asymp (1),$$

while

$$(3, 1 - \sqrt{31})(3, 1 + \sqrt{31}) = (3) \sim (1).$$

On the other hand

$$(3, 1 - \sqrt{31}) \sim (5, 1 - \sqrt{31}),$$

for

$$(3, 1 + \sqrt{31})(5, 1 - \sqrt{31}) = (4 + \sqrt{31}) \sim (1),$$

and also

$$(3, 1 + \sqrt{31}) \sim (5, 1 + \sqrt{31}).$$

### EXAMPLES FOR THE EXAMINATION OF THE NUMBER OF IDEAL CLASSES

1. For the realms  $\mathfrak{R}(i)$ ,  $\mathfrak{R}(\sqrt{-2})$ ,  $\mathfrak{R}(\sqrt{-3})$ , the Euclid method for finding the greatest common divisor is applicable and consequently in all these realms the ideals are principal ideals and in each case  $h = 1$ .

2. For the realm  $\mathfrak{R}(\sqrt{-5})$ ,  $m = -5 \equiv 3 \pmod{4}$ , so that  $D = -20$  and  $|\sqrt{D}| < 5$ . In this realm 2 and 3 are reducible and in fact

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = \mathfrak{p} \cdot \mathfrak{p}', \quad \mathfrak{p} = \mathfrak{p}', \quad N(\mathfrak{p}) = 2$$

$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = \mathfrak{p}_1 \cdot \mathfrak{p}'_1, \quad N(\mathfrak{p}_1) = 3.$$

Due to the fundamental theorem every ideal of  $\mathfrak{R}(\sqrt{-5})$  must be equivalent to at least one of the ideals  $(1)$ ,  $\mathfrak{p}$ ,  $\mathfrak{p}_1$  or  $\mathfrak{p}'_1$ , for these are all the ideals whose norms are less than  $|\sqrt{D}|$ . It was shown above (Ex. 1, above) that  $\mathfrak{p} \sim \mathfrak{p}_1 \sim \mathfrak{p}'_1 \asymp (1)$ , and consequently the number of



class-ideals is here  $h=2$ . The representatives of these two classes are (1) and  $(2, 1+\sqrt{-5})$ .

3. For the realm  $\mathfrak{R}(\sqrt{-23})$ , we have  $m \equiv 1 \pmod{4}$  and  $D = -23$ , so that  $|\sqrt{D}| < 5$ . The integers 2, 3, 4 are resolvable into factors that are not principal ideals. We have  $\omega = \frac{1+\sqrt{-23}}{2}$ ,  $\omega + \omega' = 1$ ,  $\omega^2 = \omega - 6$ ,

$$\begin{aligned} (2) &= (2, \omega)(2, \omega') = a \cdot a' & \text{and} & \quad N(a) = 2, \\ (3) &= (3, \omega)(3, \omega') = b \cdot b' & \text{and} & \quad N(b) = 3. \end{aligned}$$

It is seen that  $a^2 = (4, 2-\omega)$ ,  $a^3 = (8, 2-\omega) = (2-\omega) \sim (1)$ ;  $a' = (2, \omega') = (2, 1-\omega)$ ,  $a'^2 \sim a'$ ;  $b = (3, \omega)$ ,  $b^2 = (9, 6-\omega)$ ,  $b^2 a' = (18, 3+\omega) = (3+\omega) \sim (1)$ , so that  $b^2 \sim a$ ,  $a^2 \sim b \sim a'$ ;  $b^3 \sim a b \sim (1)$ . The representatives of these ideal classes are accordingly, (1),  $a$ ,  $a'$ ; or (1),  $a$ ,  $a^2$ ; or (1),  $b$ ,  $a$ .

4. For the realm  $R(\sqrt{31})$ ,  $m \equiv 3 \pmod{4}$ ;  $d = 124$  and  $|\sqrt{D}| < 12$ . Of the prime rational integers that are less than 12, it is seen that 2, 3, 5 are reducible, while 7 and 11 are irreducible. It is observed that

$$(2) = (39+7\sqrt{31})(39-7\sqrt{31}),$$

being the product of two principal ideals; while

$$\begin{aligned} (3) &= (3, 1+\sqrt{31})(3, 1-\sqrt{31}) = a \cdot a', & N(a) &= 3, \\ (5) &= (5, 1+\sqrt{31})(5, 1-\sqrt{31}) = b \cdot b', & N(b) &= 5. \end{aligned}$$

It was seen above that  $a$ ,  $a'$ ,  $b$ ,  $b'$  are not principal ideals and that  $a \sim b$ ,  $a' \sim b'$ . It may also be shown that  $a^2 = (9, -2+\sqrt{31})$ ,  $a^3 = (2-\sqrt{31})$ ,  $a^2 \sim a'$ .

The numbers 4, 6, 8, 9, 10 can therefore only lead to ideals that are equivalent to the ideals (1),  $a$ ,  $a^2$ , or 1,  $b$ ,  $b^2$ , or (1),  $a$ ,  $a'$ , so that  $h=3$ .

5. In the realm  $\mathfrak{R}(\sqrt{-5})$  show that  $h=2$ ; in  $\mathfrak{R}(\sqrt{7})$ ,  $h=1$ ; in  $\mathfrak{R}(\sqrt{-31})$ ,  $h=3$ ; in  $\mathfrak{R}(\sqrt{-43})$ ,  $h=1$ ; in  $\mathfrak{R}(\sqrt{13})$ ,  $h=1$ ; in  $\mathfrak{R}(\sqrt{82})$ ,  $h=4$ ; in  $\mathfrak{R}(\sqrt{-61})$ ,  $h=6$ .

To obtain all prime ideals whose norms are less than  $|\sqrt{D}|$  we have to solve the positive rational prime integers into their prime ideal factors. By multiplying these ideals together, we are able to obtain all those ideals whose norms are less than  $|\sqrt{D}|$ . Evidently this number is finite.

ART. 220. For practical purposes this above method of determining the number of ideal-classes is sufficient. There is, however, an analytic method for determining this number, a method which belongs to the "Analytic Theory of Numbers" and which is explained later (Vol. II, Chapt. IX). This theory was introduced by Dirichlet<sup>1</sup> and extended by Dedekind, Kronecker, and others.

The different powers of an ideal that is not a principal ideal, namely

$$a, a^2, a^3, \dots$$

are different ideals and determine correspondingly classes of ideals  $A, A^2, A^3, \dots$ . But since there is only a finite number of classes of ideals, the series  $A, A^2, A^3, \dots$  cannot extend indefinitely and represent different ideal-classes. If we call  $A^{a+h_1}$  the *first class* which is identical with a preceding class  $A^a$ , then is  $A^{a+h_1} = A^a$  and consequently  $A^{h_1} = 1$ . The following two assertions may be made:

1. The classes  $A, A^2, \dots, A^{h_1}$  are all different, while

$$A^{1+h_1} = A^1, \quad A^{2+h_1} = A^2,$$

etc.

2. The smallest exponent  $h_1$  for which  $A^{h_1} = 1 = K$  (Art. 217) is a *divisor* of the number of class-ideals  $h$ .

*Proof.* If the collectivity of classes is represented through  $A, A^2, \dots, A^{h_1}$ , then  $h = h_1$ , but if there is another class  $B$  that is different from any of these classes, then also  $AB, A^2B, \dots, A^{h_1}B$  are all ideal-classes different from one another and different from the classes first written. If this constitutes all the classes of the realm, then is  $h = 2h_1$ . If, however, there is another ideal-class  $C$  different from all the ideal-classes, just written, then

<sup>1</sup> *Collected Works*, Vol. I, pp. 357 and 411. See also Bachmann, *Zahlentheorie*, Vol. III.

also  $AC, A^2C, \dots, A^{h_1}C$  form again  $h_1$  new classes of ideals that are different from one another and different from all the ideal-classes hitherto introduced. By continuing this process it is seen that  $h = nh_1$ .

A direct consequence of this fact is the following theorem due to Hermite (*Oeuvres*, Paris, 1905, Vol. I, p. 274):

**THEOREM.** *If the quadratic form  $X^2 + mY^2$  is divisible by  $p$ , where  $p, X$ , and  $Y$  are rational integers and  $p$  a prime integer, then some power of  $p$ , say  $p^h$ , may be expressed in the form  $p^h = x^2 + my^2$  where  $x$  and  $y$  are rational integers. For it is evident that  $(X + i\sqrt{m}Y)(X - i\sqrt{m}Y)$  is divisible by  $p$ , and consequently  $p$  is factorable in the realm  $\mathfrak{R}(\sqrt{-m})$  into ideal factors, say  $\mathfrak{p}, \mathfrak{p}'$ , where  $\mathfrak{p} = (p, X + \sqrt{-m}Y), \mathfrak{p}' = (p, X - \sqrt{-m}Y), \mathfrak{p}\mathfrak{p}' = p$ . Further if  $A$  is the class to which  $\mathfrak{p}$  belongs, and  $A'$  the class to which  $\mathfrak{p}'$  belongs,  $A^h = 1$ ; and since  $x + i\sqrt{m}y$  is a number of the principal ideal, it follows that  $\mathfrak{p}^h = x + i\sqrt{m}y$ , if  $m \not\equiv 1 \pmod{4}$ ;  $\mathfrak{p}'^h = x - i\sqrt{m}y$ , and therefore  $p^h = x^2 + my^2$ . We further have  $\mathfrak{p}^h = t + \omega s$  if*

$$m \equiv 1 \pmod{4}; \quad p^h = \left(t + \frac{s}{2}\right)^2 + \frac{m}{4} \cdot s^2; \quad 4p^h = (2t + s)^2 + ms^2.$$

Hence  $s$  is an even integer.

**ART. 221. The Function**  $\Phi(a)$ . In the theory of rational numbers it is asked to determine the number  $\varphi(n)$  of all integers that constitute a complete system of residues with respect to  $n$  and which are relatively prime to  $n$ .

In a corresponding manner, if  $\mathfrak{a}$  is an arbitrary ideal of the realm  $\mathfrak{R}(\sqrt{m})$ , it is required to determine the number of all the integers of  $\mathfrak{R}(\sqrt{m})$  that constitute a complete system of residues with respect to  $\mathfrak{a}$  and which are

<sup>1</sup> See Dickson's *History*, Chapt. V; Euler's  $\varphi$ -function, etc.

relatively prime to  $\mathfrak{a}$ . The prime factors of  $\mathfrak{a}$  are supposed known. The number in question is denoted by  $\Phi(\mathfrak{a})$ , where for the unit ideal  $\mathfrak{a} = (1)$ ,  $\Phi(\mathfrak{a}) = 1$ .

First let  $\mathfrak{a} = \mathfrak{p}$  be a prime ideal of the *first degree* so that  $\mathfrak{p} = (p, a + \omega)$ . The number of integers of a complete system of residues with respect to  $\mathfrak{p}$  are represented through the  $N(\mathfrak{p})$  integers  $0, 1, 2, \dots, p-1$ . For let  $b + c\omega$  be any integer in  $\mathfrak{R}(\sqrt{m})$ . Note that

$$b + c\omega = c(a + \omega) + pg + r,$$

where  $g$  is a rational integer and  $r$  one of the integers  $0, 1, 2, \dots, p-1$ . And that is  $b + c\omega \equiv r \pmod{\mathfrak{p}}$ . Of these integers only  $0$  is *not* prime to  $p$ . Hence for this case

$$\Phi(\mathfrak{p}) = N(\mathfrak{p}) - 1 = N(\mathfrak{p}) \left[ 1 - \frac{1}{N(\mathfrak{p})} \right].$$

Consider next the powers of  $\mathfrak{p} = (p, a_1 + \omega)$  and observe that  $\mathfrak{p}^2$  must be equal to  $(p^2, a_2 + \omega)$ , when reduced to its cononical form, since  $N(\mathfrak{p}^2) = p^2$ . With respect to  $\mathfrak{p}^2$  as a modulus it is seen that any integer

$$A + B\omega = B(a_2 + \omega) + gp^2 + r, \quad \text{where } r < p^2.$$

Giving to  $r$  the values  $1, 2, \dots, p, p+1, \dots, 2p, \dots, p \cdot p$ , it is seen that there are  $p^2 - p$  classes of incongruent (mod.  $\mathfrak{p}^2$ ) integers that are relatively prime to  $\mathfrak{p}$ , so that

$$\Phi(\mathfrak{p}^2) = N(\mathfrak{p}^2) \left[ 1 - \frac{1}{N(\mathfrak{p})} \right].$$

Similarly, since  $\mathfrak{p}^3 = (p^3, a_3 + \omega)$ , we have

$$\Phi(\mathfrak{p}^3) = N(\mathfrak{p}^3) \left[ 1 - \frac{1}{N(\mathfrak{p})} \right],$$

etc.

Secondly let  $\mathfrak{p}$  be a prime ideal of the *second degree*  $\mathfrak{p} = (p, p\omega) = (p)$ . In this case the numbers of a complete system of residues are had through  $r + s\omega$ , where  $r, s$  take all values  $0, 1, 2, \dots, p-1$ . Among these numbers there

is only one, namely 0, which is not relatively prime to  $\mathfrak{p}$ , and we again have

$$\Phi(\mathfrak{p}) = N(\mathfrak{p}) - 1 = N(\mathfrak{p}) \left[ 1 - \frac{1}{N(\mathfrak{p})} \right].$$

We further have

$$\mathfrak{p}^k = (p^k, p^k \omega^k) = (p^k).$$

The numbers  $r + s\omega$  form a complete system of residues with respect to  $p^k$ , if for  $r, s$  the numbers  $0, 1, 2, \dots, p, p+1, \dots, p^k$  are substituted. This gives  $p^{2k} = N(\mathfrak{p}^k)$  combinations, and among these numbers there are values of  $r, s$  found in the series  $1p, 2p, 3p, \dots, p^{k-1} \cdot p$  making  $p^{2(k-1)}$  numbers that are not prime to  $p^k$ . Here again it is seen that

$$\Phi(\mathfrak{p}^k) = N(\mathfrak{p}^k) - N(\mathfrak{p}^{k-1}) = N(\mathfrak{p}^k) \left[ 1 - \frac{1}{N(\mathfrak{p})} \right].$$

To prove the theorem in general, assume that  $\Phi(\mathfrak{a})$  is determined for the case that  $\mathfrak{a} = \mathfrak{p}_1^{k_1} \mathfrak{p}_2^{k_2} \dots \mathfrak{p}_n^{k_n}$  where there are  $n$  different prime factors of  $\mathfrak{a}$ , and seek to determine  $\Phi(\mathfrak{a}_1)$  where  $\mathfrak{a}_1 = \mathfrak{p}^k \mathfrak{p}_1^{k_1} \mathfrak{p}_2^{k_2} \dots \mathfrak{p}_n^{k_n}$ , there being an additional prime factor other than  $\mathfrak{a}$  has, and which is prime to  $\mathfrak{a}$ .

When brought to their normal forms, let

$$\begin{aligned} \mathfrak{a} &= (a, a_1 + a_2 \omega), \\ \mathfrak{p}^k &= (\bar{i}, i_1 + i_2 \omega), \end{aligned}$$

and

$$\mathfrak{a}\mathfrak{p}^k = (ai, \bar{a} + a_2 i_2 \omega),$$

the norm of the last expression being  $ai\bar{a}i_2\bar{i}_2 = N(\mathfrak{a})N(\mathfrak{p}^k)$ .

The integers  $r + s\omega$  which form a complete system of residues with respect to  $\mathfrak{a}$ , are had by giving to  $r$  the values  $1, 2, \dots, a$ , and to  $s$  the values  $1, 2, \dots, a_2$ . The integers  $\bar{r} + \bar{s}\omega$  which form a complete system of residues with respect to  $\mathfrak{a}_1$  are had by giving to  $\bar{r}$  the values  $1, 2, \dots, ai$ , and to  $\bar{s}$  the values  $1, 2, \dots, a_2 i_2$ . Among the latter system of integers are the  $\bar{i}_2 \Phi(\mathfrak{a})$  integers which



are relatively prime to  $a$  as is seen by writing the numbers that constitute  $\bar{r}$  in the form  $1, 2, 3, \dots, 1a, a+1, a+2, \dots, 2a, 2a+1, \dots, ia$  and the numbers that constitute  $\bar{s}$  in the form  $1, 2, 3, \dots, 1a_2, a_2+1, a_2+2, \dots, 2a_2, 2a_2+1, \dots, ia_2$ .

Among these  $ai \cdot a_2i_2 = ii_2\Phi(a) = N(p^k)\Phi(a)$  numbers are some which contain  $p$  as a factor. The number of these integers may be computed if we observe the system of residues with respect to  $a_1$  that are relatively prime to  $a$  and which are divisible by  $p$ . This number is the number of the residues with respect to  $\frac{a_1}{p} = ap^{k-1}$  which are relatively prime to  $a$  and this number we have just seen is  $\Phi(a)N(p^{k-1})$ .

It follows that

$$\begin{aligned} \Phi(a_1) &= N(p^k)\Phi(a) - N(p^{k-1})\Phi(a) \\ &= \Phi(a)N(p^k) \left[ 1 - \frac{1}{N(p)} \right]. \end{aligned}$$

Applying this recursion formula in general to the ideal  $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ , it is seen that

$$\Phi(a) = N(a) \left[ 1 - \frac{1}{N(p_1)} \right] \left[ 1 - \frac{1}{N(p_2)} \right] \dots \left[ 1 - \frac{1}{N(p_n)} \right].$$

**THEOREM.** *If the ideal  $c$  is the product of the two ideals  $a$  and  $b$  which are relatively prime to each other, then is*

$$\Phi(c) = \Phi(a)\Phi(b).$$

For if

$$c = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} q_1^{l_1} q_2^{l_2} \dots q_m^{l_m},$$

then is

$$\begin{aligned} \Phi(c) &= N(p_1^{k_1} \dots p_n^{k_n}) N(q_1^{l_1} \dots q_m^{l_m}) \\ &\times \left[ 1 - \frac{1}{N(p_1)} \right] \dots \left[ 1 - \frac{1}{N(p_n)} \right] \left[ 1 - \frac{1}{N(q_1)} \right] \dots \left[ 1 - \frac{1}{N(q_m)} \right] \\ &= \Phi(a)\Phi(b). \end{aligned}$$



where  $\sigma_1, \dots, \sigma_\nu$  are again numbers of the same complete system of residues with respect to  $a$ . For no two of these numbers can be congruent.

If, for example,  $\sigma_\lambda \equiv \sigma_\mu \pmod{a}$ , then also  $\alpha(\rho_\lambda - \rho_\mu) \equiv 0 \pmod{a}$ , and as  $\alpha$  is relatively prime to  $a$ , we would have (Art. 213)  $\rho_\lambda \equiv \rho_\mu \pmod{a}$  which is contrary to the hypothesis.

Further, none of the ideals  $(\sigma_\lambda)$  can have a factor  $t$  in common with  $a$ . For it would follow that  $\rho_\lambda \alpha$  contains  $t$  as a factor, and since  $\alpha$  and  $a$  are relatively prime, it would follow that  $\rho_\lambda$  is divisible by  $t$ , which is contrary to the nature of  $\rho_\lambda$ .

It follows that  $\sigma_1, \sigma_2, \dots, \sigma_\nu$  are a complete system of residues with respect to  $a$  which are relatively prime to  $a$ , and consequently, neglecting the sequence, must be the same as the series of numbers  $\rho_1, \rho_2, \dots, \rho_\nu$ .

It results from the multiplication of the above congruences that

$$\rho_1 \rho_2 \cdots \rho_\nu \alpha^{\Phi(a)} \equiv \sigma_1 \cdot \sigma_2 \cdots \sigma_\nu \pmod{a},$$

or

$$\alpha^{\Phi(a)} \equiv 1 \pmod{a}.$$

COROLLARY I. If  $\alpha$  is an algebraic integer in  $\mathfrak{R}(\sqrt{m})$  that is not divisible by the prime ideal  $\mathfrak{p}$  of degree  $f$  ( $= 1$ , or  $2$ ), then is

$$\alpha^{p^f - 1} \equiv 1 \pmod{\mathfrak{p}}.$$

In other words the congruence

$$\alpha^{p^f} \equiv \alpha \pmod{\mathfrak{p}}$$

is true for any arbitrary integer  $\alpha$ .

COROLLARY II. If  $\alpha$  is an integer that is not divisible by the prime ideal  $\mathfrak{p}$  of degree  $f$ , and if  $e$  is the smallest rational integer for which

$$\alpha^e \equiv 1 \pmod{\mathfrak{p}},$$

then  $e$  is a divisor of  $p^f - 1$ .

For suppose that  $e$  is not a divisor of  $p^f - 1$ , and that the greatest common divisor of  $p^f - 1$  and  $e$  is  $e_1 < e$ . Then it is always possible to find two rational integers  $x$  and  $y$  such that

$$ex + (p^f - 1)y = e_1;$$

and since

$$\alpha^{ex} \equiv 1 \pmod{\mathfrak{p}} \quad \text{and} \quad \alpha^{(p^f - 1)y} \equiv 1 \pmod{\mathfrak{p}},$$

it also follows that

$$\alpha^{ex + (p^f - 1)y} \equiv 1 \pmod{\mathfrak{p}},$$

or

$$\alpha^{e_1} \equiv 1 \pmod{\mathfrak{p}},$$

where  $e_1 < e$  contrary to the postulate of the corollary. It follows that  $e$  must itself be a divisor of  $p^f - 1$ .

**COROLLARY III.** For an arbitrary  $k$ th power of  $\mathfrak{p}$ , the following congruence exists:

$$\alpha^{p^{fk} - 1} \equiv 1 \pmod{\mathfrak{p}^k}.$$

**ART. 223. General Congruences.** An integral function of one variable  $\xi$  of degree  $g$  with integral coefficients that belong to the realm  $\mathfrak{R}(\sqrt{m})$  may be considered with respect to an ideal-modulus  $\mathfrak{a}$ . A congruence with one unknown  $\xi$  is of degree  $g$ , if the coefficient of the highest term  $\xi^g$  is *not* divisible by  $\mathfrak{a}$ .

If the congruence

$$\alpha \xi^g + \alpha_1 \xi^{g-1} + \alpha_2 \xi^{g-2} + \cdots + \alpha_g \equiv 0 \pmod{\mathfrak{a}}$$

is given, where  $\alpha, \alpha_1, \cdots, \alpha_g$  are integral coefficients, one of the fundamental problems is:

Determine integers  $\rho$  in  $\mathfrak{R}(\sqrt{m})$  such that  $\xi = \rho$  satisfy the congruence. If  $\rho$  is such an integer, it is called a *root* of the congruence.

The simplest cases are for prime ideals for which the following fundamental theorem is true:

**THEOREM.** A congruence of the  $g$ th degree with respect to the prime ideal  $\mathfrak{p}$  as a modulus, in which the coefficient  $\alpha$

of the highest term is prime to  $\mathfrak{p}$ ,

$$f(\xi) = \alpha\xi^g + \alpha_1\xi^{g-1} + \cdots + \alpha_g \equiv 0 \pmod{\mathfrak{p}},$$

can have at most  $g$  roots incongruent with respect to  $\mathfrak{p}$ . (Cf. Lagrange, *Hist. Ac. Berlin*, 1768, p. 192).

*Proof.* If  $\rho_1$  is a root of the congruence, then is

$$f(\rho_1) \equiv 0 \pmod{\mathfrak{p}}$$

and

$$f(\xi) \equiv f(\xi) - f(\rho_1) = (\xi - \rho_1)f_1(\xi) \equiv 0 \pmod{\mathfrak{p}},$$

where  $f_1$  is of degree  $g-1$ . If further  $\rho_2, \dots, \rho_g$  are other roots, then is

$$f(\xi) = \alpha(\xi - \rho_1)(\xi - \rho_2) \cdots (\xi - \rho_g) \equiv 0 \pmod{\mathfrak{p}}.$$

For integers  $\xi$  this congruence can only be satisfied if  $\mathfrak{p}$  divides one of the factors, and that is if  $\xi - \rho_\mu \equiv 0 \pmod{\mathfrak{p}}$ , which proves the assertion. (See Art. 197).

**ART. 224. Primitive Numbers with Respect to a Prime-Ideal.** (Cf. Gauss, *Disq. Arith.*, Arts. 52-55).

Let  $\alpha$  be an integer of  $\mathfrak{R}(\sqrt{m})$  that is not divisible by the prime ideal  $\mathfrak{p}$  of degree  $f(=1, \text{ or } 2)$ ; for example a number of the complete system of residues with respect to  $\mathfrak{p}$ . It was seen above that there is always a divisor  $e$  of the number  $p^f - 1$  for which the congruence

$$\alpha^e \equiv 1 \pmod{\mathfrak{p}}$$

is satisfied.

If  $e$  is the smallest exponent which satisfies this congruence, the numbers  $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{e-1}$  are all different with respect to the modulus  $\mathfrak{p}$ .

For if there were two different integers  $e_1$  and  $e_2$  of the series  $1, 2, \dots, e-1$  for which the congruence

$$\alpha^{e_1} \equiv \alpha^{e_2} \pmod{\mathfrak{p}}$$

were true, then also

$$\alpha^{e_2}(\alpha^{e_1 - e_2} - 1) \equiv 0 \pmod{\mathfrak{p}},$$

and since  $\alpha^{e_2}$  is prime to  $\mathfrak{p}$ , it would necessarily follow that



the congruence

$$\alpha^{e_1 - e_2} \equiv 1 \pmod{\mathfrak{p}}$$

was true contrary to the hypothesis that  $e$  is the lowest exponent for which such a congruence exists.

If  $e$  is the smallest rational integer for which the congruence

$$\alpha^e \equiv 1 \pmod{\mathfrak{p}}$$

is true,  $\alpha$  is said to *belong to the exponent  $e$  with respect to  $\mathfrak{p}$* .

A number  $\bar{\omega}$  of the realm which belongs to the exponent  $p^f - 1$ , that is, where  $e = p^f - 1$  is the smallest exponent for which

$$\alpha^e \equiv 1 \pmod{\mathfrak{p}},$$

is called a *primitive* number with respect to  $\mathfrak{p}$ . (See Smith's *Report*, p. 49).

The series  $\bar{\omega}, \bar{\omega}^2, \bar{\omega}^3, \dots, \bar{\omega}^{p^f-1}$  present different  $(\text{mod. } \mathfrak{p})$  numbers of the realm  $\mathfrak{R}(\sqrt[m]{m})$  which are prime to  $\mathfrak{p}$ ; that is, they constitute a complete system of residues  $(\text{mod. } \mathfrak{p})$  which are relatively prime to  $\mathfrak{p}$ .

That this definition has a real meaning is seen in the fact that there *exist* such primitive numbers. To prove this, application may be made of a theorem which is a generalization of one that is due to Gauss.

**THEOREM.** *If  $e$  is a rational prime factor of  $p^f - 1$  and  $\mathfrak{p}$  is a prime ideal of degree  $f$  which is a divisor of the rational prime  $p$ , then there are in a complete system of residues with respect to  $\mathfrak{p}$  always  $\varphi(e)$  numbers that belong to the exponent  $e$ .*

*Proof.* It will be proved first that if there is a number  $\alpha$  which belongs to the exponent  $e$  (a divisor of  $p^f - 1$ ), then there are at least, but *not more* than,  $\varphi(e)$  incongruent numbers of the realm with respect to  $\mathfrak{p}$ , which belong to the exponent  $e$ . For, if  $r$  is a number of the series  $1, 2, \dots, e-1$ , that is relatively prime to  $e$ , then

$\alpha^r$  must also belong to the exponent  $e$ , and cannot belong to a lower exponent.

For if  $\alpha$  belongs to the exponent  $e$ , it follows that

$$\alpha^{er} \equiv 1 \pmod{\mathfrak{p}} \quad \text{or} \quad (\alpha^r)^e \equiv 1 \pmod{\mathfrak{p}}.$$

Since further  $r$  is prime to  $e$ , the congruence

$$\alpha^{re_1} \equiv 1 \pmod{\mathfrak{p}}$$

can exist only if  $re_1 \equiv 0 \pmod{e}$  or  $e_1 \equiv 0 \pmod{e}$  (cf. Art. 222). If we write instead of  $r$  those numbers  $r_1, r_2, \dots, r_\nu$  of the series  $1, 2, \dots, e-1$ , which are prime to  $e$ , we have  $\varphi(e)$  different numbers which belong to the exponent  $e$ , since, as seen above, the numbers  $\alpha, \alpha^2, \dots, \alpha^e$  are all incongruent  $\pmod{\mathfrak{p}}$ . Those powers  $\alpha^s$ , whose exponents  $s$  have a common factor  $d$  with  $e$  belong to the exponent  $\frac{e}{d} = e' < e$ .

Besides the numbers given above, there are no others which belong to the exponent  $e$ . For such numbers must satisfy the congruence

$$\xi^e \equiv 1 \pmod{\mathfrak{p}};$$

and from a theorem above, this congruence is satisfied at most by  $e$  integers that are incongruent  $\pmod{\mathfrak{p}}$ .

We have thus proved the lemma: *if there is a number  $\alpha$  which belongs to the exponent  $e$ , where  $e$  is a divisor of  $p^f - 1$ , then there are  $\varphi(e)$  such numbers.*

We may now prove the assertion: *there exist primitive numbers with respect to the prime ideal  $\mathfrak{p}$ .* For of the  $p^f - 1$  incongruent  $\pmod{\mathfrak{p}}$  numbers of a complete system of residues with respect to  $\mathfrak{p}$ , each one must belong to a definite divisor of  $p^f - 1$ .

If then  $t_1, t_2, \dots, t_m$  are the divisors of  $p^f - 1$  to which there belong numbers of the system of residues just mentioned, we must have:

$$\varphi(t_1) + \varphi(t_2) + \dots + \varphi(t_m) = p^f - 1 = N(\mathfrak{p}) - 1.$$

On the other hand we have seen that  $\sum \varphi(t) = N(\mathfrak{p}) - 1$  where  $t$  goes through *all* the divisors of  $p^f - 1$  including  $p^f - 1$ .

It follows that there exist numbers that belong to the exponent  $p^f - 1$ , and in fact  $\varphi(p^f - 1)$  such numbers, which are all incongruent (mod.  $\mathfrak{p}$ ).

**ART. 225. Wilson's Theorem.** *If  $\rho_1, \rho_2, \dots, \rho_v$  are the incongruent numbers of a complete system of residues with respect to a prime ideal  $\mathfrak{p}$ , that is not a divisor of 2, then is  $\rho_1 \cdot \rho_2 \cdot \dots \cdot \rho_v \equiv -1 \pmod{\mathfrak{p}}$ .*

For let  $\tilde{\omega}$  be a primitive number with respect to  $\mathfrak{p}$ . We may then write

$$\begin{aligned} \rho_1 &\equiv \tilde{\omega}^{e_1} \pmod{\mathfrak{p}}, \\ &\cdot \\ &\cdot \\ &\cdot \\ \rho_v &\equiv \tilde{\omega}^{e_v} \pmod{\mathfrak{p}}, \end{aligned}$$

where  $e_1, e_2, \dots, e_v$  are, neglecting the sequence, the same as the numbers  $1, 2, \dots, N(\mathfrak{p}) - 1$ .

It follows that

$$\rho_1 \rho_2 \cdot \dots \cdot \rho_v \equiv \tilde{\omega}^{\frac{N(\mathfrak{p})-1}{2} N(\mathfrak{p})} \pmod{\mathfrak{p}}.$$

Further since any integer  $\alpha$ , say, satisfies the congruence

$$\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$$

or

$$\left(\alpha^{\frac{N(\mathfrak{p})-1}{2}} - 1\right) \left(\alpha^{\frac{N(\mathfrak{p})-1}{2}} + 1\right) \equiv 0 \pmod{\mathfrak{p}},$$

it is seen that the one or the other of these factors  $\equiv 0 \pmod{\mathfrak{p}}$ ; and when we write  $\tilde{\omega}$  a *primitive number* instead of  $\alpha$ , it is seen that

$$\tilde{\omega}^{\frac{N(\mathfrak{p})-1}{2}} + 1 \equiv 0 \pmod{\mathfrak{p}},$$

since  $N(\mathfrak{p}) - 1$  is the lowest exponent such that

$$\tilde{\omega}^{N(\mathfrak{p})-1} \equiv +1 \pmod{\mathfrak{p}}.$$

By means of the Wilson Theorem it may be determined

in which cases the congruence

$$\xi^2 \equiv -1 \pmod{\mathfrak{p}},$$

$\mathfrak{p}$  being any prime ideal that does not divide 2, admits solution through integers of the realm  $\Re(\sqrt{m})$ .

It is evident that in the realm  $\Re(\sqrt{-1})$  the congruence may be solved, and therefore in the following we may neglect this realm.

1. Suppose that  $\mathfrak{p}$  is a prime ideal of the first degree, and accordingly that  $1, 2, \dots, p-1$  or  $-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -2, -1, +1, +2, \dots, \frac{p-3}{2}, \frac{p-1}{2}$  constitute a system of incongruent numbers.

It is then seen that

$$\rho_1 \cdot \rho_2 \cdots \rho_\nu = (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)^2 = (-1)^{\frac{p-1}{2}} \mu^2;$$

and consequently that

$$(-1)^{\frac{p-1}{2}} \mu^2 \equiv -1 \pmod{\mathfrak{p}}.$$

Hence the number  $\mu$  is a solution of the congruence

$$\xi^2 \equiv -1 \pmod{\mathfrak{p}},$$

when and only when

$$p-1 \equiv 0 \pmod{4}.$$

2. Suppose next that  $\mathfrak{p}$  is a prime ideal of the second degree. In this case the numbers  $r+s\omega$  for

$$r, s = -\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -2, -1, 1, 2, \dots, \frac{p-1}{2}$$

together with the numbers

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}$$

and

$$-\frac{p-1}{2}\omega, -\frac{p-3}{2}\omega, \dots, -\omega, \omega, \dots, \frac{p-1}{2}\omega$$

form a complete system of incongruent numbers (mod.  $p$ ).

It follows that

$$\rho_1 \cdot \rho_2 \cdots \rho_\nu = (-1)^{p-1+\left(\frac{p-1}{2}\right)^2} \times \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)^4 \omega^{p-1} \prod (r_1 + s_1 \omega)^2,$$

where  $r_1$  runs from 1 to  $\frac{p-1}{2}$ , and  $s_1$  runs from  $-\frac{p-1}{2}$  to  $+\frac{p-1}{2}$ . Writing  $\frac{(p-1)^2}{2} + p - 1$  in the form  $(p-1)\left(1 + \frac{p-1}{2}\right)$ , it is seen that this product is an even integer and consequently

$$\rho_1 \cdot \rho_2 \cdots \rho_\nu = \mu^2 \equiv -1 \pmod{p}.$$

It follows that the congruence

$$\xi^2 \equiv -1 \pmod{p}$$

is in an arbitrary realm *always* solvable for a prime modul  $p$  of the second degree.

**ART. 226. Linear Congruences with Respect to Ideals.**

*In the case of the linear congruence*

$$\alpha \xi \equiv \beta \pmod{i}$$

*the question is: under what condition can such a congruence be solved through an integer of the realm?*

FIRST CASE. Let the ideal  $(\alpha)$  and the ideal  $i$  be prime to each other. If then for  $\xi$  all numbers  $\rho$  of a complete system of residues with respect to  $i$  are written  $\alpha\rho_1, \alpha\rho_2, \dots, \alpha\rho_\nu$ , these numbers must again form a complete system of residues; for if

$$\alpha\rho_s \equiv \alpha\rho_t \pmod{i},$$

then is

$$\alpha(\rho_s - \rho_t) \equiv 0 \pmod{i}.$$

And, since  $\alpha$  is relatively prime to  $(i)$ , it would follow that

$$\rho_s \equiv \rho_t \pmod{i},$$

contrary to the hypothesis.



The integer  $\beta$  can therefore be congruent with respect to  $i$  to one and to only one of the numbers  $\alpha\rho$ .

If  $\alpha\rho \equiv \beta \pmod{i}$ , then is  $\xi = \rho$  a solution of the congruence and the only possible one of the entire system of residues. Besides this solution, every integer of the form  $\rho + xi + y(i_1 + i_2\omega)$  satisfies the congruence, if  $i$ ,  $i_1 + i_2\omega$  form a basis of  $i$ , and  $x$ ,  $y$  are rational integers.

Due to the Fermat Theorem,

$$\alpha^{\Phi(i)} \equiv 1 \pmod{i},$$

and consequently

$$\xi = \alpha^{\Phi(i)-1}\beta, \quad \text{or} \quad \rho = \beta\alpha^{\Phi(i)-1}.$$

Note that with rational integers the equation

$$ax + by = 1$$

may be solved by means of continued fractions, if  $a$  and  $b$  are relatively prime. This is no longer possible in the case of ideals in the realm  $\Re\sqrt{m}$ , since the Euclid Algorithm is no longer applicable. (Art. 111).

SECOND CASE. Take next the more general case where  $(\alpha)$  and  $i$  have the greatest common (ideal) divisor  $\delta$ , so that  $(\alpha) = a\delta$  and  $i = i^*\delta$ . Then clearly the congruence

$$\alpha\xi \equiv \beta \pmod{i}$$

is solvable only if  $\delta$  is a divisor of  $\beta$ , so that  $(\beta) = b\delta$ .

For if

$$(\alpha\xi - \beta) = ti = ti^*\delta,$$

then we must have  $\alpha\xi - \beta \equiv -\beta \equiv 0 \pmod{\delta}$ .

If, however,  $\beta \equiv 0 \pmod{\delta}$  is satisfied, then the congruence admits solution as is shown below.

By hypothesis  $a$  and  $i^*$  are relatively prime. It is always possible to find an integer  $\delta$  of the realm such that 1st  $(\delta)$  is divisible by the first but no higher power of  $\delta$ , and 2nd  $\frac{(\delta)}{\delta} = \delta_1$  is prime to  $i$ . (See Art. 215).

Further determine an integer  $\lambda$  of the ideal  $\delta_1$  which is prime to  $i$ , and write

$$\frac{\alpha\lambda}{\delta} = \alpha_1, \quad \frac{\beta\lambda}{\delta} = \beta_1.$$

The numbers  $\alpha_1$  and  $\beta_1$  are integers of the realm and if the congruence  $\alpha\xi \equiv \beta \pmod{i}$  is solvable through an integer of the realm, say  $\xi = \rho$ , then also the congruence  $\alpha_1\xi \equiv \beta_1 \pmod{i^*}$  is satisfied by the same integer and *vice versa*.

For if the congruence

$$\alpha\rho \equiv \beta \pmod{i}$$

is true, then also

$$\lambda\alpha\rho \equiv \lambda\beta \pmod{i},$$

or

$$\delta\alpha_1\rho \equiv \delta\beta_1 \pmod{i};$$

and consequently

$$\alpha_1\rho \equiv \beta_1 \pmod{i^*}.$$

Reciprocally, if

$$\alpha_1\rho \equiv \beta_1 \pmod{i^*},$$

then also

$$\delta\alpha_1\rho \equiv \delta\beta_1 \pmod{i},$$

or

$$\lambda\alpha\rho \equiv \lambda\beta \pmod{i};$$

and since  $\lambda$  is relatively prime to  $i$ , it follows that

$$\alpha\rho \equiv \beta \pmod{i}.$$

Further since  $\alpha_1$  is prime to  $i^*$ , the congruence

$$\alpha_1\xi - \beta_1 \equiv 0 \pmod{i^*}$$

may be satisfied by an integer  $\rho$ , and consequently also the given congruence  $\alpha\xi \equiv \beta \pmod{i}$  has  $\rho$  as a solution, if the greatest common divisor of  $(\alpha)$  and  $i$  is also a divisor of  $(\beta)$ .

We may write all the solutions of the congruence  $\alpha_1\xi \equiv \beta_1 \pmod{i^*}$  in the form  $\xi = \rho + xi^* + y(i_1^* + i_2^*\omega)$ , ( $x, y$  rational integers) where  $i^*$  and  $i_1^* + i_2^*\omega$  form a basis of  $i^*$ ,

while all the solutions of the congruence  $\alpha\xi \equiv \beta \pmod{i}$  are of the form  $\xi = \rho + si + t(i_1 + i_2\omega)$  ( $s, t$  rational integers), where  $i$  and  $i_1 + i_2\omega$  form a basis of  $i$ . Observe that  $N(i) = N(\mathfrak{d})N(i^*)$ .

These latter  $ii_2$  integers repeat themselves in the sequences of the former  $i^*i_2^*$  integers, so that there are  $\frac{ii_2}{i^*i_2^*}$  incongruent numbers with respect to the modulus  $i$  which satisfy the original congruence, and this number is  $N(\mathfrak{d})$ .

What has been proved may be formulated as follows:

**THEOREM.** *A linear congruence  $\alpha\xi \equiv \beta \pmod{i}$  may be satisfied by an integer of the realm, if and only if the greatest common divisor  $\mathfrak{d}$  of the ideal  $(\alpha)$  and the ideal  $i$  is also a divisor of the ideal  $(\beta)$ , and in this case the congruence has exactly  $N(\mathfrak{d})$  incongruent solutions.*

This theorem is in its entire development true, if the modulus  $i$  is replaced by an integer  $\gamma$  of the realm; and the result may be formulated as follows:

A Diophantine equation with integral coefficients  $\alpha, \beta, \gamma$  belonging to the realm  $\mathfrak{R}(\sqrt{m})$ :

$$\alpha\xi + \gamma\eta = \beta,$$

admits solution (and therefore infinitely many solutions) if the greatest common ideal divisor of  $(\alpha)$  and  $(\beta)$  is also a divisor of  $(\gamma)$ .

The following theorem for simultaneous congruences is often of use:

**THEOREM.** *If  $a_1, a_2$  are two ideals that are prime to each other, and if  $\alpha_1, \alpha_2$  are any two integers of the realm, there is always an integer  $\xi$  which simultaneously satisfies both congruences*

$$\xi \equiv \alpha_1 \pmod{a_1}, \quad \xi \equiv \alpha_2 \pmod{a_2}.$$

*Proof.* Suppose that the integer  $\rho$  of the realm satisfies the congruence

$$\xi \equiv \alpha_1 \pmod{\mathfrak{a}_1}.$$

Suppose further that  $\mathfrak{a}_1 = (i, i_1 + i_2\omega)$ , so that the general solution of the above congruence is  $\xi = \rho + \sigma i + \tau(i_1 + i_2\omega)$ , where  $\sigma$  and  $\tau$  are integers of the realm. In order that  $\xi$  may also satisfy the second congruence, the integers  $\sigma$  and  $\tau$  must be so chosen that

$$\rho + \sigma i + \tau(i_1 + i_2\omega) \equiv \alpha_2 \pmod{\mathfrak{a}_1},$$

and

$$\sigma i + \tau(i_1 + i_2\omega) \equiv \alpha_2 - \rho \pmod{\mathfrak{a}_2}.$$

Next write  $\sigma = A\xi_1$  and  $\tau = B\xi_1$  and so choose  $A$  and  $B$  as rational integers that

$$Ai + B(i_1 + i_2\omega) = \alpha_1^*$$

say, is relatively prime to  $\mathfrak{a}_2$ , which is possible since  $\alpha_1^*$  is an integer of the ideal  $\mathfrak{a}_1$ , which ideal is prime to  $\mathfrak{a}_2$ .

It is then seen that  $\xi_1$  may be determined as a root of the congruence

$$\alpha_1^* \xi \equiv \alpha_2 - \rho \pmod{\mathfrak{a}_2}.$$

The quantities  $\sigma$  and  $\tau$  thus determined offer the required value of  $\xi$ . (Sommer, *Vorlesungen*, etc., p. 91).

*Remark.* The congruences  $\kappa_1 \xi \equiv \alpha_1 \pmod{\mathfrak{a}_1}$ ,  $\kappa_2 \xi \equiv \alpha_2 \pmod{\mathfrak{a}_2}$  where  $\kappa_1$  is prime to  $\mathfrak{a}_1$  and  $\kappa_2$  to  $\mathfrak{a}_2$ , and where  $\mathfrak{a}_1$  and  $\mathfrak{a}_2$  are relatively prime, may through multiplication by respectively  $\kappa_1^{\phi(\mathfrak{a}_1)-1}$  and  $\kappa_2^{\phi(\mathfrak{a}_2)-1}$  be brought to the two forms of congruences above considered.

EXAMPLE. Derive the necessary and sufficient conditions for the solution of two simultaneous congruences where  $\kappa_1$  and  $\mathfrak{a}_1$  as also  $\kappa_2$  and  $\mathfrak{a}_2$  are no longer relatively prime.

## QUADRATIC CONGRUENCES AND THE SYMBOL $\left(\frac{\alpha}{\mathfrak{p}}\right)$

ART. 227. The most general congruence of the second degree with respect to the modulus  $\mathfrak{p}$  is

$$(1) \quad \alpha \xi^2 + 2\alpha_1 \xi + \alpha_2 \equiv 0 \pmod{\mathfrak{p}},$$

where  $\alpha, \alpha_1, \alpha_2$  are arbitrary integers of the realm. If  $\alpha, \alpha_1, \alpha_2$  are all prime to  $\mathfrak{p}$ , the above congruence has a root, if the congruence

$$\alpha(\alpha\xi^2 + 2\alpha_1\xi + \alpha_2) \equiv 0 \pmod{\mathfrak{p}}$$

admits solution and *vice versa*. (Read Smith's *Report*, pp. 55 et seq.)

The last congruence may be written

$$(\alpha\xi + \alpha_1)^2 + \alpha\alpha_2 - \alpha_1^2 \equiv 0 \pmod{\mathfrak{p}};$$

and the question whether the congruence (1) is solvable in integers of  $\mathfrak{K}(\sqrt{m})$  is identical with the question whether the combined congruences

$$(2a) \quad \sigma^2 + \alpha^* \equiv 0 \pmod{\mathfrak{p}}$$

$$(2b) \quad \alpha\xi + \alpha_1 \equiv \sigma \pmod{\mathfrak{p}}$$

may be solved. Since (2b) admits solution when  $\sigma$  is known, the question to be answered is whether (2a) is solvable.

If in the original congruence  $\alpha$  or  $\alpha_2$  are divisible by  $\mathfrak{p}$ , this congruence reduces to one of the first degree.

If on the other hand  $\alpha_1$  is divisible by  $\mathfrak{p}$ , the congruence (1) reduces to

$$\alpha\xi^2 + \alpha_2 \equiv 0 \pmod{\mathfrak{p}}.$$

Since  $\alpha$  is prime to  $\mathfrak{p}$  this congruence admits solution if

$$(3) \quad \alpha^{N(\mathfrak{p})-2}(\alpha\xi^2 + \alpha_2) \equiv 0 \pmod{\mathfrak{p}}$$

can be solved.

Due to the Fermat Theorem the last congruence takes the form

$$\xi^2 + \alpha^* \equiv 0 \pmod{\mathfrak{p}};$$

and the question as to the solution of the general congruence of the second degree resolves itself into the question respecting the solution of a congruence of the first degree in the special cases or of a *pure* congruence of



the second degree of the form

$$(1^1) \quad \xi^2 - \alpha \equiv 0 \pmod{p}.$$

It is therefore only necessary to consider this congruence, and we begin with the case where the prime modulus  $p$  is not a divisor of the principal ideal (2).

If  $\alpha$  is divisible by  $p$ , we have the congruence  $\xi^2 \equiv 0 \pmod{p}$  which admits a double solution. Hence only the case where  $\alpha$  is relatively prime to  $p$  is left to be considered.

If  $\bar{\omega}$  is a primitive number with respect to  $p$ , there is an integral positive exponent  $a$  such that

$$\bar{\omega}^a \equiv \alpha \pmod{p};$$

and it is evident that the given congruence (1<sup>1</sup>) is solvable only when  $a$  is an even integer, say  $a = 2a_1$ , in which case  $\xi = \bar{\omega}^{a_1}$  is the evident solution as is also  $\xi = -\bar{\omega}^{a_1}$ . We shall next see that the sufficient and necessary condition for this is that

$$\alpha^{\frac{N(p)-1}{2}} = (\bar{\omega}^a)^{\frac{N(p)-1}{2}} \equiv +1 \pmod{p},$$

a result which may be expressed as follows:

**THEOREM.** *The quadratic congruence  $\xi^2 \equiv \alpha \pmod{p}$  with respect to a prime modulus  $p$ , which is not a divisor of (2) is for an integer  $\alpha$ , prime to  $p$ , solvable by two incongruent integers of the realm, when and only when*

$$\alpha^{\frac{N(p)-1}{2}} \equiv +1 \pmod{p}.$$

**ART. 228.** If a congruence  $\xi^2 \equiv \alpha \pmod{p}$ , where  $\alpha$  is not divisible by  $p$ , is solvable, we say  $\alpha$  is a *quadratic residue*<sup>1</sup> with respect to  $p$ ; and if this congruence does not admit of solution, we say that  $\alpha$  is a *quadratic non-residue* with respect to  $p$ .

<sup>1</sup> Dirichlet, *Zahlentheorie*, p. 75.

The first case is denoted by the symbol

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1;$$

while in the second case, the symbol

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$$

is used to denote that there is *no* solution.

Due to the generalized Fermat Theorem

$$\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}};$$

or

$$\left(\alpha^{\frac{N(\mathfrak{p})-1}{2}} - 1\right)\left(\alpha^{\frac{N(\mathfrak{p})-1}{2}} + 1\right) \equiv 0 \pmod{\mathfrak{p}}.$$

Both factors on the left are not divisible by  $\mathfrak{p}$ ; for in that case  $2\alpha^{\frac{N(\mathfrak{p})-1}{2}}$  would be divisible by  $\mathfrak{p}$ , which is not true since neither 2 nor  $\alpha^{\frac{N(\mathfrak{p})-1}{2}}$  is divisible by  $\mathfrak{p}$ . It follows that either

$$\alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv 1 \pmod{\mathfrak{p}} \quad \text{or} \quad \alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv -1 \pmod{\mathfrak{p}}.$$

In the first case we have

$$\alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv (\tilde{\omega}^a)^{\frac{N(\mathfrak{p})-1}{2}} \equiv 1 \pmod{\mathfrak{p}},$$

which is true if  $a$  is an even integer, and we then have

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1.$$

In the second case we have

$$\alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv (\tilde{\omega}^a)^{\frac{N(\mathfrak{p})-1}{2}} \equiv -1 \pmod{\mathfrak{p}}$$

and consequently  $a$  is odd and therefore

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1.$$

If, therefore,  $\mathfrak{p}$  is not a divisor of 2 and if  $\alpha$  is any integer of the realm  $\Re(\sqrt{m})$  that is not divisible by this prime

ideal, it is seen that  $\alpha$  is a quadratic residue or non-residue with respect to  $\mathfrak{p}$  according as

$$\alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv +1 \quad \text{or} \quad \alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv -1 \pmod{\mathfrak{p}}.$$

Both cases are expressed through the congruence

$$\alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right), \pmod{\mathfrak{p}}.$$

Due to the theorem relative to the existence of primitive numbers, and the fact that  $\bar{\omega}, \bar{\omega}^2, \dots, \bar{\omega}^{N(\mathfrak{p})-1}$  represent a complete system of incongruent numbers with respect to  $\mathfrak{p}$ , it also follows that *there are  $\frac{N(\mathfrak{p})-1}{2}$  incongruent quadratic residues and an equal number of non-residues with respect to the prime ideal  $\mathfrak{p}$ , where  $\mathfrak{p}$  is not a divisor of 2.*

**THEOREM.** *If  $\alpha$  and  $\beta$  are two integers of  $\Re(\sqrt{m})$  that are not divisible by  $\mathfrak{p}$ , then is*

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right).$$

*Proof.* We have

$$\left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{\frac{N(\mathfrak{p})-1}{2}}, \quad \left(\frac{\beta}{\mathfrak{p}}\right) \equiv \beta^{\frac{N(\mathfrak{p})-1}{2}}, \quad \pmod{\mathfrak{p}};$$

and therefore

$$\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) = (\alpha\beta)^{\frac{N(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha\beta}{\mathfrak{p}}\right), \quad \pmod{\mathfrak{p}}.$$

It follows that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha\beta}{\mathfrak{p}}\right).$$

The case where  $\mathfrak{p}$  is a divisor of 2 or of the ideal (2) may be treated independently.

For if in the realm  $\Re(\sqrt{m})$  the ideal (2) is reducible into two factors  $\mathfrak{p}$  and  $\mathfrak{p}'$ , then  $N(\mathfrak{p}) = 2$  and  $\Phi(\mathfrak{p}) = 1$ , and there

is only one incongruent integer (mod.  $\mathfrak{p}$ ), namely  $\rho = 1$ . Since  $\alpha$  by hypothesis is prime to  $\mathfrak{p}$ , it is seen that  $\alpha \equiv 1 \pmod{\mathfrak{p}}$ , and consequently  $\xi^2 \equiv 1 \pmod{\mathfrak{p}}$  is solvable.

In Art. 216, Cases I and II, it was seen that 2 is either  $= \mathfrak{p}\mathfrak{p}'$  or to  $\mathfrak{p}^2$ , when  $m \equiv 2 \pmod{4}$  or  $m \equiv 3 \pmod{4}$ ; and it is irreducible (Art. 216, Case III) when  $m \equiv 1 \pmod{4}$ , and that is, when  $m = 5, 13, 21, 29$ , etc. In this case  $N(\mathfrak{p}) - 1 = 3$ . Here the integers  $1, \omega, 1 + \omega$  form a system of incongruent residues, mod. (2). Observe, however, that

$$\begin{aligned} \xi^2 &\equiv 1 \pmod{\mathfrak{p}} && \text{admits solution } \xi = 1, \\ \xi^2 &\equiv \omega \pmod{\mathfrak{p}} && \text{“ “ } \xi = 1 + \omega, \\ \xi^2 &\equiv 1 + \omega \pmod{\mathfrak{p}} && \text{“ “ } \xi = \omega. \end{aligned}$$

Hence in all cases  $\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$  where  $\mathfrak{p} = (2)$  or is a divisor of (2).

ART. 229. If we wish to extend the previous considerations by taking a quadratic congruence

$$\xi^2 - \alpha \equiv 0 \pmod{\mathfrak{a}},$$

in which  $\mathfrak{a}$  is an arbitrary ideal modulus, we must first consider the case

$$(1) \quad \xi^2 - \alpha \equiv 0 \pmod{\mathfrak{p}^k},$$

which is a congruence with respect to the  $k$ th power of a prime ideal. This case alone we shall discuss here.

I. Suppose that  $\mathfrak{p}$  is *not* a divisor of (2). It is evident that the congruence (1) can be solved only if the congruence  $\xi^2 - \alpha \equiv 0 \pmod{\mathfrak{p}}$  admits solution, and that is if

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1.$$

But if this condition is satisfied and if  $\lambda$  is a solution of the latter congruence, where  $\lambda$  is also prime to  $\mathfrak{p}$ , there are an infinite number of roots of the form  $\xi = \lambda + \mathfrak{p}\rho$ ,

where  $p$  is a prime rational integer that is divisible by  $\mathfrak{p}$ , and where  $\rho$  runs through all the integers of the realm. Among these numbers  $\lambda + p\rho$  there must be a root of the congruence

$$\xi^2 - \alpha \equiv 0 \pmod{\mathfrak{p}^k},$$

if such a root exists.

We first put  $k=2$  and assume that  $p$  is not divisible by  $\mathfrak{p}^2$ . We must then determine  $\rho$  so that

$$(\lambda + p\rho)^2 - \alpha \equiv 0 \pmod{\mathfrak{p}^2},$$

or

$$2p\lambda\rho + \lambda^2 - \alpha \equiv 0 \pmod{\mathfrak{p}^2}.$$

If  $\lambda^2 - \alpha \equiv 0 \pmod{\mathfrak{p}^2}$ , it is only necessary to put  $\rho = 0$ . If this case is excluded, we must determine whether or not an integral value may be found for  $\rho$  such that the congruence

$$2p\lambda\rho + \lambda^2 - \alpha \equiv 0 \pmod{\mathfrak{p}^2}$$

is satisfied.

Since  $\lambda$  satisfies the congruence  $\lambda^2 - \alpha \equiv 0 \pmod{\mathfrak{p}}$ , it follows that  $\mathfrak{p}$ , the greatest common divisor of  $2p\lambda\rho$  and  $(\lambda^2 - \alpha)$ , also divides  $\lambda^2 - \alpha$ , and consequently the resulting congruence admits solution. If  $\rho = \rho_0$  satisfies this congruence, then  $\xi = \lambda + p\rho_0$  is a solution of the congruence  $\xi^2 - \alpha \equiv 0 \pmod{\mathfrak{p}^2}$ .

In an analogous manner it may be shown that the congruence

$$\xi^2 \equiv \alpha \pmod{\mathfrak{p}^3}$$

admits solution; and in general the following theorem is had:

**THEOREM.** *If  $\mathfrak{p}$  is a prime ideal of  $\mathfrak{K}(\sqrt{m})$  and is not a divisor of (2) and is not a divisor of the discriminant of the realm, and if  $\alpha$  is an integer of the realm that is not divisible by  $\mathfrak{p}$ , then the congruence*

$$\xi^2 \equiv \alpha \pmod{\mathfrak{p}^k}$$



admits solution or not, according as

$$\left(\frac{a}{p}\right) = +1 \quad \text{or} \quad \left(\frac{\alpha}{p}\right) = -1.$$

If  $p^2$  is a divisor of the rational prime integer  $p$ , and that is; if  $p$  is a divisor of the discriminant (Art. 216, end of Case III), the discussions respecting the solution of the general congruence must be somewhat modified.

It is easy to see that in this case the congruence

$$\xi^2 - \alpha \equiv 0 \pmod{p^k}$$

is only solvable for an arbitrary exponent  $k$ , if

$$\xi^2 - \alpha \equiv 0 \pmod{p^2}$$

admits solution.

II. The case where (2) is divisible by the prime ideal  $\mathfrak{p}$  may be settled in a manner similar to the preceding case and offers the following theorem:

**THEOREM.** *If  $\mathfrak{p}$  is a prime ideal of the realm  $\mathfrak{R}(\sqrt{m})$  and is a divisor of (2), and if  $\alpha$  is an integer of the realm that is relatively prime to  $\mathfrak{p}$ , then the congruence  $\xi^2 - \alpha \equiv 0 \pmod{p^k}$ , where  $k$  is an arbitrary rational integer, admits solution if, and only if the congruence*

$$\xi^2 - \alpha \equiv 0 \pmod{p^6} \tag{i}$$

*has a solution, in the case that  $\mathfrak{p}$  is a prime ideal of the first degree, and if secondly*

$$\xi^2 - \alpha \equiv 0 \pmod{p^3} \tag{ii}$$

*has a solution, where  $\mathfrak{p}$  is a prime ideal of the second degree.*

Observe that if  $\eta$  satisfies the congruence  $\eta^2 \equiv \alpha \pmod{2^3}$ , so that

$$\eta^2 - \alpha = 2^3\gamma,$$

and if we substitute  $\xi = \eta + \lambda 2^2$  in the congruence  $\xi^2 \equiv \alpha \pmod{2^4}$ , we have

$$0 \equiv \xi^2 - \alpha \equiv 2^3[\gamma + \lambda\eta + 2\lambda^2] \pmod{2^4},$$

and this congruence may be satisfied since  $\lambda$  may be

determined so as to satisfy the congruence  $\gamma + \lambda\eta \equiv 0 \pmod{2}$ .

Similarly, if

$$\xi^2 - \alpha \equiv 0 \pmod{2^k}, k \equiv 3,$$

can be solved so that  $\eta^2 - \alpha = 2^k\gamma$ , then by the substitution  $\xi = \eta + \lambda 2^{k-1}$  it is seen that we can solve  $\xi^2 - \alpha \equiv 0 \pmod{2^{k+1}}$ .

The question for what values of  $\alpha$  are the congruences (i) and (ii) solvable, may be determined through a discussion of all possible individual cases. It is seen that for both cases we must have

$$\alpha \equiv 1 \pmod{p^6} \quad \text{or} \quad \alpha \equiv 1 \pmod{2^3};$$

and in either case there are four incongruent solutions, namely  $\pm 1$  and  $\pm 3$ .

A method is *not* given here for the calculation of the symbol  $\left(\frac{\alpha}{p}\right)$ . In a later chapter a more general symbol and the accompanying theory is discussed (see Chapter X). A more detailed account of what has been given above with numerous illustrative examples is found in Chapter XII of Reid's *The Elements of the Theory of Algebraic Numbers*.

**ART. 230. Units<sup>1</sup> of the Quadratic Realm.** Among the integers of a realm appear the "units" which play an interesting rôle. By these units is understood every integer of the realm which is a divisor of  $\pm 1$ , or, what amounts to the same thing, every integer whose norm is equal to  $\pm 1$ . In a discussion regarding *algebraic units* it must first of all be proved that there *exist* such units which are different from  $\pm 1$ .

**THEOREM I.** *In an arbitrary imaginary realm, the only units are  $\pm 1$ . However, in the realm  $\Re(\sqrt{-1})$  other*

<sup>1</sup> See Smith's *Report*, p. 98; Sommer, *Vorlesungen*, etc., p. 98.

units are  $\pm\sqrt{-1}$ , and in the realm  $\Re(\sqrt{-3})$ , further units are  $\pm\frac{1\pm\sqrt{-3}}{2}$ .

*Proof.* Consider first the realm  $\Re(\sqrt{-1})$ . In this realm  $x + \sqrt{-1}y$  is a unit if its norm =  $\pm 1$ ; and that is if  $x^2 + y^2 = \pm 1$ . It is clear that  $x^2 + y^2 = -1$  cannot be satisfied by real values of  $x$  and  $y$ . However, the equation  $x^2 + y^2 = +1$  may be satisfied by the four systems of values as given in Art. 99, which offer the units  $\pm 1, \pm i$ , which are the four fourth roots of unity.

Further in the realm  $\Re(\sqrt{-3})$ , whose basis is  $1, \frac{1+\sqrt{-3}}{2}$ , an integer  $x + \frac{1+\sqrt{-3}}{2}y$  may be a unit of the realm, if

$$N\left(x + \frac{1+\sqrt{-3}}{2}y\right) = \pm 1;$$

and that is, if

$$\left(x + \frac{1}{2}y\right)^2 + \frac{3}{4}y^2 = \pm 1.$$

It is evident that when the lower sign to the right is taken, the corresponding equation cannot be solved in real integral values of  $x, y$ . However, the equation

$$x^2 + xy + y^2 = +1$$

admits six solutions with the corresponding units  $\pm 1,$

$$\pm\omega = \pm\frac{1+\sqrt{-3}}{2}, \quad \pm\omega' = \pm\frac{1-\sqrt{-3}}{2}$$

(Art. 99) quantities, that are the six sixth roots of unity.

ART. 231. For every other arbitrary *imaginary realm*  $\Re(\sqrt{m})$ , an integer of the form

$$x + \sqrt{m}y, \quad \text{if } m \not\equiv 1 \pmod{4},$$

or of the form

$$x + \frac{1+\sqrt{m}}{2}y, \quad \text{if } m \equiv 1 \pmod{4},$$

can be a unit only if

$$x^2 - my^2 = \pm 1$$

in the first case, and if

$$(x + \frac{1}{2}y)^2 - \frac{m}{4}y^2 = \pm 1$$

in the second case. Note that  $m$  is a negative number in both cases, as the question before us is regarding imaginary realms.

In the first case  $|m| \equiv 2$  and in the second case  $|m| \equiv 7$ . In either case the only solutions are  $x = \pm 1$ . It follows that  $\pm 1$  are the only units in the general imaginary realms.

**THEOREM II.** *In every real realm  $\Re(\sqrt{m})$  there exist an infinite number of units different from  $\pm 1$ , and among them there is one fundamental or principal unit  $\epsilon$  which in absolute value is greater than 1 and is such that every unit of the realm may be expressed in the form  $\epsilon^e$ , where  $e$  is a positive or negative rational integer.*

The proof of this theorem is divided into two parts: *First*, it is proved that in every real realm  $\Re(\sqrt{m})$  there are an infinite number of units which are different from  $\pm 1$ ; and *then* the fundamental unit  $\epsilon$  is derived which has the properties stated in the theorem.

The first part of the proof is identical with the proof that the equation

$$x^2 - my^2 = \pm 1 \quad [\text{if } m \not\equiv 1 \pmod{4}],$$

or

$$(x + \frac{1}{2}y)^2 - \frac{m}{4}y^2 = \pm 1 \quad [\text{if } m \equiv 1 \pmod{4}]$$

admits solution in integral rational values of  $x, y$  (at least for  $+1$  on the right hand side of the above equations) for every positive integer  $m$ .

Denote the discriminant of the realm by  $d$  and observe

that  $1, \omega = \sqrt{m}$  are a basis when  $m \not\equiv 1 \pmod{4}$  and that  $1, \frac{1+\sqrt{m}}{2} = \omega$  constitute a basis when  $m \equiv 1 \pmod{4}$ .

Consider the linear forms with real coefficients

$$\begin{aligned} f &= x - \omega y, \\ f' &= x - \omega' y, \end{aligned}$$

with determinant  $\omega - \omega'$ , which is positive and equal to  $\sqrt{d}$ . It is clear that

$$ff' = x^2 - my^2, \quad \text{when} \quad m \not\equiv 1 \pmod{4};$$

and

$$ff' = x^2 + xy + \frac{1-m}{4}y^2, \quad \text{when} \quad m \equiv 1 \pmod{4}.$$

Due to the Minkowski Theorem (Art. 26) if  $k$  and  $k_1$  denote real positive quantities such that  $kk_1 = \sqrt{d}$ , it is always possible to find rational integers  $x, y$  such that

$$\begin{aligned} |f| &= |x - \omega y| \leq k, \\ |f'| &= |x - \omega' y| \leq k_1. \end{aligned}$$

First let  $k=1$  and  $k_1 = \sqrt{d}$  and determine two rational integers  $x_1, y_1$  such that

$$\begin{aligned} |x_1 - \omega y_1| &\leq 1, \\ |x_1 - \omega' y_1| &\leq \sqrt{d}. \end{aligned}$$

Let

$$\alpha_1 = x_1 - \omega y_1 \quad \text{and} \quad \alpha'_1 = x_1 - \omega' y_1.$$

Next let

$$k_1 = \frac{|\alpha_1|}{2} \quad \text{and} \quad k_2 = \frac{2\sqrt{d}}{|\alpha_1|}$$

and determine two rational integers  $x_2$  and  $y_2$  so that

$$\begin{aligned} |x_2 - \omega y_2| &\leq \frac{|\alpha_1|}{2}, \\ |x_2 - \omega' y_2| &\leq \frac{2\sqrt{d}}{|\alpha_1|}; \end{aligned}$$



and write  $\alpha_2 = x_2 - \omega y_2$ ,  $\alpha'_2 = x_2 - \omega' y_2$ . Then write

$$k = \frac{|\alpha_2|}{2}, \quad k_1 = \frac{2\sqrt{d}}{|\alpha_2|},$$

and determine integers  $x_3, y_3$  such that

$$|x_3 - \omega y_3| \leq \frac{|\alpha_2|}{2},$$

$$|x_3 - \omega' y_3| \leq \frac{2\sqrt{d}}{|\alpha_2|},$$

and put  $\alpha_3 = x_3 - \omega y_3$ ,  $\alpha'_3 = x_3 - \omega' y_3$ , etc.

Note that  $x_1, y_1$  are not the same as  $x_2, y_2$ , and that  $x_2, y_2$  are different from  $x_3, y_3$ .

In this manner we may determine an infinite series of integers  $\alpha_1, \alpha_2, \alpha_3, \dots$ , such that  $|\alpha_1| > |\alpha_2| > |\alpha_3| \dots$ .

Note, however, that  $(\alpha_1), (\alpha_2), (\alpha_3), \dots$  form an infinite number of ideals whose norms are all in absolute value  $\leq \sqrt{d}$ . On the other hand it was proved (Art. 211) that there are only a finite number of ideals whose norms are less than a given quantity. Hence in the series above the ideals must repeat themselves, so that  $(\alpha_1) = (\alpha_r)$ , say.

Since  $|\alpha_1| > |\alpha_r|$  it follows that  $\frac{\alpha_1}{\alpha_r} \neq \pm 1$ .

It is further seen that  $\frac{\alpha_1}{\alpha_r}$  is an integer, and also that  $\frac{\alpha_r}{\alpha_1}$  is an integer, the reciprocal of the first integer.

Hence (Art. 90) we may write  $\alpha_1 = \epsilon_r \alpha_r$ , where  $\epsilon_r$  is a unit that is  $\neq \pm 1$ , and where

$$|\epsilon_r| = \frac{|\alpha_1|}{|\alpha_r|} > 1.$$

Since  $\epsilon_r$  is a unit,  $N(\epsilon_r) = \pm 1$ , and it is clear that  $N(\epsilon_r^2) = +1$ .

Hence in every real realm there are algebraic units whose norms = +1. At the same time it is proved that

Pell's equations

$$\begin{aligned} x^2 - my^2 = 1 & \quad \text{when} \quad m \not\equiv 1 \pmod{4}, \\ x^2 + xy + \frac{1-m}{4}y^2 = 1 & \quad \text{when} \quad m \equiv 1 \pmod{4}, \end{aligned}$$

always admit solution in integral values of  $x, y$ . (See Art. 99.)

However, it has not been shown<sup>1</sup> that the equations

$$x^2 - my^2 = -1 \quad \text{and} \quad x^2 + xy + \frac{1-m}{4}y^2 = -1$$

admit solution. Only for special values of  $m$  has it been determined whether or not these equations admit solution.

ART. 232. After it has been shown that in every real realm there are units which are different from  $\pm 1$ , it is easy to see that the powers in positive and negative integral exponents of such a unit  $\epsilon_r$  offer an infinite number of other units that are different from  $\epsilon_r$ .

If  $\epsilon$  is any unit, then for any integral exponent  $a$ , the following equation is true:

$$N(\epsilon^a) = N(\epsilon)^a = (\pm 1)^a,$$

and consequently also  $\epsilon^a$  is a unit.

If, further,  $a, a_1$  are integers such that  $a > a_1 > 0$ , and if

$$|\epsilon| > 1, \quad \text{then is} \quad |\epsilon^a| > |\epsilon^{a_1}|,$$

while if

$$|\epsilon| < 1, \quad \text{then is} \quad |\epsilon^a| < |\epsilon^{a_1}|.$$

It is evident that  $\epsilon^a$  and  $\epsilon^{a_1}$  are different from each other and that their product is not equal to  $\pm 1$ .

Corresponding to every integer  $\epsilon$ , whose absolute value is less than 1, there is another unit  $\frac{1}{\epsilon}$ , whose absolute value is greater than 1.

<sup>1</sup> See H. Schubert, *Unterrichts und Vorlesungspraxis*, Vol. 2, p. 160, Leipzig, 1905.

If the equations

$$x^2 - my^2 = -1 \quad \text{or} \quad x^2 + xy + \frac{1-m}{4}y^2 = -1$$

admit solution; and that is, if in  $\mathfrak{R}(\sqrt{m})$  there is a unit  $\epsilon_s$  such that  $N(\epsilon_s) = -1$ , the odd powers of  $\epsilon_s$  give an infinite number of units whose norm =  $-1$ , so that there are an infinite number of solutions of the above equation. The even powers of  $\epsilon_s$  on the other hand offer an infinite number of solutions of the equations

$$x^2 - my^2 = +1, \quad x^2 + xy + \frac{1-m}{4}y^2 = +1,$$

since  $N(\epsilon_s^{2a}) = +1$ .

The units whose absolute value are greater than unity may be arranged according to their magnitudes. If  $x_1, y_1$  and  $x_2, y_2$  are *positive* integral solutions of

$$x^2 - my^2 = \pm 1 \quad \text{or} \quad (x + \frac{1}{2}y)^2 - \frac{m}{4}y^2 = \pm 1,$$

and if  $x_1 > x_2$ , then also it is seen that  $y_1 > y_2$  and *vice versa*.

It is also observed that if  $m \not\equiv 1 \pmod{4}$  and if  $\eta_i = x_i + y_i\sqrt{m}$  is a unit in  $\mathfrak{R}(\sqrt{m})$ ; if further  $x_i$  is positive, then  $|\eta_i| > 1$  when  $y_1$  is positive. If further  $\eta_1 = x_1 + y_1\sqrt{m}$ ,  $\eta_2 = x_2 + y_2\sqrt{m}$  are units of this nature, and if  $y_1$  and  $y_2$  are both positive, and if  $y_1 > y_2$  then also is  $|\eta_1| > |\eta_2|$  and *vice versa*.

If the solutions of the equations

$$x^2 - my^2 = \pm 1 \quad \text{or} \quad x^2 + xy + \frac{1-m}{4}y^2 = \pm 1$$

are determined for the upper sign and as far as possible for the lower sign, and if the corresponding units  $\eta_i$  are determined when  $|\eta_i| > 1$ , and if they are arranged according to the magnitudes of  $y_i$ , we have the absolute values of  $\eta_i$  themselves, the smallest one corresponding to the smallest value of  $y$ . Denote this unit by  $\epsilon$ , where

neglecting the factor  $-1$ ,  $\epsilon$  is completely determined and is the *fundamental unit* of the realm, being such that  $|\epsilon| > 1$ .

If  $\eta$  is an arbitrary unit of the realm such that  $|\eta| > 1$ , then a positive integer  $e$  may be found such that

$$|\epsilon^e| \equiv |\eta| < |\epsilon^{e+1}|$$

or

$$1 \equiv \frac{|\eta|}{|\epsilon^e|} < |\epsilon|.$$

From this it would follow that there is a unit  $\frac{\eta}{\epsilon^e}$  of the realm whose absolute value lies between 1 and  $|\epsilon|$ ; but this contradicts the definition of  $\epsilon$ . It follows that  $\eta = \epsilon^e$ .

In the same manner it may be shown that a unit whose absolute value is  $< 1$ , is equal to  $\pm \frac{1}{\epsilon^{e_1}}$  where  $e_1$  is a positive rational integer. And it is thus proved that all the units of the realm  $\mathfrak{R}(\sqrt{m})$  may be expressed in the form  $\pm \epsilon^e$  where  $e$  goes through all rational integral values (see Gauss, *Disq. Arith.*, V, 200).

If the realm contains units whose norms  $= -1$ , it is evident that the norm of the fundamental unit must be  $-1$ . For if  $\eta$  is a unit whose norm  $= +1$ , then  $\eta$  raised to all rational integral powers offer units whose norms  $= +1$ .

Write  $\epsilon = x_1 + y_1\omega$  where  $y_1$  is positive, and observe that  $x_1, y_1$  (when  $m \not\equiv 1 \pmod{4}$ ) and  $x_1 + \frac{y_1}{2}, y_1$  (when  $m \equiv 1 \pmod{4}$ ) offer the smallest integral positive solutions of the equations:

$$x^2 - my^2 = \pm 1 \quad \text{or} \quad x^2 + xy + \frac{1-m}{4}y^2 = \pm 1.$$

The positive signs to the right are to be taken when

$N(\epsilon) = +1$ ; and when  $N(\epsilon) = -1$ , the negative signs on the right must be used.

If it is not certain that the norm of the principal unit is  $-1$ , that is, whether the two above equations with negative sign to the right, admit solution, we may proceed as follows:

By solving the equations

$$x^2 - my^2 = +1 \quad \text{or} \quad x^2 + xy + \frac{1-m}{4}y^2 = +1,$$

compute the unit  $\eta$  which is least in absolute value and such that  $|\eta| > 1$ . Write  $\eta = x_1 + \omega y_1$ .

If  $\epsilon$  and not  $\eta$  were the fundamental unit where  $N(\epsilon) = -1$ , then since  $N(\epsilon^2) = +1$ , we must have

$$\epsilon^2 = (x + \omega y) = \pm \eta = \pm (x_1 + \omega y_1).$$

If these equations do *not* admit solution in integral values of  $x, y$ , then  $\eta$  and not  $\epsilon$  is the fundamental unit.

ART. 233. What has been proved above for the imaginary and real quadratic realms may be summarized as follows:

THE DIRICHLET THEOREM. *In a quadratic realm all the units may be expressed in one and in only one way through a fundamental unit in the form  $\rho\epsilon^e$  where  $\rho$  is a root of unity which belongs to the realm (for the case  $\Re(\sqrt{-1})$  or  $\Re(\sqrt{-3})$ ) and is otherwise equal to  $\pm 1$ , and where  $\epsilon = +1$  for imaginary realms, and is different from 1 for real realms.*

#### EXAMPLES

1. For the realm  $\Re(\sqrt{3})$ , the fundamental unit is  $\epsilon = 2 + \sqrt{3}$ . Note that the equation

$$x^2 - 3y^2 = \pm 1$$

may be solved only for the upper sign, and that  $x=2, y=1$  are the smallest (positive) values for the solution of the equation  $x^2 - 3y^2 = 1$ .



Further units are

$$\begin{aligned}\eta_1 &= \epsilon^2 = 7 + 4\sqrt{3}, \\ \eta_2 &= \epsilon^3 = 26 + 15\sqrt{3},\end{aligned}$$

etc. We further have

$$\begin{aligned}\epsilon' &= \frac{1}{\epsilon} = 2 - \sqrt{3}, \\ \epsilon'^2 &= 7 - 4\sqrt{3}, \\ \epsilon'^3 &= 26 - 15\sqrt{3},\end{aligned}$$

etc. The norm of all the units is  $+1$ .

2.  $\mathfrak{R}(\sqrt{14})$ . The smallest integral solution of the equation

$$x^2 - 14y^2 = +1$$

is had for  $x=15$ ,  $y=4$ , so that

$$\begin{aligned}\epsilon &= 15 + 4\sqrt{14}, \\ \epsilon^2 &= 449 + 120\sqrt{14}, \\ \epsilon^3 &= 13455 + 3596\sqrt{14},\end{aligned}$$

etc.

$$\begin{aligned}\epsilon' &= \frac{1}{\epsilon} = 15 - 4\sqrt{14}, \\ \epsilon'^2 &= 449 - 120\sqrt{14},\end{aligned}$$

etc. The equation

$$x^2 - 14y^2 = -1$$

does *not* admit solution in integral values of  $x$ ,  $y$ .

3.  $\mathfrak{R}(\sqrt{5})$ . The smallest integral solution of the equation

$$x^2 + xy - y^2 = -1,$$

is  $x=0$ ,  $y=1$ , so that

$$\begin{aligned}\epsilon &= \omega, & \text{and } N(\epsilon) &= -1, \\ \epsilon^2 &= 1 + \omega, & N(\epsilon^2) &= +1, \\ \epsilon^3 &= 1 + 2\omega, & N(\epsilon^3) &= -1,\end{aligned}$$

etc. It is also seen that

$$\epsilon' = \frac{1}{\epsilon} = \omega'.$$

## ART. 234. Realms in Which There Is an Odd Number of Classes.

**THEOREM.**<sup>1</sup> *Every integral or fractional number  $\alpha$  of the realm  $\mathfrak{R}(\sqrt{m})$ , whose norm is  $+1$ , may be expressed as the*

<sup>1</sup> Hilbert, *Zahlb.*, Chapter XV, § 54; Sommer, *Vorlesungen*, p. 107.

quotient of two conjugate algebraic integers in the form  $\frac{\gamma}{\gamma'}$ .

*Proof.* An integral or fractional number  $\alpha$  of the realm  $\mathfrak{K}(\sqrt{m})$  may always be expressed in the form

$$\alpha = \frac{a}{c} + \frac{b}{c}\omega,$$

where  $a, b, c$  are rational integers whose greatest common divisor is unity.

Further, since  $N(\alpha) = +1$ , it is seen that  $a$  and  $b$  are relatively prime.

The proof must be divided into two parts according as  $m \equiv 1 \pmod{4}$  or  $m \not\equiv 1 \pmod{4}$ .

CASE I.  $m \not\equiv 1 \pmod{4}$ ,  $\omega = \sqrt{m}$ . If we put

$$\alpha = \frac{1}{c}(a + b\omega) = \frac{x + y\omega}{x + y\omega'},$$

it is seen that  $x$  and  $y$  are to be determined from the equations

$$\begin{aligned} \left(\frac{a}{c} - 1\right)x - \frac{b}{c}my &= 0, \\ \frac{b}{c}x - \left(\frac{a}{c} + 1\right)y &= 0. \end{aligned}$$

These equations may be solved in integral values of  $x, y$  if the determinant vanishes; and that is, if

$$\Delta = -\frac{a^2}{c^2} + 1 + \frac{b^2}{c^2}m$$

is zero. This is true since the determinant just written is  $1 - N(\alpha) = 0$ . As solutions we have

$$x = \frac{1}{t}(a + c), \quad y = \frac{b}{t},$$

where  $t$  is a common divisor of  $a + c$  and  $b$ .

CASE II.

$$m \equiv 1 \pmod{4}, \quad \omega = \frac{1 + \sqrt{m}}{2}, \quad \omega' = \frac{1 - \sqrt{m}}{2}.$$

Again we may write

$$\alpha = \frac{1}{c}(a + b\omega) = \frac{x + y\omega}{x + y\omega'}$$

We have for the determination of the integers  $x, y$  the two equations

$$\begin{aligned} \left(\frac{a}{c} - 1\right)x + \left(\frac{a}{c} + \frac{b}{c} \frac{1-m}{4}\right)y &= 0, \\ \frac{bx}{c} - \left(\frac{a}{c} + 1\right)y &= 0, \end{aligned}$$

whose determinant is

$$\Delta = -\frac{a^2}{c^2} + 1 - \frac{ab}{c^2} - \frac{b^2}{c^2} \frac{1-m}{4} = 1 - N(\alpha) = 0.$$

As in the preceding case we may write

$$x = \frac{a+c}{t}, \quad y = \frac{b}{t},$$

$t$  being any divisor of  $a+c$  and  $b$ .

In both cases  $\gamma$  has the form

$$\frac{1}{t}(a+c+b\omega) = \frac{c}{t}(1+\alpha).$$

If as a particular case  $\alpha$  is an integer of the realm and consequently a unit, we may write for  $\gamma$  the expression  $1+\epsilon$ .

**ART. 235. THEOREM.** *If the discriminant of a real realm  $\Re(\sqrt{m})$  contains only one prime number, then the norm of the fundamental unit of this realm is  $-1$ .*

It is seen that the discriminant of the realm  $\Re(\sqrt{2})$  is  $8 = 2^3$ , while that of the realm  $\Re(\sqrt{p})$  is  $p$ , if  $p \equiv 1 \pmod{4}$ . These are the only quadratic realms whose discriminants contains only one prime factor.

Suppose that  $\epsilon$  is the fundamental unit. Further assume that  $N(\epsilon) = +1$ . Then due to the preceding theorem we may write  $\epsilon = \frac{\gamma}{\gamma'}$ , where  $\gamma$  is an integer and  $\gamma'$

its conjugate. It follows that  $\epsilon\gamma' = \gamma$  or  $(\gamma) = (\gamma')$ . Hence  $(\gamma)$  being an ambiguous ideal<sup>1</sup> is divisible only by ambiguous ideals. Besides rational integers the only ambiguous ideal (Art. 216, third case, end) is  $\sqrt{p}$ . It follows that  $(\gamma) = (a)$  where  $a$  is a rational integer, or  $(\gamma) = (\sqrt{p})$ , where 2 is included among the prime rational integers.

In the first case  $\gamma = \eta a$  and in the second  $\gamma = \eta\sqrt{p}$ , where  $\eta$  is an algebraic unit.

It further follows that

$$\epsilon = \frac{\eta a}{\eta' a} = \pm \eta^2, \quad \text{or} \quad \epsilon = \frac{\eta\sqrt{p}}{-\eta'\sqrt{p}} = \pm \eta^2.$$

And consequently  $\epsilon$  contrary to the assumption is *not* the fundamental unit.

This theorem proved by Lejeune Dirichlet, *Works*, I, 224 is also proved by Hilbert, *Zahlb.*, XVII, § 68.

**THEOREM.** *If the discriminant of a realm  $\mathfrak{K}(\sqrt{m})$  contains only one prime integer  $p$ , the number of classes  $h$  of the realm is odd.*

If contrary to the assertion, we assume that  $h$  is an even integer, we can determine an ideal  $i$  which is *not* a principal ideal such that  $i^2 \sim 1$  and  $ii' \sim 1$ . (Note that if  $a$  is any ideal,  $a^h \sim 1$ ).

It follows that  $i \sim i'$  or  $\frac{i}{i'} = \alpha$ , where  $\alpha$  is an algebraic number (rational or integral). And since  $i = \alpha i'$ , it is seen that

$$N(i) = N(\alpha)N(i') \quad \text{or} \quad N(\alpha) = \pm 1.$$

As shown in the preceding theorem, the norm of the fundamental unit  $\epsilon$  being  $-1$ , we may write

$$\alpha = \frac{\gamma'}{\gamma} \quad \text{if} \quad N(\alpha) = +1,$$

<sup>1</sup> An ambiguous ideal is one that is equal to its conjugate and which is not divisible by a rational integer.

and

$$\epsilon\alpha = \frac{\gamma'}{\gamma} \quad \text{if} \quad N(\alpha) = -1.$$

It follows that

$$(\gamma)i = (\gamma')i.$$

Hence the ideal  $(\gamma i)$  can have as factors only rational integers and ambiguous ideals.

The realm  $\Re(\sqrt{-1})$  has the ambiguous ideal  $(1 + \sqrt{-1})$ , and every other realm  $\Re(\sqrt{m})$  [in which  $m=2$ , or  $m=p \equiv 1 \pmod{4}$ ] has the ambiguous ideal  $\sqrt{m}$ .

It follows that  $(\gamma)i = (a)$ , or  $= (a\sqrt{m})$  or  $a(1 + \sqrt{-1})$ . And these are all fundamental ideals so that in each of these cases  $i \sim (1)$ . This is, however, contrary to the hypothesis that  $i$  was *not* a principal ideal.

**ART. 236. The Hilbert Number-Rings.**<sup>1</sup> If  $\alpha, \beta, \gamma, \dots$  are arbitrary algebraic *integers* of the realm  $\Re(\sqrt{m})$ , the aggregate of all integers which are had from these algebraic integers together with rational integers through the usual operations of addition, subtraction, and multiplication, and that is the aggregate of rational integral functions of  $\alpha, \beta, \gamma, \dots$ , with integral rational coefficients forms what Hilbert (*Zahlb.*, Chapt. IX) called a "number ring" (*Zahlring*), or *ring*. It is simply a realm of integrity as defined in Art. 182 and Art. 28.

A case of some interest is presented in connection with the realms of rationality  $\Re(\sqrt{m})$  where  $m \equiv 1 \pmod{4}$ . It was seen in Art. 98 that a basis of all integers of such realms is  $1, \omega = \frac{1 + \sqrt{m}}{2}$ . Associated with such a realm we may study the ring or realm of integrity that has as basis the two elements  $1, \sqrt{m}$ . This ring may be denoted by  $r(\sqrt{m})$ .

<sup>1</sup> See *Report on Algebraic Numbers*, pp. 59, 74.



It is evident that

1st, every integer of  $\mathfrak{r}(\sqrt{m})$  is an integer of  $\mathfrak{R}(\sqrt{m})$ ;

2nd, every integer of  $\mathfrak{r}(\sqrt{m})$  has the form  $x + y\sqrt{m}$ , where  $x, y$  are rational integers;

3rd, if  $\omega_1, \omega_2$  and  $\omega_1^*, \omega_2^*$  are two bases of the ring  $(\mathfrak{r}\sqrt{m})$ , then

$$\omega_1^* = r\omega_1 + s\omega_2, \quad \omega_2^* = t\omega_1 + u\omega_2,$$

where the rational integers  $r, s, t, u$  are connected by the relation  $ru - st = \pm 1$  (see Art. 94). The expression

$$D_r = \begin{vmatrix} 1, & \sqrt{m} \\ 1, & -\sqrt{m} \end{vmatrix}^2 = \begin{vmatrix} \omega_1, & \omega_2 \\ \omega_1', & \omega_2' \end{vmatrix}^2 = \begin{vmatrix} \omega_1^*, & \omega_2^* \\ \omega_1'^*, & \omega_2'^* \end{vmatrix}^2 = 4m$$

is called the *discriminant* of the ring. It is (see Art. 98) a multiple of the discriminant of the realm  $\mathfrak{R}(\sqrt{m})$ .

If  $i = (\alpha, \beta, \gamma, \dots)$ , then is

$$(\alpha, \beta, \gamma, \dots) = (\alpha, \beta, \gamma, \dots, \alpha\lambda_1 + \beta\lambda_2 + \gamma\lambda_3 + \dots),$$

where  $\lambda_1, \lambda_2, \lambda_3, \dots$  are *integers* of the ring. The notions and definitions which have been given for *bases* of ideals, *norms* of ideals, *conjugate* ideals, *products* of ideals, etc. are at once applicable to ring ideals.

If, for example,  $i_r = (\alpha, \beta, \gamma, \dots)$ , and if  $i$  is the greatest common divisor of all the rational integers of this ring; if further  $\alpha = a_1 + b_1\sqrt{m}$ ,  $\beta = a_2 + b_2\sqrt{m}$ ,  $\dots$ , and if  $i_2$  is the greatest common divisor of  $b_1, b_2, \dots$ , then the basis of the ring ideal  $i_r$  is  $i, i_1 + i_2\omega$ , where  $N(i_1 + i_2\omega) \equiv 0 \pmod{i}$ , since every rational integer that may appear as an element of the ideal  $i$  must be divisible by  $i$ .

It is also seen (Art. 209) that  $N(i_r) = ii_2$ .

However, all the theorems that have been derived for the integers of a realm of rationality  $\mathfrak{R}(\sqrt{m})$  are not at once applicable to the associated ring ideals.

For example in the ring  $\mathfrak{r}(\sqrt{-3})$  the number 4 may be factored in the two ways

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

where  $2, 1 + \sqrt{-3}, 1 - \sqrt{-3}$  are irreducible integers of the ring.

For it may be shown that no rational integral values of  $x, y$  satisfy either of the equations

$$\begin{aligned} (1 + \sqrt{-3}) &= 2(x + y\sqrt{-3}), \\ 2 &= (1 + \sqrt{-3})(x + y\sqrt{-3}). \end{aligned}$$

If we wish to set up the ideal prime factors of 4, we do not find that such a factorization is *unique*, as is the case for the realm  $\mathfrak{R}(\sqrt{-3})$ .

For write

$$i_r = (2, 1 + \sqrt{-3}), \quad i'_r = (2, 1 - \sqrt{-3}).$$

We have at once

$$\begin{aligned} i_r i'_r &= (2^2, 2(1 + \sqrt{-3}), 2(1 - \sqrt{-3}), 4) \\ &= (2)[2, 1 + \sqrt{-3}, 1 - \sqrt{-3}] = (2)(2, 1 + \sqrt{-3}). \end{aligned}$$

Note, however, in the realm  $\mathfrak{R}(\sqrt{-3})$ , that

$$i = (2, 1 + \sqrt{-3}) = (2, 2\omega) = (2),$$

is a principal ideal and that in this realm

$$\frac{1 + \sqrt{-3}}{2} = \omega = \epsilon,$$

say, is a *unit*.

It follows that  $1 + \sqrt{-3} = 2\epsilon$  and  $1 - \sqrt{-3} = 2\epsilon'$ . In general an ideal of the realm  $\mathfrak{R}(\sqrt{m})$  is *not* at the same time a ring ideal; however, there are always an infinite number of realm ideals which are at the same time ring ideals.

ART. 237. The greatest common divisor of *all* realm ideals which are at the same time ring ideals is called the *leader of the ring* or *ring-leader*. This ring-leader for the realms  $\mathfrak{R}(\sqrt{m})$  is the ideal (2).

THEOREM. A realm ideal  $i$  is a ring ideal, if and only if the realm ideal is divisible by the ideal (2).

For if  $i$  is a realm ideal which is divisible by (2) and if

$\mathfrak{i} = (2)\mathfrak{i}_1$ , where  $\mathfrak{i}_1 = (i, i_1 + i_2\omega)$ , then clearly  $\mathfrak{i}$  contains only integers of the ring of the form  $2i, 2i_1 + i_2(1 + \sqrt{m})$  and consequently is a ring ideal. Hence if the realm ideal  $\mathfrak{i} = (a, b + c\sqrt{m})$  is at the same time a ring ideal, then  $a$  must be an even integer, otherwise  $a \cdot \omega = a \frac{1 + \sqrt{m}}{2}$ , which is an integer in the realm ideal, is *not* an integer in the ring ideal. Similarly  $b - c$  must be *even*; otherwise  $(b + c\sqrt{m})\omega'$  [an integer of the realm ideal]

$$= (b - c)\omega' + c\omega'(\sqrt{m} + 1) = (b - c)\omega' + c \frac{1 - m}{2}$$

is *not* an integer of the ring ideal.

From this theorem it follows at once that the ideal (2) is the ring-leader of the ring  $\mathfrak{r}(\sqrt{m})$ .

If  $\mathfrak{i} = (\alpha, \beta, \gamma, \dots)$  is an ideal in  $\mathfrak{R}(\sqrt{m})$ , where  $\alpha = a + a_1\omega, \beta = b + b_1\omega$ , etc., and  $\mathfrak{i}_r = (\alpha, \beta, \gamma, \dots)$  is a ring ideal in  $\mathfrak{r}(\sqrt{m})$ , where  $\alpha = a + a_1\sqrt{m}, \beta = b + b_1\sqrt{m}, \dots$ , the ideal  $\mathfrak{i}$  is the *associate* of the ideal  $\mathfrak{i}_r$ , and if  $\mathfrak{i}$  is *prime* to the ring leader (2), then  $\mathfrak{i}_r$  is called a *regular ring ideal*.

It may be shown that the simple theorems for divisibility, which are true for the realm ideals, are also true of *regular ring ideals*, if the product and quotient of two ring ideals are defined in an analogous manner as they were for the realm ideals.

This is put into evidence through the following two theorems:

**THEOREM.** *If  $\mathfrak{i}$  is an ideal of the realm  $\mathfrak{R}(\sqrt{m})$ , which is prime to the ideal (2), there always exists in the ring  $\mathfrak{r}(\sqrt{m})$  a regular ideal  $\mathfrak{i}_r$  which is associated with the ideal  $\mathfrak{i}$ .*

*Proof.* Let  $\mathfrak{i}$  be the realm ideal

$$\mathfrak{i} = (a, b + c\omega)$$

with basal elements  $a, b + c\omega$ . If further  $\mathfrak{i}$  is prime to (2),  $a$  must necessarily be an odd integer; and as  $a$  is divisible by  $c$  (Art. 206),  $c$  must also be odd.

This being supposed, the ring ideal

$$i_r = (a, 2b + 2c\omega)$$

is associated with the realm ideal  $i$ .

For, due to the fact that

$$-a(b + c\omega) + \frac{a+1}{2}(2b + 2c\omega) = b + c\omega,$$

it is evident that

$$i = \left( a, -a(b + c\omega) + \frac{a+1}{2}(2b + 2c\omega) \right) = \left( a, \frac{a+1}{2}(2b + 2c\omega) \right),$$

and since  $a$  and  $\frac{a+1}{2}$  are relatively prime,

$$\left( a, \frac{a+1}{2}(2b + 2c\omega) \right) = (a, 2b + 2c\omega).$$

ART. 238. THEOREM. *The product of two regular ring ideals is an ideal associated with the product of the associated realm ideals.*

If, as in the preceding proof,

$$i = (a, b + c\omega) \quad \text{and} \quad h = (a_1, b_1 + c_1\omega)$$

are two realm ideals associated with the ring ideals

$$i_r = (a, 2b + 2c\omega) \quad \text{and} \quad h_r = (a_1, 2b_1 + 2c_1\omega),$$

it is seen that

$$\begin{aligned} ih &= (aa_1, a(b_1 + c_1\omega), a_1(b + c\omega), (b + c\omega)(b_1 + c_1\omega)) \\ &= (aa_1, a(2b_1 + 2c_1\omega), a_1(2b + 2c\omega), \\ &\quad 4(b + c\omega)(b_1 + c_1\omega)) = i_r h_r. \end{aligned}$$

For due to the fact that 4 and  $aa_1$  are relatively prime, it is possible to find two integers  $k$  and  $g$  such that

$$maa_1 + g4 = 1.$$

Hence

$$\begin{aligned} kaa_1(b + c\omega)(b_1 + c_1\omega) + g4(b + c\omega)(b_1 + c_1\omega) \\ = (b + c\omega)(b_1 + c_1\omega) \end{aligned}$$

may be added as an element to the last written ideal,

while

$$-aa_1(b+c\omega) + a_1\frac{a+1}{2}(2b+2c\omega) = a_1(b+c\omega)$$

and

$$-a_1a(b_1+c_1\omega) + a\frac{a_1+1}{2}(2b_1+2c_1\omega) = a(b_1+c_1\omega).$$

And when these two expressions have been added as elements, the equality of the above ideals follows.

Observe that  $aa_1$  and  $\frac{a_1+1}{2}a$  have only the common factor  $a$ .

This theorem taken with the preceding theorem shows that every regular ring ideal may be decomposed into a product of regular prime ring ideal factors in *only one way*. It is evident if  $i_r$  is a regular ring ideal and if  $i$  is the associated realm ideal, prime to the ideal (2), that  $i$  may in a unique manner be factored into a product of prime ideals, which are all prime to (2). To each of these prime factors there corresponds a regular ring ideal, and their product is associated with the realm ideal  $i$ . But, as  $i_r$  is the ring ideal associated with  $i$ , it is seen that this product of ring ideals is  $i_r$ .

The norm of a regular ring ideal is equal to the norm of the associated realm ideal, and the theorems regarding the norms of regular ring ideals have their analogies in those of realm ideals.

Two regular ring ideals  $a_r$  and  $b_r$  are equivalent and written  $a_r \sim b_r$ , if there exist in the ring realm  $r(\sqrt{m})$  two integers  $\alpha, \beta$ , so that  $\beta a_r = \alpha b_r$ .

All equivalent ideals belong to a definite class, and there are a finite number of these classes (Art. 218).

Regarding the *units* of the regular ring ideals, the following theorem is proved.



**THEOREM.** *The units of an imaginary ring  $r(\sqrt{m})$  are  $\pm 1$ ; while there are an infinite number of units of every real realm ring which may be expressed through the fundamental unit  $\epsilon_r$  in the form  $\epsilon_r^e$ , where  $e$  takes all possible positive and negative integral rational values.*

*Proof.* It follows from Arts. 99 and 231 regarding realm ideals that it is only necessary to prove the above assertion for real realms and real rings. The proof is given in two parts.

Let  $\frac{m-1}{4}$  be an *even* integer, that is,  $m \equiv 1 \pmod{8}$ , and let  $\epsilon = x + y\omega$  be the fundamental unit in the realm  $\Re(\sqrt{m})$ .

It follows, since

$$N(\epsilon) = \pm 1 = x^2 + xy + \frac{1-m}{4}y^2,$$

that  $y$  is an *even* integer while  $x$  is odd; and consequently

$$\epsilon = x + \frac{y}{2} + \frac{y}{2}\sqrt{m}$$

is also a unit in  $r(\sqrt{m})$  so that  $\epsilon = \epsilon_r$ .

If next  $\frac{m-1}{4}$  is an *odd* integer; so that  $m \equiv 5 \pmod{8}$ ; and if again  $\epsilon = x + y\omega$  is the fundamental unit of  $\Re(\sqrt{m})$ , then from the relation

$$\pm 1 = x^2 + xy + \frac{1-m}{4}y^2,$$

it follows that 1st,  $y$  is even,  $x$  odd; or, 2nd,  $y$  odd,  $x$  even; or, 3rd,  $y$  odd,  $x$  odd. For 1st case  $\epsilon = \epsilon_r$  as above. However, for the 2nd and 3rd cases note that

$$\epsilon^3 = x_1 + y_1\omega$$

is a unit of the ring, since

$$y_1 = 3xy(x+y) + y^3 \left( 1 + \frac{m-1}{4} \right),$$

which is an *even* integer.

Hence for the 2nd and 3rd cases it follows that  $\epsilon_r = \epsilon^3$ . Further note that the norm of the fundamental unit  $\epsilon_r$  is positive or negative according as  $N(\epsilon)$  is positive or negative.

## CHAPTER X

### THE QUADRATIC LAW OF RECIPROCITY AND ITS ANALOGUE IN THE QUADRATIC REALMS

ART. 239. The Realms  $\Re(\sqrt{-1})$ ,  $\Re(\sqrt{2})$ ,  $\Re(\sqrt{-2})$  are Limiting Cases of this law and as such are here considered.<sup>1</sup>

As will be seen in Art. 264, it was a desire to derive the general reciprocity law as Gauss had done for the cubic and biquadratic residues, that led Kummer in his arduous studies of the ideal numbers. And this was an underlying notion of Kronecker in his investigations of the higher forms, and their decomposition into linear factors. It is therefore not out of place to devote some space to the discussion of this Law of Reciprocity and later in Vol. II to the discussion of the Kronecker forms.

ART. 240. **The Realm  $\Re(\sqrt{-1})$ .** Next to the realm of rational numbers the simplest realm is the realm  $\Re(\sqrt{-1})$ . In this realm it has been seen that Euclid's method of finding the greatest common divisor is applicable. Hence (Art. 208) every ideal is a principal ideal.

If an odd prime rational integer is factorable in this realm, it consists of two prime ideals, so that

$$(p) = \mathfrak{p} \cdot \mathfrak{p}';$$

and consequently,

$$p = (x + \sqrt{-1}y)(x - \sqrt{-1}y)$$

<sup>1</sup> With Sommer I follow the treatment of Hilbert, *Bericht der deutschen math. Vereinigung*, Vol. IV, pp. 280 et seq. See also Smith's *Report*, p. 75, and p. 120 for Kummer's Law of Reciprocity.

or

$$p = x^2 + y^2.$$

Since  $p$  is an odd integer, this representation is only possible if, say,  $x$  is odd and  $y$  even; and consequently, a necessary condition for the factoring of  $p$  is  $p \equiv 1 \pmod{4}$ . See also Art. 246.

This condition is also sufficient; that is, if  $p$  is an odd prime integer, such that  $p \equiv 1 \pmod{4}$ , then  $\sqrt{p}$  is factorable in  $\Re(i)$ . For the quadratic realm  $\Re(\sqrt{p})$  has as a fundamental unit  $\epsilon$  whose norm is  $-1$  (see Sommer, p. 109; see also theorem in Art. 235). This carries with it also the consequence that there exists the equation

$$\left(x + \frac{y}{2}\right)^2 - \frac{p}{4}y^2 = -1.$$

It follows that the congruence

$$(2x + y)^2 + 4 \equiv 0 \pmod{p}$$

admits solution. If the rational integer  $z$  is chosen to satisfy the congruence

$$2z \equiv 1 \pmod{p},$$

it is seen through the multiplication of the above congruence by  $z^2$  that

$$X^2 + 1 \equiv 0 \pmod{p}$$

admits solution and *vice versa*.

If  $X = a$  is a solution of this congruence, it is seen that  $p$  may be decomposed into two factors so that

$$(p) = (p, a + i)(p, a - i).$$

Further, since all ideals in this realm are principal ideals, it follows that

$$p = (x + iy)(x - iy).$$

Since a prime number  $p \equiv 3 \pmod{4}$  is irreducible in the realm  $\Re(\sqrt{-1})$ , it follows that the congruence

$$x^2 + 1 \equiv 0 \pmod{p}$$

does *not* admit solution when  $p \equiv 3 \pmod{4}$ .

The integer 2, which is a divisor of the discriminant  $d = -4$  of the realm  $\mathfrak{R}(\sqrt{-1})$ , is decomposable into the two ideal factors  $(2) = (1 + \sqrt{-1})(1 - \sqrt{-1}) = (1 - \sqrt{-1})^2$  in the realm  $\mathfrak{R}(i)$ . In this case  $(1 \pm \sqrt{-1})$  are the *ambiguous* ideals of the realm. We accordingly have the theorem due to Fermat and first proved by Euler, namely (see Kronecker, *Werke*, Vol. 2, pp. 3 et seq.):

*The quadratic congruence*

$$x^2 + 1 \equiv 0 \pmod{p}$$

*admits solution when and only when  $p$  is of the form  $4n+1$ ; or, a number of the form  $x^2+1$  can only have divisors of the form  $4n+1$ .*

In other words

$$\left(\frac{-1}{p}\right) = +1, \quad \text{if } p = 4n+1,$$

and

$$\left(\frac{-1}{p}\right) = -1, \quad \text{if } p \equiv 3 \pmod{4},$$

which statements are connected through the formula

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

The following is a consequence of what has just been proved: If  $m$  is a rational integer which contains prime factors of the form  $p = 4n+3$ , the congruence  $x^2 + 1 \equiv 0 \pmod{m}$  does *not* admit solution; and that is, the Diophantine equations

$$x^2 - my^2 = -1 \quad \text{and} \quad x^2 + xy + \frac{1-m}{4}y^2 = -1,$$

cannot be solved. It follows further that the fundamental unit  $\epsilon$  of a realm  $\mathfrak{R}(\sqrt{m})$ , whose discriminant contains a factor of the form  $4n+3$ , is such that always the norm

$$N(\epsilon) = +1.$$



ART. 241. **The Realm  $\mathfrak{R}(\sqrt{2})$ .** All ideals are principal ideals since the Euclid method of division is applicable. Of particular interest are those rational prime integers which are factorable in this realm.

If  $p$  is an odd prime that is factorable in  $\mathfrak{R}(\sqrt{2})$ , there are two rational integers  $x, y$  which satisfy the equation

$$p = x^2 - 2y^2.$$

The fundamental unit is

$$\epsilon = 1 + \sqrt{2}, \quad N(\epsilon) = -1.$$

It may be proved that if  $p = x^2 - 2y^2$  admits solution, then also  $-p = x_1^2 - 2y_1^2$  admits solution; for we may write

$$(p) = (x + y\sqrt{2})(1 + \sqrt{2})(x - y\sqrt{2})(1 - \sqrt{2}),$$

or

$$-p = (x + 2y)^2 - 2(x + y)^2 = x_1^2 - 2y_1^2.$$

The Diophantine equation  $p = x^2 - 2y^2$ , where  $p$  is an odd prime number, can only be satisfied if  $x$  is odd and  $y$  either even or odd. In the first case

$$p = (2n + 1)^2 - 2(2m)^2 = 4n(n + 1) - 8m^2 + 1,$$

or

$$p \equiv 1 \pmod{8}.$$

In the second case

$$p = (2n + 1)^2 - 2(2m + 1)^2 = 4n(n + 1) - 4m(m + 1) - 1,$$

or

$$p \equiv -1 \pmod{8}.$$

These conditions are *sufficient* for the solution of the equation  $p = x^2 - 2y^2$ ; and that is, for the decomposition of  $p$  into factors. For, write  $p_1 = p$  when  $p \equiv 1 \pmod{8}$  and put  $p_1 = -p$  when  $p \equiv -1 \pmod{8}$ . It follows that  $p_1$  is a prime of the form  $p_1 \equiv 1 \pmod{8}$  and hence from the theorem (see Art. 235), the realm  $\mathfrak{R}(\sqrt{p_1})$  contains an odd number of classes. Further (see Art. 216, Case III), since  $x^2 - p_1 \equiv 0 \pmod{8}$ , the ideal (2) is factorable

in the form  $(2, a + \omega)(2, a + \omega')$ , where  $a$  is a rational integer. It follows that either

$$\mathfrak{p}'\mathfrak{p} = (2) = (2, 1 + \omega)(2, 1 + \omega'), \text{ or } \mathfrak{p}'\mathfrak{p} = (2) = (2, \omega)(2, \omega').$$

Since the number of classes  $h$  is odd, there exists an odd number  $2g + 1$  which is a divisor of  $h$  and for which  $\mathfrak{p}^{2g+1}$  and  $\mathfrak{p}'^{2g+1}$  are principal ideals, so that

$$\mathfrak{p}^{2g+1} = (x + y\omega) \quad \text{and} \quad \mathfrak{p}'^{2g+1} = (x + y\omega').$$

Through multiplication,

$$2^{2g+1} = x^2 + xy + y^2 \frac{1 - p_1}{4}.$$

It follows that

$$(2x + y)^2 - 4 \cdot 2^{2g+1} \equiv 0 \pmod{p_1}.$$

Due to the Fermat Theorem there is a rational integer  $k$  such that  $(2^{2g+2})^k \equiv 1 \pmod{p_1}$ . It is seen through multiplication of the above congruence by  $(2^{2g+2})^{k-1}$ , that

$$z^2 - 2 \equiv 0 \pmod{p_1}.$$

If  $z = a$  is a root of this congruence, it follows that  $(p_1) = (p_1, a - \sqrt{2})(p_1, a + \sqrt{2})$ . Further, since in the realm  $\mathfrak{R}(\sqrt{2})$  there exists only the principal class ( $h = 1$ ), it is seen that

$$(p_1) = (x + y\sqrt{2})(x - y\sqrt{2}).$$

At the same time it is evident that the congruence  $x^2 - 2 \equiv 0 \pmod{p}$  may be solved only when  $p \equiv \pm 1 \pmod{8}$ . Observe that the prime integer 2 admits the factorization  $(2) = (\sqrt{2})(\sqrt{2})$ , as is required in the general theory.

We may now enunciate the following theorem (see also Art. 216, Case III):

**THEOREM.** *The quadratic congruence  $x^2 - 2 \equiv 0 \pmod{p}$  is solvable when and only when  $p \equiv \pm 1 \pmod{8}$ ; and that is, an integer of the form  $x^2 - 2$  has only divisors of the form  $8n \pm 1$ .*

It follows also that  $\left(\frac{2}{p}\right) = +1$ , if  $p$  is an odd prime of the form  $p \equiv \pm 1 \pmod{8}$ ; while  $\left(\frac{2}{p}\right) = -1$ , if  $p \equiv \pm 3 \pmod{8}$ . These two formulas may be expressed in the one formula  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ .

ART. 242. **The Realm  $\mathfrak{K}(\sqrt{-2})$ .** Through similar considerations it may be shown that *the quadratic congruence  $x^2 + 2 \equiv 0 \pmod{p}$  admits solution for odd prime numbers  $p \equiv 1$  and  $p \equiv 3 \pmod{8}$  and is not solvable for  $p \equiv 5$  or  $p \equiv 7 \pmod{8}$* ; and that is,

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}}.$$

We derived in Arts. 240 and 241 the two formulas

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{and} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}};$$

and it also follows at once from the formula

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

that

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}}.$$

ART. 243. **The Quadratic Law of Reciprocity for Odd Rational Prime Integers.** After determining the limiting cases for  $\left(\frac{-1}{p}\right)$  and  $\left(\frac{2}{p}\right)$ , we are next concerned with the value of  $(p/q)$  where  $p$  and  $q$  are any odd primes that are different from each other. Legendre, 1785, and again in 1798, found that

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

which is known as the *Quadratic Law of Reciprocity*.

Euler<sup>1</sup> had already noted that a certain reciprocity existed regarding the possibility of solving the two congruences

$$x^2 - q \equiv 0 \pmod{p} \quad \text{and} \quad x^2 - p \equiv 0 \pmod{q},$$

(see Euler, *opus cit.*, Anal. 1, 1783, p. 64).

The following proof of this law is due essentially to Kummer (*Abh. der Kgl. Akad.*, Berlin, 1861). See also Hilbert, *Zahlbericht*, Chap. XVII, §§ 68-69.

For convenience, denote positive prime integers of the form  $4n+1$  by  $p, p_1, p_2, \dots$ , and let  $q, q_1, q_2, \dots$ , denote positive prime integers of the form  $4n+3$ . Then in the proof the three combinations of integers  $p, p_1; p, q; q, q_1$  are to be considered separately.

FIRST CASE. If the quadratic congruence

$$x^2 - p \equiv 0 \pmod{p_1},$$

admits solution, that is, if  $(p/p_1) = 1$ , then as seen above  $p_1$  in the realm  $\mathfrak{R}(\sqrt{p})$  may be resolved into two different prime ideals so that

$$(p_1) = (p_1, a + \omega)(p_1, a + \omega') = \mathfrak{p}\mathfrak{p}'.$$

Since the number of classes  $h$  in this realm is odd, the discriminant containing only the one prime number  $p_1$ , there is always an odd number  $h_1 = 2g + 1$ , which is a divisor of  $h$ , and is such that the  $h_1$  power of  $\mathfrak{p}$  as well as of  $\mathfrak{p}'$  are principal ideals. Further, the norm of the fundamental unit  $\epsilon$  is  $-1$ . Hence, if  $\mathfrak{p}\mathfrak{p}' = -p_1$ , then is  $N(\epsilon)\mathfrak{p}\mathfrak{p}' = +p_1$ . Accordingly, we may write

$$p_1^{2g+1} = (x + y\omega)(x + y\omega'),$$

or

$$p_1^{2g+1} = (x + y/2)^2 - \frac{p}{4}y^2.$$

<sup>1</sup> For the history of this subject see Kronecker, Vol. II, p. 3, and further see Bachmann, *Niedere Zahlentheorie*, Vol. I, p. 200; Baumgart, *Zeitschrift für Math. u. Physik*, Bd. 30, p. 169; Dirichlet-Dedekind, *Zahlentheorie* (4<sup>th</sup> Edition) p. 95.

From this follows the congruence

$$(2x+y)^2 - p_1(2p_1^2)^2 \equiv 0 \pmod{p};$$

and from this congruence follows as above,

$$z^2 - p_1 \equiv 0 \pmod{p}.$$

It is thus seen that if  $(p/p_1) = +1$ , then is  $(p_1/p) = 1$ .

It also follows further that if  $(p/p_1) = -1$ , then  $(p_1/p) = -1$ ; for if  $(p_1/p) = +1$ , it must necessarily follow that  $(p/p_1) = +1$  contrary to the hypothesis.

SECOND CASE. In the congruence  $x^2 - p \equiv 0 \pmod{q}$ , suppose that  $(p/q) = +1$ , so that  $q$  in the realm  $\Re(\sqrt{p})$  is factorable. It follows that

$$(q) = (q, a + b\omega)(q, a + b\omega').$$

Due to the fact that the number of classes of  $\Re(\sqrt{p})$  is an odd number (see theorem in Art. 235) it is seen that if  $\epsilon$  is the fundamental unit in  $\Re(\sqrt{p})$  that  $N(\epsilon) = -1$ , and as above there exists an equation

$$q^{2g+1} = \left(x + \frac{y}{2}\right)^2 - \frac{p}{4}y^2.$$

From this it is seen that the congruence

$$x^2 - q \equiv 0 \pmod{p},$$

admits solution, and that is, if

$$(p/q) = +1, \quad \text{then is also} \quad (q/p) = +1.$$

Reciprocally, it may be proved that if  $(q/p) = 1$ , then is also  $(p/q) = 1$ . For if  $x^2 - q \equiv 0 \pmod{p}$  admits solution, then due to the fact that

$$(-q/p) = (-1/p)(q/p) = (q/p)(-1)^{\frac{p-1}{2}} = (q/p),$$

it is seen that  $x^2 + q \equiv 0 \pmod{p}$  admits solution. This latter result may be derived independently as follows:

The congruence  $z^2 \equiv -1 \pmod{p}$  is solvable, since  $p$  is of the form  $4n+1$ . If  $z$  is a solution of this congruence, then associated with the congruence  $x^2 - q \equiv 0 \pmod{p}$



there is a second congruence  $(zx)^2 - z^2q \equiv 0 \pmod{p}$ , in which  $z$  is relatively prime to  $p$ , and consequently,  $x^2 + q \equiv 0 \pmod{p}$ . Since,  $(-q/p) = +1$ , it follows that in the imaginary realm  $\Re(\sqrt{-q})$ , the prime integer  $p$  is factorable and since  $-q \equiv 1 \pmod{4}$ , and as the norm of an integer in an imaginary realm is always positive, it follows as above that  $x^2 - p \equiv 0 \pmod{q}$  admits solution.

It has thus been shown that if

$$(a) \quad (p/q) = +1, \quad \text{then also is} \quad (q/p) = +1;$$

and if

$$(b) \quad (q/p) = +1, \quad \text{then also is} \quad (p/q) = +1.$$

And from this it is seen at once that if  $(p/q) = -1$ , then also  $(q/p) = -1$ ; for if  $(q/p) = +1$ , then from what was just proved  $(p/q) = +1$ , and *not*  $-1$ .

THIRD CASE. Let the two prime numbers be  $q$  and  $q_1$ . If in the first place  $(q/q_1) = -1$ , then is  $(-q/q_1) = +1$ , since  $(-q/q_1) = (-1/q_1)(q/q_1)$  and  $(-1/q_1) = -1$ . The prime number  $q_1$  is factorable in the imaginary realm  $\Re(\sqrt{-q})$ , and as  $-q \equiv 1 \pmod{4}$ , the discriminant of this realm consists of only one prime factor. The number of classes is odd, and as in the preceding case  $(q_1/q) = +1$ .

In the second place suppose that  $(q/q_1) = +1$ , then the fact that  $(q_1/q) = -1$  does *not* follow from the preceding methods. A proof, however, as given by Hilbert, *loc. cit.*, is had, if we consider the realm  $\Re(\sqrt{qq_1})$ . For this realm it is seen that  $m = qq_1 \equiv 1 \pmod{4}$ , and the discriminant of the realm is  $D = qq_1$ . In this realm (end of Case III, Art. 216) the only prime numbers that are divisible by the square of prime ideals are  $q$  and  $q_1$ . Write  $(q) = q^2$  and  $(q_1) = q_1^2$ . Here  $q$ ,  $q_1$  and  $qq_1 = \sqrt{qq_1} = \sqrt{m}$  are the only ambiguous ideals. It is evident that  $qq_1$  is a principal ideal. It may be shown as follows that  $q$  and  $q_1$  are also principal ideals.

Let  $\epsilon$  be the fundamental unit in  $\mathfrak{R}(\sqrt{qq_1})$ , where (Art. 240, end)  $N(\epsilon) = +1$ . Hence due to the theorem in Art. 234, there is a number  $\alpha$  of the realm  $\mathfrak{R}(\sqrt{qq_1})$  which is not rational, but is such that  $\epsilon = \frac{\alpha}{\alpha'}$ . It follows that  $(\alpha) = (\alpha)'$ , and that every ideal which is a divisor of  $(\alpha)$  is also a divisor of  $(\alpha)'$ . Suppose then that (1),  $(\alpha)$  is of the form  $\eta a$  where  $\eta$  is a unit of the realm and  $a$  a rational number, or (2), suppose that  $(\alpha) = \eta\sqrt{qq_1}$ . In the first case

$$\epsilon = \frac{\alpha}{\alpha'} = \frac{\eta a}{\eta' a} = \pm \eta^2,$$

and in the second,

$$\epsilon = \frac{\eta\sqrt{qq_1}}{\eta'\sqrt{qq_1}} = \pm \eta^2;$$

and this is a contradiction to the assumption that  $\epsilon$  is a fundamental unit of  $\mathfrak{R}(\sqrt{qq_1})$ . Hence the only other forms that  $(\alpha)$  can have are  $(\alpha) = (a)q$  and  $(\alpha) = (a)q_1$  and in either case  $q \sim 1$ ,  $q_1 \sim 1$ . It follows by taking the norm of  $q$ , that

$$\pm q_1 = (x + y/2)^2 - \frac{qq_1}{4}y^2,$$

or

$$\pm 4q_1 = (2x + y)^2 - qq_1y^2.$$

This Diophantine equation may be solved only if  $2x + y$  is divisible by  $q_1$ . It may therefore be written more simply

$$\pm 4 = q_1X^2 - qY^2. \quad (i)$$

To determine the sign of the left-hand side we may make use of the assumption that  $(q/q_1) = 1$ . Writing equation (i) in the form of a congruence, it is seen that

$$qY^2 \pm 4 \equiv 0 \pmod{q_1},$$

or

$$Y_1^2 \pm 4q \equiv 0 \pmod{q_1}.$$

Hence, in virtue of the assumption it is seen that the *minus* sign is to be taken. It then follows from (i) that

$$-4 = q_1X^2 - qY^2,$$

or

$$q_1X^2 \equiv -4 \pmod{q}, \quad \text{or} \quad X_1^2 \equiv -4q_1 \pmod{q},$$

and finally,

$$X_1^2 + 4q_1 \equiv 0 \pmod{q}.$$

Thus with the assumption  $(q/q_1) = +1$ , we have necessarily  $(-q_1/q) = +1$ , or  $(q_1/q) = -1$ .

To repeat the results thus established, we have simultaneously

$$(q/q_1) = +1 \quad \text{and} \quad (q_1/q) = -1$$

and further

$$(q/q_1) = -1 \quad \text{and} \quad (q_1/q) = +1.$$

With this is established completely, the reciprocal relations between the prime numbers  $q$  and  $q_1$ .

ART. 244. The above results combined may be stated in the theorem.

THEOREM. *If  $p$  and  $q$  are any odd positive prime integers, their mutual residue character is expressed through the Legendre formula*

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

with the limiting cases

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

See also H. J. S. Smith, Vol. I, pp. 55 et seq. and Wertheim, *Anfangsgründe der Zahlentheorie*, pp. 320–22.<sup>1</sup>

<sup>1</sup> Among the references to the treatment of the quadratic law of reciprocity in the quadratic realms mention may be made of the following:

D. Hilbert, *Math. Annalen*, Vol. 51, pp. 1–127, and *Gött. Nachrichten*, 1898.

*Das allgemeine quadratische Reziprocitätsgesetz*, etc., by K. S. Hilbert. Göttingen Dissertation, 1900.

## EXAMPLES OF THE LAW OF RECIPROCITY

1. Due to the formula

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right),$$

it is seen that

$$\left(\frac{6}{7}\right) = \left(\frac{2}{7}\right) \left(\frac{3}{7}\right) = \left(\frac{3}{7}\right).$$

Further,

$$\left(\frac{3}{7}\right) \left(\frac{7}{3}\right) = -1, \quad \text{so that} \quad \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

2.

$$(27/17) = (10/17) = (2/17)(5/17) = (5/17).$$

$$(5/17)(17/5) = 1, \quad \text{so that} \quad (5/17) = (17/5) = (2/5) = -1.$$

3. Show that

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right) \left(\frac{73}{1847}\right) = +1$$

$$\left(\frac{601}{1013}\right) = 1 \quad \text{and that} \quad \left(\frac{402}{929}\right) = +1.$$

4. Show that

$$\left(\frac{x}{7}\right) = -1, \quad \text{for} \quad x = 73, 97, 241, 313, 409;$$

and

$$\left(\frac{x}{11}\right) = -1, \quad \text{for} \quad x = 193, 337, 457, 673.$$

5. Show that the solutions of  $\left(\frac{x}{41}\right) = 1$  are

$$x = 82n + \begin{cases} 1, & 5, & 9, & 21, & 23, & 25, & 31, & 33, & 37, & 39, \\ 81, & 77, & 73, & 61, & 59, & 57, & 51, & 49, & 45, & 43, \end{cases}$$

where  $n$  is any integer.

*Quadratische Reciprocitätsgesetze in algebraischen Zahlkörpern.* By Gottfried Ruckle. Göttingen Dissertation (1901).

*Das quad. Reciprocitätsgesetz im quadratischen Zahlkörper mit der Classenzahl 1.* Göttingen Dissertation (1898) by Heinrich Dörrie.

*Der Klassenkörper der quad. Körper, etc.* Göttingen Dissertation (1903) by Rudolf Fueter.

Various papers by Ph. Furtwängler in the *Abhand. und Nach. von der Kgl. Ges. der Wissenschaften zu Göttingen*. See also *Math. Annalen*, Vol. 63.

6. Show that the solutions of  $\left(\frac{x}{59}\right) = -1$  are

$$x = 118n + \begin{cases} 11, 13, 23, 31, 33, 37, 39, 43, 47, 55, 61, 65, 67, 69, 73, \\ 77, 83, 89, 91, 93, 97, 99, 101, 103, 109, 111, 113, 115, 117. \end{cases}$$

ART. 245. A generalized form of the Law of Reciprocity due to Jacobi<sup>1</sup> (*Werke*, Vol. VI, p. 262) is as follows.

If  $p, q, r, \dots$ , are any positive integers that are relatively prime to the integer  $a$ , we may introduce by definition the symbolic equality

$$\left(\frac{a}{p \cdot q \cdot r \cdot \dots}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) \left(\frac{a}{r}\right) \dots$$

Then, if  $P$  and  $Q$  are any factorable integers that are relatively prime, it may be proved that

$$\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.$$

ART. 246. **Expressions of Integers through Sums of Squares.** Through the factoring of numbers in special realms it is possible to derive by means of the theory of ideals certain interesting theorems which have been known for a long time. Possibly others may be discovered in this manner.

I. *The Realm  $\mathfrak{R}(i)$ .* (1) In Art. 240 it was shown that in the realm  $\mathfrak{R}(\sqrt{-1})$  every rational prime integer of the form  $p = 4n + 1$ , and  $p = 2$  were essentially factorable in only one way in the form

$$p = (x + \sqrt{-1}y)(x - \sqrt{-1}y),$$

and that any other factors differed only from the numbers  $x \pm \sqrt{-1}y$  by multiples of  $\pm 1$  or  $\pm \sqrt{-1}$ . Otherwise formulated, this means that every prime number of the

<sup>1</sup> Jacobi, *Ueber die Kreistheilung*, etc. *Monatsbericht der Akad. der Wiss. zu Berlin*, Oct. 16, 1837, pp. 127-136; *Crelle*, Vol. 30, pp. 166-182. See also *Report on Alg. Nos.*, p. 72.



form  $p=4n+1$  or  $p=2$  may be expressed as the sum of two squares  $p=x^2+y^2$  in *essentially only one way*. Dickson<sup>1</sup> refers to this as Girard's Theorem. That the theorem was known in the time of Diophantus, see Jacobi, Vol. VII, p. 332.

The derivation of the two numbers  $x$  and  $y$  was done by Legendre<sup>1</sup> by developing  $\sqrt{p}$  in a continued fraction.

If one wishes to derive by trial the integers  $x$  and  $y$ , the following observation may shorten the work.

From the equation  $p=x^2+y^2$ , it follows that

$$(1) \quad (zx)^2+1 \equiv 0 \pmod{p},$$

where  $z$ , reduced  $\pmod{p}$  lies between  $-p/2$  and  $+p/2$ . If  $w$  is a solution of the congruence (1), it is seen that  $x$  must be a divisor of  $w+ap$ , where  $a$  is a rational integer.

It is clear that  $x$  is not larger than  $\sqrt{\frac{p}{2}}$  and that  $a$  must be such that  $w+ap$  is situated between  $-\frac{p}{2}\sqrt{\frac{p}{2}}$  and  $+\frac{p}{2}\sqrt{\frac{p}{2}}$ .

(2) If  $p$  and  $p_1$  are any two odd prime integers of the form  $4n+1$ , then in the realm  $\Re(\sqrt{-1})$

$$p = (x+iy)(x-iy),$$

$$p_1 = (x_1+iy_1)(x_1-iy_1).$$

There are two combinations of these factors, the one being

$$pp_1 = \{(x+iy)(x_1+iy_1)\} \{(x-iy)(x_1-iy_1)\}$$

$$= (X+iY)(X-iY)$$

and the other

$$pp_1 = \{(x+iy)(x_1-iy_1)\} \{(x-iy)(x_1+iy_1)\}$$

$$= (X_1+iY_1)(X_1-iY_1).$$

Thus it is seen that the product  $pp_1$  may be expressed as the sum of two squares in two essentially different ways.

<sup>1</sup> See Dickson, *History of the Theory of Numbers*, Vol. II, p. 228; see also p. 234. A table for the values of  $x$  and  $y$  is given for the primes from 1 to 12,000 by Jacobi, Vol. VI, pp. 265 et seq.

If

$$p_1 = 2 = (1+i)(1-i),$$

then is

$$2p = (1+i)(1-i)(x+iy)(x-iy);$$

and since  $1+i=i(1-i)$ , it follows that  $2p$  may be expressed as the sum of two squares in only one way.

II. *The Realm*  $\Re(\sqrt{-2})$ . In this realm the only units are  $\pm 1$  and the number of classes  $h$  is  $= 1$ . Observe that  $p = 2 = -(\sqrt{-2})^2$  while every rational prime integer of the form  $8n+1$ , or  $8n+3$  is factorable as the product of two different prime numbers in essentially only one way and of the form (see Art. 242)

$$p = (x + \sqrt{-2}y)(x - \sqrt{-2}y).$$

And this otherwise formulated is:

*Every positive odd prime integer  $p$  of the form  $8n+1$  or  $8n+3$  may be expressed in only one way in the form*

$$p = x^2 + 2y^2,$$

where  $x$  and  $y$  are rational integers.

Values of  $x$  and  $y$  for  $p$  of the form  $8n+1$  are given by Jacobi, Vol. VI, p. 271.

III. *The Realm*  $\Re(\sqrt{-3})$ . Here again  $h=1$ . If  $p = x^2 + 3y^2$ , then there is an integer  $z$ , such that  $pz^2 = X^2 + 3$ , or  $X^2 + 3 \equiv 0 \pmod{p}$ . Further observe that

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Hence in order that  $p$  be factorable,  $p$  must be of the form  $p = 3n+1$ . And  $p$  being of this form, the equation

$$p = \left(x + y \frac{1 + \sqrt{-3}}{2}\right) \left(x + y \frac{1 - \sqrt{-3}}{2}\right)$$

may be satisfied in only one way, where  $x$  is an odd and  $y$  an even integer.

Noting that  $\frac{-1 \pm \sqrt{-3}}{2}$  are the cubic roots of unity

$= \omega, \omega^2$ , say, write

$$p = (a + b\omega)(a + b\omega^2),$$

or

$$p = \{\omega(a + b\omega)\} \{(a + b\omega^2)\omega^2\},$$

$$p = \{\omega^2(a + b\omega)\} \{(a + b\omega^2)\omega\},$$

etc. Then the condition that  $x$  be odd and  $y$  even is satisfied:

- (1) for  $a + b\omega$  ( $a$  being even,  $b$  odd),
- (2) for  $(a + b\omega)\omega^2$  ( $a$  being odd,  $b$  even),
- (3) for  $(a + b\omega)\omega = -b + (a - b)\omega$  (where  $a$  and  $b$  are both odd).

Otherwise expressed, there is only one way of factoring a prime integer  $p \equiv 1 \pmod{3}$  in the form

$$p = (x + y\sqrt{-3})(x - y\sqrt{-3});$$

and that is:

*Every rational prime integer  $p$  of the form  $3n + 1$  may always and in only one way be expressed in the form*

$$p = x^2 + 3y^2.$$

These theorems may be extended to the exposition of factorable rational integers through the form  $x^2 + 2y^2$  and  $x^2 + 3y^2$ ,  $x^2 + my^2$ . By means of the theory of ideals innumerable special cases<sup>1</sup> for the presentation of integers through the forms  $x^2 + my^2$  may be derived. This is treated later when the relations existing between the composition of forms and the theory of ideals is given (Art. 283). For primes of the form  $3n + 1$  see Jacobi's table in Jacobi's *Werke*, Vol. VI, p. 268.

IV. *The Realm  $\Re(\sqrt{2})$ .* In this realm  $h = 1$ , while there are an indefinite number of units derived by raising the fundamental unit  $\epsilon = 1 + \sqrt{2}$  to different integral powers. In this realm prime integers  $p$  of the form  $8n + 1$  and  $8n + 7$  are factorable (Art. 241).

<sup>1</sup> See Dickson, *History*, etc., Vol. III, p. 3, where many references are found.

From the factoring of  $(p)$  into its prime ideal factors, namely,

$$(p) = (x + y\sqrt{2})(x - y\sqrt{2})$$

combined with the units of the realm there arise an infinite number of expressions of the numbers  $p$  in the form  $x^2 - 2y^2$ . For if  $p = x^2 - 2y^2$ , then is

$$-p = (x + 2y)^2 - 2(x + y)^2$$

(Art. 241). Further since

$$-p = (x + y\sqrt{2})\epsilon(x - y\sqrt{2})\epsilon',$$

it is seen that

$$-p = (x - 2y)^2 - 2(x - y)^2.$$

And writing

$$p = (x + y\sqrt{2})\epsilon^2(x - y\sqrt{2})\epsilon'^2,$$

we also have

$$p = (3x + 4y)^2 - 2(2x + 3y)^2.$$

And thus we have the theorem:

*Every positive or negative prime integer, which when taken positive is of the form  $8n \pm 1$ , may be expressed in an infinite number of ways in the form  $x^2 - 2y^2$ , and all the different ways are had from a single way through application of the units  $\pm \epsilon^k$  of the realm,  $k$  a positive integer.*

In this connection many other interesting examples are found in Legendre, *Théorie des nombres*, Vol. I, Second Part. See also Dickson, *History of the Theory of Numbers*, Vol. II, p. 255; Vol. III, p. 55; Cunningham (*Tables. Quadratic Partitions*. London) for values of  $x, y$  in  $p = x^2 + y^2$ ,  $p = x^2 \pm 2y^2$ ,  $p = x^2 + ry^2$  ( $r = -5, 7, 3, -3, +5$ , etc.).

#### HILBERT'S SYMBOL FOR NORM-RESIDUES <sup>1</sup>

ART. 247. Having distributed the ideals into classes the next step in the classification is to distribute the

<sup>1</sup> Hilbert, p. 286.

classes into genera (Gauss, *Disq. Arith.*), this being an extension in the quadratic realm of an analogous distribution and classification in the realm of rational integers. This classification is simplified through the introduction of a symbol that is an extension of Legendre's symbol and due to Hilbert (*Zahlbericht*, Chap. 17, §§ 64–66, 70, and Chap. 18, §§ 71–78).

DEFINITION. Let  $p$  be a positive rational prime integer, while  $m, n$  are two arbitrary rational integers, the only restriction being that  $m$  must not contain a squared factor. If further there are algebraic integers  $\alpha$  of the realm  $\mathfrak{R}(\sqrt{m})$  such that  $n \equiv N(\alpha) \pmod{p^e}$  for every rational positive integer  $e$ , then this fact is denoted by putting the symbol

$$\left(\frac{n, m}{p}\right) \text{ equal to } +1.$$

If, however, there is no integer  $\alpha$  of the realm  $\mathfrak{R}(\sqrt{m})$  which is such that

$$n \equiv N(\alpha) \pmod{p},$$

and if the congruence

$$n \equiv N(\alpha) \pmod{p^e}$$

cannot be satisfied by integers of the realm for every positive integral value of  $e$ , this fact is denoted by putting

$$\left(\frac{n, m}{p}\right) = -1.$$

In the first case the rational integer  $n$  is called a *norm-residue* and in the second case a *norm-non-residue* of the realm  $\mathfrak{R}(\sqrt{m})$  with respect to  $p$  as a modulus. As in the case of the Legendre symbol, there are certain properties of the Hilbert symbol which simplify computation in numerical examples. Before expressing these properties in definite rules we may make the following remarks.



I. In the realm  $\mathfrak{R}(\sqrt{m})$  observe that

$$N(\alpha) = (x - \sqrt{m}y)(x + \sqrt{m}y), \quad \text{if} \quad m \not\equiv 1 \pmod{4}.$$

Hence, if

$$n_1 \equiv (x - \sqrt{m}y)(x + \sqrt{m}y) \pmod{p^e},$$

then also

$$n = k^2 n_1 \equiv (kx - \sqrt{m}ky)(kx + \sqrt{m}ky) \pmod{p^e}.$$

It follows that

$$\left(\frac{n, m}{p}\right) = \left(\frac{n_1, m}{p}\right) \quad \text{if} \quad n = k^2 n_1,$$

where  $k$  is a rational integer. And it is evident that the formula is also true when  $m \equiv 1 \pmod{4}$ .

II. Of the numbers that form a complete system of incongruent residues with respect to  $p$  as a modulus, namely,  $1, 2, \dots, p-1$ , half are residues  $\pmod{p}$  and the other half are non-residues  $\pmod{p}$ . See Dirichlet-Dedekind, § 33 (4<sup>th</sup> Edition). Denote the residues by  $r_1, r_2, \dots, r_{\frac{p-1}{2}}$  and the non-residues by  $n_1, n_2, \dots, n_{\frac{p-1}{2}}$ .

If any one of the non-residues be denoted by  $n$ , then among the differences  $d_1 = r_1 - n, d_2 = r_2 - n, \dots, d_{\frac{p-1}{2}} = r_{\frac{p-1}{2}} - n$ , there is at least one non-residue  $\pmod{p}$ .

This is evident for the case  $n = 3$ . If  $p$  is  $> 3$ , observe that no two of the  $d$ 's can be congruent  $\pmod{p}$ . It follows that no two of the  $d$ 's can be congruent to one and the same residue.

Suppose next that all the  $d$ 's were quadratic residues, so that, say,

$$d_1 \equiv r_{k_1} \pmod{p},$$

where  $r_{k_1}$  is to be found among the  $r$ 's above. Hence,

$$r_1 - n \equiv r_{k_1} \pmod{p},$$

or,

$$n \equiv r_1 - r_{k_1} \pmod{p};$$

and similarly,

$$\begin{aligned} n &\equiv r_2 - r_{k_2} \pmod{p}, \\ &\dots\dots\dots \\ n &\equiv r_{\frac{p-1}{2}} - r_{k_{\frac{p-1}{2}}} \pmod{p}, \end{aligned}$$

where  $r_{k_1}, r_{k_2}, \dots, r_{k_{\frac{p-1}{2}}}$  is the same system of residues  $\pmod{p}$  neglecting the order as  $r_1, r_2, \dots, r_{\frac{p-1}{2}}$ . Through addition it is seen that

$$n \frac{p-1}{2} \equiv 0 \pmod{p},$$

which is not true since neither  $n$  nor  $\frac{p-1}{2}$  is divisible by  $p$ . It follows that at least one of the  $d$ 's must be a non-residue. We may show that at least one of the  $d$ 's is a residue. For, assuming that they are all non-residues, it is seen that

$$\begin{aligned} d_1 = r_1 - n &\equiv n_{k_1} \\ r_2 - n &\equiv n_{k_2} \\ &\cdot \\ &\cdot \\ &\cdot \\ r_{\frac{p-1}{2}} - n &\equiv n_{k_{\frac{p-1}{2}}}. \end{aligned}$$

Observing (see Dirichlet-Dedekind, § 43) that

$$r_1 + r_2 + \dots + r_{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

as is also the sum

$$n_{k_1} + n_{k_2} + \dots + n_{k_{\frac{p-1}{2}}} \equiv 0 \pmod{p},$$

it follows through adding the above congruences that

$$-n \frac{p-1}{2} \equiv 0 \pmod{p}.$$

And this is *not* true.

Similarly if  $r$  is any one of the  $\frac{p-1}{2}$  residues  $r_1, r_2, \dots, r_{\frac{p-1}{2}}$ , then among the differences  $r_i \pm r, n_i \pm n, n_i - r$ , some are residues and some non-residues (mod.  $p$ ).

ART. 248. The signs which are to be associated with the Hilbert symbol are determined by means of the four theorems which follow.

THEOREM I. *If  $n, m$  are two rational integers while  $p$  is an odd prime integer which is a factor of neither  $n$  nor  $m$ , then is*

$$(A) \quad \left(\frac{n, m}{p}\right) = +1,$$

$$(B) \quad \left(\frac{n, p}{p}\right) = \left(\frac{p, n}{p}\right) = \left(\frac{n}{p}\right).$$

*If further both  $n$  and  $m$  are divisible by the first power only of  $p$ , then is*

$$(C) \quad \left(\frac{n, m}{p}\right) = \left(\frac{-nm}{p^2}\right).$$

*Proof of (A).* First let  $m \equiv 2 \pmod{4}$  or  $m \equiv 3 \pmod{4}$ . The first theorem asserts that

$$n \equiv x^2 - my^2 \pmod{p},$$

or

$$x^2 - my^2 - n \equiv 0 \pmod{p}, \tag{i}$$

admits solution in rational integral values of  $x, y$ .

1. Consider the case  $\left(\frac{n}{p}\right) = +1, \left(\frac{m}{p}\right) = \pm 1$ . A solution is at once offered by taking  $y \equiv 0 \pmod{p}$  and for  $x$  any value that satisfies the congruence  $x^2 \equiv n \pmod{p}$ .

2. Take next the cases  $\left(\frac{m}{p}\right) = 1, \left(\frac{n}{p}\right) = \pm 1$ . In these cases we may write  $m \equiv z^2 \pmod{p}$ , where  $z$  is a definite

rational integer and then (i) takes the form

$$x^2 - z^2y^2 - n \equiv 0 \pmod{p}. \quad (\text{ii})$$

Since  $n \equiv n_1 \pmod{p}$ , where  $n_1$  may always be taken as an odd integer, we may always choose  $y$  so that

$$zy \equiv \frac{n_1 - 1}{2} \pmod{p},$$

and  $x$  so that

$$x \equiv \frac{n_1 + 1}{2} \pmod{p}.$$

These values satisfy (ii) and therefore also (i).

3. The remaining case is had when  $\left(\frac{n}{p}\right) = -1$ ,  $\left(\frac{m}{p}\right) = -1$ .

Observe that a non-residue multiplied by a residue is always a non-residue, while the product of two non-residues is a residue. Hence the product  $my^2$  for the integers  $y=1, 2, \dots, p-1$ , goes over all non-residues  $\pmod{p}$  twice. And when for  $x$  all the residues  $\pmod{p}$  are substituted successively in  $x^2 - n$ , there is at least one non-residue (see previous article). And thus it is seen that (ii) admits solution in this remaining case.

If  $m \equiv 1 \pmod{4}$ , theorem (A) resolves itself into proving that

$$n \equiv \left(x + \frac{y}{2}\right)^2 - \frac{m}{4}y^2 \pmod{p},$$

or that the congruence

$$4n \equiv (2x + y)^2 - my^2 \pmod{p},$$

admits solution.

The above proofs are at once applicable and with them it is proved that for the first power of  $p$ , there exists always an integer  $\alpha$  of the realm  $\Re(\sqrt{m})$  such that

$$n \equiv N(\alpha) \pmod{p}.$$

It remains finally to prove that there is an integer  $\alpha$  in the realm  $\Re(\sqrt{m})$  which is such that  $n \equiv N(\alpha) \pmod{p^e}$ ,

where  $p^e$  is any positive power of  $p$ . The proof is one of induction.

Suppose that  $\alpha_1 = a + b\omega$  is an integer of the realm  $\mathfrak{R}(\sqrt{m})$  for which the congruence  $n \equiv N(\alpha_1) \pmod{p^{e-1}}$  is satisfied.

1. When  $m \not\equiv 1 \pmod{4}$ ,  $a^2 - mb^2 - n = gp^{e-1}$ , where  $g$  is a rational integer. Further, in the expression  $x^2 - mb^2 - n$ , put  $x = a + up^{e-1}$ ,  $y = b + vp^{e-1}$ , and choose  $u$  and  $v$  such that  $2ua - 2mbv + g \equiv 0 \pmod{p}$ . It is clear that

$$n \equiv N(x + y\omega) \pmod{p^e}.$$

2. A similar proof is applicable when  $m \equiv 1 \pmod{4}$ . Thus it is proved that if there exists an integer  $\alpha_1$  in  $\mathfrak{R}(\sqrt{m})$  such that  $n \equiv N(\alpha_1) \pmod{p^{e-1}}$ , it is possible to determine two rational integers  $x, y$  such that

$$n \equiv N(x + \omega y) \pmod{p^e}.$$

As it was shown that there is always an integer  $\alpha$  such that  $n \equiv N(\alpha) \pmod{p}$ , it is seen that the congruence  $n \equiv N(x + \omega y) \pmod{p^e}$  may always be satisfied; and this fact is denoted by the symbol  $\left(\frac{n, m}{p}\right) = 1$ .

ART. 249. *Proof of (B)*. If  $m = p$ , the congruences  $x^2 - py^2 - n \equiv 0 \pmod{p^e}$ , when  $p \not\equiv 1 \pmod{4}$ ,  $(2x + y)^2 - py^2 - 4n \equiv 0 \pmod{p^e}$ , when  $p \equiv 1 \pmod{4}$ , admit solutions for all positive integral values of  $e$ , if and only if  $\left(\frac{n}{p}\right) = 1$ , and cannot be solved if  $\left(\frac{n}{p}\right) = -1$ .

If  $n = p$ , the congruences  $x^2 - my^2 - p \equiv 0 \pmod{p^e}$  and  $(2x + y)^2 - my^2 - 4p \equiv 0 \pmod{p^e}$  may be solved when and only when  $x^2 - my^2 \equiv 0 \pmod{p}$ , or  $(2x + y)^2 - my^2 \equiv 0 \pmod{p}$ , and that is when  $\left(\frac{m}{p}\right) = 1$ . It follows that

$$\left(\frac{n, p}{p}\right) = \left(\frac{p, n}{p}\right) = \left(\frac{n}{p}\right).$$



The theorem is at once applicable if  $n$  or  $m$  is divisible by  $p$ , say  $n = n_1 p$ . It is seen that

$$\left(\frac{pn_1, m}{p}\right) = \left(\frac{m, pn_1}{p}\right) = \left(\frac{m}{p}\right).$$

*Proof of (C).* If both  $m$  and  $n$  are divisible by  $p$ , say  $m = pm_1$ ,  $n = pn_1$ , but neither of them by  $p^2$ , then the congruences in question  $x^2 - my^2 - n \equiv 0 \pmod{p^e}$ , and  $(2x + y)^2 - my^2 - 4n \equiv 0 \pmod{p^e}$ , admit solution when and only when a congruence of the form  $pX^2 - m_1Y^2 - n_1 \equiv 0 \pmod{p}$  exists. And the necessary and sufficient condition for this is, as shown above, that

$m_1Y^2 + n_1 \equiv 0 \pmod{p}$  or  $(m_1Y)^2 + m_1n_1 \equiv 0 \pmod{p}$ ,  
a condition which is denoted by the symbol  $\left(\frac{-m_1n_1}{p}\right) = 1$ .

It has thus been proved that

$$\left(\frac{n, m}{p}\right) = \left(\frac{-nm}{p^2}\right).$$

**THEOREM II.** *If  $m$  and  $n$  are two arbitrary rational odd integers, the following relations exist*

$$(A) \quad \left(\frac{n, m}{2}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}},$$

$$(B) \quad \left(\frac{n, 2}{2}\right) = \left(\frac{2, n}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

In the proof of Formula (A) we have to show that there exist solutions of the congruences

$$(1) \quad x^2 - my^2 - n \equiv 0 \pmod{2^e}, \quad \text{if } m \not\equiv 1 \pmod{4},$$

and

$$(2) \quad x^2 + xy + \frac{1-m}{4}y^2 - n \equiv 0 \pmod{2^e}, \quad \text{if } m \equiv 1 \pmod{4};$$

while in the proof of Formula (B) it is necessary to show that there are solutions of the congruences

$$(3) \quad x^2 - 2y^2 - n \equiv 0 \pmod{2^e},$$

and of

$$(4) \quad x^2 - ny^2 - 2 \equiv 0 \pmod{2^e}, \quad \text{if } n \not\equiv 1 \pmod{4},$$

$$(5) \quad x^2 + xy + \frac{1-n}{4}y^2 - 2 \equiv 0 \pmod{2^e}, \quad \text{if } n \equiv 1 \pmod{4}.$$

It is evident that all of the above congruences may be solved for  $e=1$ . We first show that they may be solved also for any value of  $e$  greater than 3, if they permit solution for  $e=3$ .

Suppose for example that  $x=a, y=b$ , is a solution of the congruence

$$x^2 - my^2 - n \equiv 0 \pmod{2^3}$$

and that  $a^2 - mb^2 - n$  is *not* divisible by  $2^4$ . Write  $x = a + 2^2u, y = b + 2^2v$ . It follows that

$$x^2 - my^2 - n = a^2 - mb^2 - n + 8(au - mbv) + 16(u^2 - mv^2),$$

and consequently,

$$x^2 - my^2 - n \equiv 0 \pmod{2^4}$$

provided

$$\frac{a^2 - mb^2 - n}{8} + au - mbv \equiv 0 \pmod{2},$$

and that is,

$$1 + au - mbv \equiv 0 \pmod{2}.$$

Since either  $a$  or  $b$  must be an odd integer this last congruence admits solution. Similarly, if  $a_1$  and  $b_1$  are solutions of

$$x^2 - my^2 - n \equiv 0 \pmod{2^4},$$

we may derive solutions of this congruence when the modulus is  $2^5, 2^6, \dots$ .

Next suppose that  $x=a, y=b$ , is a solution of the congruence

$$x^2 + xy + \frac{1-m}{4}y^2 - n \equiv 0 \pmod{2^3}.$$

Write  $x = a + 8u$  and  $y = b + 8v$  and determine  $u$  and  $v$  such

that

$$av + bu + 1 \equiv 0 \pmod{2}.$$

The corresponding values of  $x$  and  $y$  satisfy the congruence

$$x^2 + xy + \frac{1-m}{4}y^2 - n \equiv 0 \pmod{2^4}.$$

It only remains to determine what values of  $m$  and  $n$  satisfy the congruences

$$\begin{aligned} x^2 - my^2 - n &\equiv 0 \pmod{8}, \\ x^2 + xy + \frac{1-m}{4}y^2 - n &\equiv 0 \pmod{8}. \end{aligned}$$

These may be put down in a table,<sup>1</sup> the even integers being added for future reference. The values are, of course, given for  $m$  and  $n \pmod{8}$ . The values of  $n$  are those for which the corresponding congruences are solvable.

$m$	$n$
1	1, 3, 5, 7, 2, 6
2	1, 7, 2
3	1, 5, 6
5	1, 3, 5, 7
6	1, 3, 6
7	1, 5, 2

And from this table it is seen when  $m$  and  $n$  are odd that

$$\left(\frac{n, m}{2}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

For example,

$$\left(\frac{3, 5}{2}\right) = (-1)^2 = +1,$$

<sup>1</sup> Hilbert, *Bericht*, p. 290; Sommer, *Vorlesungen*, p. 135.

showing that there is a solution of the associated congruence; while

$$\left(\frac{7, 3}{2}\right) = (-1)^3 = -1,$$

and the corresponding congruence does not admit solution.

When  $n$  is an odd integer it is seen that

$$\left(\frac{2, n}{2}\right) = \left(\frac{n, 2}{2}\right) = +1$$

or  $-1$ , according as  $n \equiv \pm 1 \pmod{8}$  or  $n \equiv \pm 3 \pmod{8}$ . And this is

$$(B) \quad \left(\frac{2, n}{2}\right) = \left(\frac{n, 2}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

The above table may be used for a discussion of the cases where  $p=2$  and  $m$  or  $n$  as well as when both  $m$  and  $n$  are even integers.

ART. 250. THEOREM III. *If  $m, n, m_1, n_1$ , are rational integers and all odd, then is*

$$(A) \quad \left(\frac{n, 2m_1}{2}\right) = \left(\frac{n, 2}{2}\right) \left(\frac{n, m_1}{2}\right);$$

$$(B) \quad \left(\frac{2n_1, m}{2}\right) = \left(\frac{2, m}{2}\right) \left(\frac{n_1, m}{2}\right);$$

$$(C) \quad \left(\frac{2n_1, 2m_1}{2}\right) = \left(\frac{-m_1n_1, 2m_1}{2}\right).$$

*Proof of (A).* It is clear that the congruence  $x^2 - 2m_1y^2 - n \equiv 0 \pmod{2^e}$  can be satisfied only when there are solutions for the case  $e=3$ . We may therefore take for  $m_1$  and  $n$  the values

$m_1$	$n$
1	1, 7
3	1, 3.

These values give a positive value to the symbol in the formula

$$\left(\frac{n, 2m_1}{2}\right) = (-1)^{\frac{n^2-1}{8} + \frac{n-1}{2} \cdot \frac{m_1-1}{2}}.$$

And this is a verification of the formula

$$\left(\frac{n, 2m_1}{2}\right) = \left(\frac{n, 2}{2}\right) \left(\frac{n, m_1}{2}\right).$$

*Proof of (B).* To determine the value of the symbol  $\left(\frac{2n_1, m}{2}\right)$ , the two cases

$$(1) \quad m \equiv 3 \pmod{4}$$

and

$$(2) \quad m \equiv 1 \pmod{4}$$

are to be considered.

For the case (1) it may be proved that the congruence

$$x^2 - my^2 - 2n_1 \equiv 0 \pmod{2^3}$$

is satisfied for the values in the table

$n_1$	$m$
1 or 5	1, 7
3 or 7	1, 3.

These values together with the values for which

$$\left(\frac{2n_1, m}{2}\right) = -1,$$

may be united in the expression

$$\left(\frac{2n_1, m}{2}\right) = (-1)^{\frac{m^2-1}{8} + \frac{n_1-1}{2} \cdot \frac{m-1}{2}},$$

and that is

$$\left(\frac{2n_1, m}{2}\right) = \left(\frac{2, m}{2}\right) \left(\frac{n_1, m}{2}\right),$$

where  $m \not\equiv 1 \pmod{4}$ .



Case (2) where  $m \equiv 1 \pmod{4}$ . In this case it is to be determined whether the congruence

$$x^2 + xy + \frac{1-m}{4}y^2 - 2n_1 \equiv 0 \pmod{2^e}$$

admits solution. This congruence may be written

$$(2x+y)^2 - my^2 - 8n_1 \equiv 0 \pmod{2^{e+2}},$$

or

$$X^2 - mY^2 - 8n_1 \equiv 0 \pmod{2^{e_1}}. \tag{i}$$

There is a solution for  $e_1 = 3$ , if

$$X^2 - mY^2 \equiv 0 \pmod{2^3} \tag{ii}$$

has a solution.

Reciprocally, the congruence (i) has a solution for  $e_1 = 4$  and  $e_1 > 4$  if  $X$  and  $Y$  are such rational integers that  $X^2 - mY^2 \equiv 0 \pmod{2^3}$  while  $X^2 - mY^2 \not\equiv 0 \pmod{2^4}$ . And that is,  $X$  and  $Y$  cannot be even integers. It follows that the congruence (ii) admits solution only for  $m \equiv 1 \pmod{8}$ . In particular, there are then two rational integers,  $x, y$ , which are solutions of the congruence (i); and it may be proved as above that this congruence may be solved for every value of  $e$  provided  $m \equiv 1 \pmod{8}$ . In the present case the nature of the integers  $n_1$  is immaterial; and we simply have

$$\left(\frac{2n_1, m}{2}\right) = +1, \quad \text{if} \quad m \equiv 1 \pmod{8},$$

$$\left(\frac{2n_1, m}{2}\right) = -1, \quad \text{if} \quad m \equiv 5 \pmod{8};$$

or, finally,

$$\left(\frac{2n_1, m}{2}\right) = \left(\frac{2, m}{2}\right) \left(\frac{n_1, m}{2}\right), \quad \text{where} \quad m \equiv 1 \pmod{4}.$$

*Proof of (C).* The value of the symbol  $\left(\frac{2n_1, 2m_1}{2}\right)$  depends upon the property of the congruence

$$x^2 - 2m_1y^2 - 2n_1 \equiv 0 \pmod{2^e}.$$

This congruence admits solution for all values of  $e$  for which there are solutions of the congruence

$$2m_1x^2 - (2m_1y)^2 - 4m_1n_1 \equiv 0 \pmod{2^{e+1}}.$$

Hence  $x$  must be an even integer. Write  $x = 2X$  and  $m_1y = Y$ . The congruence divided by 4 then becomes

$$Y^2 - 2m_1X^2 + m_1n_1 \equiv 0 \pmod{2^{e-1}}. \quad (\text{ii})$$

Upon comparison of (ii) with (i) it is evident that

$$\left(\frac{2n_1, 2m_1}{2}\right) = \left(\frac{-m_1n_1, 2m_1}{2}\right).$$

ART. 251. THEOREM IV. *If  $m, n, m_1, n_1$ , are arbitrary rational integers, having no squared factors and if  $p$  is a rational prime integer, the following relations are true:*

$$(A) \quad \left(\frac{-m, m}{p}\right) = +1,$$

$$(B) \quad \left(\frac{n, m}{p}\right) = \left(\frac{m, n}{p}\right),$$

$$(C) \quad \left(\frac{nn_1, m}{p}\right) = \left(\frac{n, m}{p}\right) \left(\frac{n_1, m}{p}\right),$$

$$(D) \quad \left(\frac{n, mm_1}{p}\right) = \left(\frac{n, m}{p}\right) \left(\frac{n, m_1}{p}\right).$$

*Proof of (A).* This relation is evidently true, since  $-m$  is the norm of  $\sqrt{m}$ , so that for every integer  $p$

$$-m \equiv N(\sqrt{m}) \pmod{p^e}.$$

*Proof of (B).* Take first  $p$  a prime integer  $\neq 2$ . Then if  $n$  and  $m$  are prime to  $p$ , it follows from Theorem I that

$$\left(\frac{n, m}{p}\right) = 1 = \left(\frac{m, n}{p}\right).$$

If further  $n = n_1p$  and  $m$  not divisible by  $p$ ,

$$\left(\frac{pn_1, m}{p}\right) = \left(\frac{m}{p}\right) = \left(\frac{m, pn_1}{p}\right).$$

(See (B) Theorem I). If  $m = pm_1$  and when  $n$  is not

divisible by  $p$ ,

$$\left(\frac{n, pm_1}{p}\right) = \left(\frac{n}{p}\right) = \left(\frac{pm_1, n}{p}\right).$$

Finally if  $m$  and  $n$  are both divisible by  $p$ , it follows from (C) of Theorem I that

$$\left(\frac{m, n}{p}\right) = \left(\frac{n, m}{p}\right) = \left(\frac{-mn}{p^2}\right).$$

Take *secondly* the case where  $p=2$ . From Theorem III this follows immediately if at least one of the numbers  $m$  or  $n$  is odd. If, however, both  $m$  and  $n$  are even, then is

$$\begin{aligned} \left(\frac{n, m}{2}\right) &= \left(\frac{2n_1, 2m_1}{2}\right) = \left(\frac{-m_1n_1, 2m_1}{2}\right) \\ &= \left(\frac{-m_1n_1, 2}{2}\right) \left(\frac{-m_1n_1, m_1}{2}\right) \end{aligned}$$

(see Theorem III, (C)); while

$$\left(\frac{m, n}{2}\right) = \left(\frac{-m_1n_1, 2}{2}\right) \left(\frac{-m_1n_1, n_1}{2}\right).$$

Further,

$$\left(\frac{-m_1n_1, m_1}{2}\right) = (-1)^{\frac{-m_1n_1-1}{2} \cdot \frac{m_1-1}{2}}$$

and

$$\left(\frac{-m_1n_1, n_1}{2}\right) = (-1)^{\frac{-m_1n_1-1}{2} \cdot \frac{n_1-1}{2}}.$$

Since  $m_1 \equiv \pm 1 \pmod{2}$  and  $n_1 \equiv \pm 1 \pmod{2}$ , it is seen that

$$\frac{-m_1n_1-1}{2} \cdot \frac{m_1-n_1}{2} \equiv 0 \pmod{2}.$$

And this proves (B).

*Proof of (C).* Let  $p$  be a prime integer *not* equal to 2. Suppose first that  $p$  is relatively prime to both  $nn_1$  and  $m$ . In this case

$$\left(\frac{nn_1, m}{p}\right) = 1 = \left(\frac{n, m}{p}\right) \left(\frac{n_1, m}{p}\right).$$

If however  $m = pm_1$ , then is

$$\left(\frac{nn_1, pm_1}{p}\right) = \left(\frac{nn_1}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n_1}{p}\right) = \left(\frac{n, pm_1}{p}\right)\left(\frac{n_1, pm_1}{p}\right).$$

An analogous formula may be derived if  $nn_1$  is divisible by  $p$ .

Next let  $p = 2$ . Observe that if  $m$ ,  $n$ , and  $n_1$  are odd integers

$$\frac{(n-1)(n_1-1)}{2} \equiv 0 \pmod{2},$$

and that is,

$$\frac{nn_1-1}{2} \equiv \frac{n-1}{2} + \frac{n_1-1}{2} \pmod{2}.$$

It is then at once evident from Theorem II that

$$\left(\frac{nn_1, m}{2}\right) = \left(\frac{n, m}{2}\right)\left(\frac{n_1, m}{2}\right).$$

Again, observing when  $m$ ,  $n$ ,  $n_1$  are odd integers that

$$\frac{n^2n_1^2-1}{8} \equiv \frac{n^2-1}{8} + \frac{n_1^2-1}{8} \pmod{2},$$

it is seen through direct calculation that

$$\left(\frac{nn_1, 2}{2}\right) = \left(\frac{n, 2}{2}\right)\left(\frac{n_1, 2}{2}\right).$$

If either of the integers  $nn_1$  or  $m$  is divisible by 2, apply Theorem III with the results just established.

*Proof of (D).* First apply Formula (B) of the present Theorem, then (C) and finally (B) to the resulting factors.

*Remark.* If  $N(\alpha)$  is the norm of  $\alpha$  in the realm  $\Re(\sqrt{m})$ , then, since

$$\left(\frac{N(\alpha), m}{p}\right) = +1$$

for every prime integer  $p$ , it follows that

$$\left(\frac{n \cdot N(\alpha), m}{p}\right) = \left(\frac{n, m}{p}\right).$$





Next write  $r = t - 1$ , and define as the *character-system* of the ideal  $\mathfrak{a}$  in the realm  $\Re(\sqrt{m})$  the  $r$  units

$$\left(\frac{n, m}{l_1}\right), \left(\frac{n, m}{l_2}\right), \dots, \left(\frac{n, m}{l_r}\right).$$

(See Sommer, p. 141.) Due to the definition of the symbol  $\left(\frac{n, m}{p}\right)$  the character-system of a principal ideal consists only of positive integers. Observe that for imaginary realms the integer  $n$  is always positive while for real realms  $m$  is positive always.

#### EXAMPLES

1. In the realm  $\Re(\sqrt{-21})$ , the discriminant  $D = -84$ . The prime divisors are  $l_1 = 2, l_2 = 3, l_3 = 7$ . Observe that for the number  $-1$ , the character system is

$$\left(\frac{-1, -21}{2}\right) = (-1)^{(-1)(-11)} = -1,$$

$$\left(\frac{-1, -21}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

$$\left(\frac{-1, -21}{7}\right) = \left(\frac{-1}{7}\right) = -1.$$

Hence for any number, say 3, we have the character-system

$$\left(\frac{3, -21}{2}\right) = -1, \quad \left(\frac{3, -21}{3}\right) = \left(\frac{7}{3}\right) = 1, \quad \left(\frac{3, -21}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

If

$$\mathfrak{a} = (5, 3 + \sqrt{-21}), \quad n = N(\mathfrak{a}) = 5,$$

we have for the character-system of  $\mathfrak{a}$

$$\left(\frac{5, -21}{2}\right) = 1, \quad \left(\frac{5, -21}{3}\right) = \left(\frac{5}{3}\right) = -1, \quad \left(\frac{5, -21}{7}\right) = \left(\frac{5}{7}\right) = -1.$$

2. In the realm  $\Re(\sqrt{34})$ , the discriminant  $D = 136, l_1 = 2, l_2 = 17$ .

In this real realm the character-system of  $-1$  is

$$\left(\frac{-1, 34}{2}\right) = (-1)^{\frac{1-1}{8} + \frac{1-1}{2} \cdot \frac{17-1}{2}} = +1,$$

$$\left(\frac{-1, 34}{17}\right) = \left(\frac{-1}{17}\right) = +1;$$

and here  $r=t=2$ .

For  $\alpha = (3, 1 + \sqrt{34})$ ,  $n = N(\alpha) = 3$ ; and the character-system of  $\alpha$  is

$$\left(\frac{3, 34}{2}\right) = (-1)^{1+8} = -1, \quad \left(\frac{3, 34}{17}\right) = \left(\frac{3}{37}\right) = -1.$$

3. In the real realm  $\mathfrak{R}(\sqrt{51})$ ,  $D=204$ ,  $l_1=2$ ,  $l_2=3$ ,  $l_3=17$ . The character-system of  $-1$  is

$$\left(\frac{-1, 51}{2}\right) = -1, \quad \left(\frac{-1, 51}{3}\right) = -1, \quad \left(\frac{-1, 51}{17}\right) = +1.$$

Observe that associated with 3, for example, there is a negative unit and as there are both negative and positive units, we have  $r=t-1=2$ . Let  $\alpha = (5, 6 + \sqrt{51})$ , so that

$$\left(\frac{n, 51}{3}\right) = \left(\frac{\pm 5}{3}\right) = +1, \quad \text{if } n = -5.$$

Hence, the character-system for  $\alpha$  is

$$\left(\frac{-5, 51}{2}\right) = -1, \quad \left(\frac{-5, 51}{17}\right) = -1.$$

**ART. 253. THEOREM.** *All ideals of one and the same ideal-class have the same character-system.*

*Proof.* Let  $\alpha$  and  $\beta$  be two ideals of the realm  $\mathfrak{R}(\sqrt{m})$ , which belong to the same class. Hence (Art. 217), there are two integers of  $\mathfrak{R}(\sqrt{m})$ , say  $\alpha$  and  $\beta$  such that  $(\alpha)\alpha = (\beta)\beta$ . Write  $N[(\alpha)\alpha] = N$  and  $N[(\beta)\beta] = N_1$ , so that  $N = N_1$ . Further, put  $\pm N(\alpha) = n$  and  $\pm N(\beta) = n_1$ . Hence, for all prime numbers, in particular,  $p = l_1, l_2, \dots, l_i$ , we have

$$\left(\frac{N, m}{p}\right) = \left(\frac{N(\alpha), m}{p}\right) \left(\frac{n, m}{p}\right) = \left(\frac{n, m}{p}\right),$$

since  $\left(\frac{N(\alpha), m}{p}\right)$  is always  $= +1$ ; and

$$\left(\frac{N_1, m}{p}\right) = \left(\frac{N(\beta), m}{p}\right) \left(\frac{n_1, m}{p}\right).$$

Since  $N = N_1$ , it follows that

$$\left(\frac{n, m}{p}\right) = \left(\frac{n_1, m}{p}\right).$$

And this is true for  $p = l_1, l_2, \dots, l_t$ .

**ART. 254. Distribution of Ideal-Classes into Genuses.**

It is clear that all classes which have the same character-system may be united into a group; and we may say these classes belong to a *genus*. The genus which contains the principal class, may be called the *principal genus*. Its character-system consists of only positive units.

Due to the formula

$$\left(\frac{nn', m}{p}\right) = \left(\frac{n, m}{p}\right) \left(\frac{n', m}{p}\right),$$

it is seen that the multiplication of the ideal-classes of two genres offers the ideal classes of one genus, whose character-system is had through the multiplication of the corresponding characters of the two genres. In particular, it is seen that the character-system of the square of an ideal class taken out of any genus consists of only positive units, so that the square of every ideal class belongs to the principal genus.

The following theorem may be proved in regard to the number of classes which belong to a genus.

**THEOREM.** *The genres into which the ideal-classes are distributed all contain the same number of ideal-classes.*<sup>1</sup>

*Proof.* Let  $H_1, H_2, H_3, \dots, H_f$ , be the classes which constitute the principal genus. If this does not include all the classes of the realm, let  $K$  be a class which does

<sup>1</sup> Sommer, p. 143.

not belong to the principal genus. It is proved below *first* that the classes  $KH_1, KH_2, \dots, KH_f$ , are all different from one another; and *secondly*, they all have one and the same character-system and therefore belong to the same genus. For, let  $i, \mathfrak{h}_1, \mathfrak{h}_2, \dots, \mathfrak{h}_f$ , be ideals, respectively, of the classes  $K, H_1, H_2, \dots, H_f$ . It is clear, for example, that  $i\mathfrak{h}_1$  is not equivalent to  $i\mathfrak{h}_2$  for (see Art. 217) otherwise  $\mathfrak{h}_1 \sim \mathfrak{h}_2$ , which is *not* true. Hence,  $KH_1 \neq KH_2$ . And similarly  $KH_i \neq KH_j (i, j = 1, 2, \dots, f; i \neq j)$ .

Further note that

$$\left(\frac{\pm N(i\mathfrak{h}_1), m}{l_i}\right) = \left(\frac{\pm N(i), m}{l_i}\right) \left(\frac{\pm N(\mathfrak{h}_1), m}{l_i}\right)$$

with similar expressions for  $\mathfrak{h}_2, \dots, \mathfrak{h}_f$ .

It is clear by considering the right-hand side of these equations that all the classes  $KH_1, KH_2, \dots, KH_f$ , have the same character-system. If all the ideals of the realm  $\mathfrak{R}(\sqrt{m})$  are contained in the classes  $H_1, H_2, \dots, H_f; KH_1, KH_2, \dots, KH_f$ , the theorem is proved. If, however, there are ideals that do not belong to any of these classes, denote such a one by  $\mathfrak{l}$  and let  $\mathfrak{l}$  belong to the class  $L$ . Form the classes  $LH_1, LH_2, \dots, LH_f$ . As above, denote by  $i$  an ideal of the class  $K$  and let  $i\mathfrak{l} = (\iota)$ , where  $(\iota)$  is a principal ideal (Art. 218). Hence  $(\iota)\mathfrak{l} = i\mathfrak{l} = ia$ , where  $a = i\mathfrak{l}$ . From the relation  $(\iota)\mathfrak{l} = ia$ , it is seen that

$$\begin{aligned} \left(\frac{\pm N((\iota)\mathfrak{l}), m}{l_k}\right) &= \left(\frac{\pm N(\mathfrak{l}), m}{l_k}\right) \\ &= \left(\frac{\pm N(i), m}{l_k}\right) \left(\frac{\pm N(a), m}{l_k}\right) \quad (k = 1, 2, \dots, f). \end{aligned}$$

Further if  $L$  had the same character-system as  $K$ , or  $KH_s$ , it is clear that

$$\left(\frac{\pm N(a), m}{l_k}\right) = 1, \quad \text{where} \quad k = 1, 2, \dots, f.$$

Were this the case, it is seen, due to the relation  $(\iota)I = ia$ , that  $L = KH_s$ , which by hypothesis is not true.

By continuing this process it is seen that eventually all the ideal-classes have been reached. And this proves the theorem.

*Remark.* In Art. 235 it was proved that if the discriminant of the realm  $(\mathfrak{R}\sqrt{m})$  contains only one prime integer, the number of ideal-classes is an odd integer. In this case the character-system consists of only one unit. As this unit could be either  $+1$  or  $-1$ , it is clear that the number of genuses could be at most 2. There would then be an even number of ideal-classes. However, since this number must be odd, there can be only one genus. Further, as there are principal ideals in every realm, and the genus to which such ideals belong is a principal genus, the character-system must be  $+1$ .

This is a special case of the general theorem of the following article.

**ART. 255. THEOREM.** *If  $m$  and  $n$  are two rational integers, which have no squared factors, and if both  $m$  and  $n$  are not negative, then is*

$$\prod_p \left( \frac{n, m}{p} \right) = +1,$$

where the product is taken over all possible prime integers  $p$ .

*Proof.* From Theorem I (A) of Art. 248, for every odd prime integer  $p (\neq 2)$ , which is not a divisor of either  $m$  or  $n$ ,  $\left( \frac{n, m}{p} \right) = +1$ . Hence if  $m$  and  $n$  are positive odd integers that are relatively prime, there remain in the computation of the value of  $\prod_p \left( \frac{n, m}{p} \right)$ , besides  $p = 2$ , only those prime integers that are divisors of  $m$  or  $n$ . And we have simply

$$\prod_p \left( \frac{n, m}{p} \right) = \left( \frac{n, m}{2} \right) \left( \frac{n}{p_1} \right) \dots \left( \frac{n}{p_\mu} \right) \left( \frac{m}{q_1} \right) \left( \frac{m}{q_2} \right) \dots \left( \frac{m}{q_\nu} \right),$$



where  $p_1, \dots, p_\mu$ , are the prime factors of  $m$ , while  $q_1, \dots, q_\nu$ , are the prime factors of  $n$ .

By definition (Art. 245) the Jacobi symbol is defined through the equality

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right) \left(\frac{n}{p_2}\right) \cdots \left(\frac{n}{p_\mu}\right),$$

while

$$\left(\frac{m}{n}\right) = \left(\frac{m}{q_1}\right) \left(\frac{m}{q_2}\right) \cdots \left(\frac{m}{q_\nu}\right),$$

and it was seen that

$$\left(\frac{n}{m}\right) \left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

It was also seen that

$$\left(\frac{n, m}{2}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

With this it is proved that  $\prod_p \left(\frac{n, m}{p}\right) = +1$  under the given conditions.

*Secondly* let  $m$  and  $n$  be taken as above, with the exception that either  $m$  or  $n$  is negative.

If  $n$  is negative, write  $n = -n_1$ , where  $n_1$  is positive. We then have

$$\prod_p \left(\frac{n, m}{p}\right) = \prod_p \left(\frac{-n_1, m}{p}\right) = \prod_p \left(\frac{-1, m}{p}\right) \prod_p \left(\frac{n_1, m}{p}\right),$$

where the second product on the right = +1.

The Jacobi symbol  $\left(\frac{-1}{m}\right)$  means

$$\left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right) \left(\frac{-1}{p_2}\right) \cdots \left(\frac{-1}{p_\mu}\right),$$

where the  $p$ 's are defined as above. Hence,

$$\prod_p \left(\frac{-1, m}{p}\right) = \left(\frac{-1, m}{2}\right) \left(\frac{-1}{m}\right).$$

However,

$$\left(\frac{-1, m}{2}\right) = (-1)^{\frac{m-1}{2}}$$

(Art. 249) and also (Dirichlet-Dedekind, *Zahlentheorie*, p. 107)

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$

The theorem is again proved in this case.

If  $m$  were negative  $= -m_1$ , the theorem is proved by using (B) of Theorem IV, Art. 251.

*Thirdly* take the case where  $m$  and  $n$  are odd integers, which have the one common factor  $r$ , so that  $m = r \cdot m_1$ ,  $n = r \cdot n_1$ . It is seen that here

$$\begin{aligned} \prod_p \left(\frac{n, m}{p}\right) &= \left(\frac{n, m}{2}\right) \left(\frac{-m_1 n_1}{r}\right) \left(\frac{n}{m_1}\right) \left(\frac{m}{n_1}\right) \\ &= \left(\frac{n, m}{2}\right) \left(\frac{-m_1 n_1}{r}\right) \left(\frac{r}{m_1}\right) \left(\frac{n_1}{m_1}\right) \left(\frac{r}{n_1}\right) \left(\frac{m_1}{n_1}\right) \\ &= (-1)^{\frac{m_1 r - 1}{2} \cdot \frac{n_1 r - 1}{2} + \frac{r-1}{2} + \frac{m_1 - 1}{2} \cdot \frac{r-1}{2} + \frac{n_1 - 1}{2} \cdot \frac{r-1}{2} + \frac{m_1 - 1}{2} \cdot \frac{n_1 - 1}{2}} = +1. \end{aligned}$$

It remains to consider the cases in which either  $m$  or  $n$  or both  $m$  and  $n$  contain the factor 2.

Let  $m$  be odd and  $n$  even  $= 2n_1$ , say. It is seen that

$$\prod_p \left(\frac{2n_1, m}{p}\right) = \prod_p \left(\frac{2, m}{p}\right) \prod_p \left(\frac{n_1, m}{p}\right) = \prod_p \left(\frac{2, m}{p}\right).$$

Further, using the Jacobi symbol, observe that

$$\prod_p \left(\frac{2, m}{p}\right) = \left(\frac{2, m}{2}\right) \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} \cdot (-1)^{\frac{m^2-1}{8}} = +1.$$

And that is,

$$\prod_p \left(\frac{2n_1, m}{p}\right) = +1.$$

Next, let  $m = 2m_1$ , while  $n$  is odd; then due to the fact that

$$\left(\frac{n, m}{p}\right) = \left(\frac{m, n}{p}\right),$$

the theorem is again proved.

Finally, let  $m$  and  $n$  be both even, say  $n = 2n_1$  and  $m = 2m_1$ . In this case,

$$\begin{aligned} \prod_p \left( \frac{2n_1, 2m_1}{p} \right) &= \prod_p \left( \frac{2, 2m_1}{p} \right) \prod_p \left( \frac{n_1, 2m_1}{p} \right) = \prod_p \left( \frac{2, 2m_1}{p} \right) \\ &= \prod_p \left( \frac{2, 2}{p} \right) \prod_p \left( \frac{2, m_1}{p} \right) = \prod_p \left( \frac{2, 2}{p} \right). \end{aligned}$$

When  $p \neq 2$ , it is clear that  $\left( \frac{2, 2}{p} \right) = +1$ . And further,  $\left( \frac{2, 2}{2} \right) = +1$ ; for in the realm  $\mathfrak{R}(\sqrt{2})$  it is seen that 2 is the norm of  $2 + \sqrt{2}$ .

It may be shown as follows that at least one of the numbers  $m$  and  $n$  must be positive in order that the above conclusions be true. For, suppose they were both negative and put  $m = -m_1$ ,  $n = -n_1$ , where  $m_1$  and  $n_1$  are both positive. We may then write

$$\begin{aligned} \prod_p \left( \frac{-n_1, -m_1}{p} \right) &= \prod_p \left( \frac{-1, -m_1}{p} \right) \prod_p \left( \frac{n_1, -m_1}{p} \right) \\ &= \prod_p \left( \frac{-1, -m_1}{p} \right) = \prod_p \left( \frac{-1, -1}{p} \right) \prod_p \left( \frac{-1, m_1}{p} \right) \\ &= \prod_p \left( \frac{-1, -1}{p} \right) = \left( \frac{-1, -1}{2} \right) = -1. \end{aligned}$$

*Remark.* If  $m$  is negative, and if  $N(i)$  is the norm of the ideal  $i$  in the realm  $\mathfrak{R}(\sqrt{m})$ , then  $n = \pm N(i)$  is to be taken positive in the computation of the character-system of the ideal  $i$ ; if, however,  $m$  is positive, then  $n = \pm N(i)$  may be taken either positive or negative with the condition, however, that  $\prod_p \left( \frac{n, m}{p} \right) = +1$ .

ART. 256. Let  $i$  be an ideal that is not a principal ideal and give to  $n$  the values  $\pm N(i)$  as indicated above, where  $i$  without loss of generality may be assumed to be free of

rational factors. We may then write

$$1 = \prod_p \left( \frac{n, m}{p} \right) = \prod_p' \left( \frac{n, m}{p} \right),$$

where the product denoted by  $\prod_p'$  extends only over the prime factors of  $m$  and  $n$  together with the prime factor  $p=2$ , if either  $m$  or  $n$  is an even integer.

If as above  $q_1, q_2, \dots, q_v$  are the odd prime factors of  $m$  which are not also factors of  $n$ , then due to the assumption relative to  $n$ , namely, that it is the norm of an ideal which is not a principal ideal, it follows that

$$\left( \frac{m}{q_1} \right) = +1, \quad \left( \frac{m}{q_2} \right) = +1, \quad \dots, \quad \left( \frac{m}{q_v} \right) = +1.$$

We then have remaining the equation

$$\bar{\prod}_p \left( \frac{n, m}{p} \right) = +1,$$

where the product  $\bar{\prod}$  is taken only over the prime factors of  $m$  with possibly the prime integer  $p=2$ .

Next observe that when  $m \equiv 2 \pmod{4}$  or when  $m \equiv 3 \pmod{4}$ , then  $D=4m$ , and that when  $m \equiv 1 \pmod{4}$ , then  $D=m$ .

Denoting by  $\prod_p'' \left( \frac{n, m}{p} \right)$  the product taken over all the prime factors of the discriminant of the realm  $\mathfrak{R}(\sqrt{m})$ , where  $n$  is the norm of any ideal (not principal) of the realm, then is

$$\prod_p'' \left( \frac{n, m}{p} \right) = +1,$$

if  $m \equiv 2$  or  $3 \pmod{4}$ ; while if  $m \equiv 1 \pmod{4}$ ,

$$1 = \bar{\prod}_p \left( \frac{n, m}{p} \right) = \left( \frac{n, m}{2} \right) \prod_p'' \left( \frac{n, m}{p} \right).$$

Observe that  $\left( \frac{n, m}{2} \right) = +1$ , if  $m \equiv 1 \pmod{4}$ , when  $n$  is

*odd.* The integer  $n$  (as norm of an ideal that is not a principal ideal) contains 2 as a simple factor only if 2 is factorable in the realm  $\Re(\sqrt{m})$  and that is (Art. 216, Case III) when  $m \equiv 1 \pmod{8}$  and in this case (see Theorem B, Art. 250)

$$\left(\frac{n, m}{2}\right) = +1;$$

with this it follows that

$$\prod_p'' \left(\frac{n, m}{p}\right) = +1,$$

and that the product of the units which constitute the character-system of an ideal that is not a principal ideal is  $= +1$ . Further, observing that the character-system of a principal ideal consists only of positive units, it appears that the results of the investigation just made may be formulated in the following theorem:

**THEOREM.<sup>1</sup>** *The product of all the  $r$  units of a character-system of an arbitrary ideal is always equal  $+1$ ; or, a system of  $r$  units  $\pm 1$  can present the character-system of an ideal, only if their product is equal  $+1$ .*

The number of different arrangements of the units  $+1$  and  $-1$  taken  $r$  at a time is clearly  $2^r$ , while the number of such arrangements, whose product is  $+1$  is  $2^{r-1}$ . Thus in a quadratic realm there are possible at most  $2^{r-1}$  genuses.

The question now before us is: corresponding to the above possibilities, do there in fact exist genuses and if so, how many are there in a fixed realm? It will be shown that there are  $2^{r-1}$  such genuses. Before taking up this proof, however, a careful investigation of the properties of the ambiguous classes of the realm is necessary.

<sup>1</sup> Hilbert, *Bericht*, p. 293; Sommer, *Vorlesungen*, p. 149; Dirichlet, *Zahlentheorie*, p. 319; Gauss, *Disq. Arithm.*, Arts. 229-31.



**ART. 257. The Ambiguous Classes.** In the quadratic realm  $\mathfrak{R}(\sqrt{m})$  it may happen that when  $-\sqrt{m}$  is written for  $\sqrt{m}$  in an ideal, that ideal remains unchanged. If  $a$  and  $a'$  are two conjugate ideals in general they do not belong to the same ideal class. Those special classes of the realm  $\mathfrak{R}(\sqrt{m})$  which contain both  $a$  and  $a'$ , where  $a$  is not a principal ideal, are called *ambiguous* classes.

Every ideal of an ambiguous class is equivalent to its conjugate; and that is  $i \sim i'$ .

The square  $A^2$  of an ambiguous class  $A$  is a principal class and reciprocally, if the square of an ideal-class is the principal class, this class is ambiguous. Those classes are clearly ambiguous, which contain ambiguous ideals. It is also conceivable that there are ambiguous classes which do not contain ambiguous ideals.

To find the number of ambiguous classes, we may proceed in such a way that first those classes are determined which contain ambiguous ideal, and to this number add the number of ambiguous classes which do *not* contain ambiguous ideals.

In virtue of the theorem (Art. 216 under Case III) regarding the ideal factors of the discriminant of the realm, it was seen that every prime rational integer which is a divisor of this discriminant is equal to the square of an ambiguous ideal. If then  $l_1, l_2, \dots, l_t$ , are the different prime rational factors of the discriminant and  $I_1, I_2, \dots, I_t$ , the corresponding ideal-factors of these prime numbers in the realm  $\mathfrak{R}(\sqrt{m})$ , it is clear that there are  $t$  different ambiguous prime ideals. The product of any two, of any three, etc., of these prime ideals are again ambiguous ideals; or, neglecting the product of all these ambiguous ideals, which is equal to the ideal  $(\sqrt{m})$ , their number is  $2^t - 1$ . In other words, not including the

principal ideal which is equivalent to (1), there are  $2^t - 1$  different ambiguous ideals in the given realm.

To calculate the number of different ambiguous classes, which are determined by the ambiguous ideals of the realm, Hilbert introduced the notion of the *independent* ambiguous classes. (See Hilbert, *Bericht*, p. 303.)

DEFINITION. A system of ambiguous classes is called a system of ambiguous classes *independent* of one another, if no class can be expressed through the product of any powers of the other classes, and where none of the classes is the principal class.

For the ambiguous independent classes, which arise from the ambiguous prime ideals of the realm there exists the following fundamental theorem:

ART. 258. THEOREM. *The  $t$  ambiguous ideals which are divisors of the discriminant of a quadratic realm  $\mathfrak{K}(\sqrt{m})$  determine (1) in the case of an imaginary realm always  $t - 1$  independent ambiguous classes, and (2) in the case of a real realm either  $t - 2$  or  $t - 1$  independent ambiguous classes according as the norm of the fundamental unit of the realm is  $+1$  or  $-1$ . Corresponding to the two cases there are for the imaginary realm  $2^t - 1$  and for the real realms either  $2^{t-2}$  or  $2^{t-1}$  different ambiguous classes with ambiguous ideals. (See Hilbert, *Bericht*, p. 306.)*

I. Proof of (1) where the realm is *imaginary*.

1. For the realm  $\mathfrak{K}(\sqrt{-1})$  it is seen that  $D = -4$ ,  $l_1 = 2$ ,  $t = 1$ . The only ambiguous ideal of this realm is  $\mathfrak{l} = (1 + \sqrt{-1}) \sim 1$ . There is here one ambiguous class, which is the principal class and no *independent* ambiguous class.

2. For the realm  $\mathfrak{K}(\sqrt{-2})$ ,  $D = -8$ ,  $l_1 = 2$ ,  $t = 1$ . And since  $\mathfrak{l}_1 = \sqrt{-2} \sim 1$ , there is also here only one ambiguous class.

3. The same is true for the realm  $\Re(\sqrt{-3})$ , whose discriminant is  $D = -3$ . The two realms  $\Re(\sqrt{-1})$  and  $\Re(\sqrt{-3})$  are the only two imaginary realms in which there are units which differ from  $\pm 1$ . For the other imaginary realms, where  $|m| > 3$ , the only units are  $\pm 1$ .

4. Let  $(\alpha) = x + y\omega$  be an ambiguous principal ideal of the imaginary realm  $\Re(\sqrt{m})$ . It is seen that we must have  $x + y\omega = \epsilon(x + y\omega')$ , where  $\epsilon$  is a unit of the realm. If then  $|m| > 3$ , it follows that either

$$(1) \quad x + y\omega = x + y\omega'$$

or

$$(2) \quad x + y\omega = -x - y\omega'.$$

The equation (1) is possible if  $y = 0$  and  $x$  equal to an arbitrary rational integer, say  $a$ . The equation (2) however offers solutions

$$1. \quad \text{for } \omega = \sqrt{m}, \quad x = 0, \quad y = b, \text{ say,}$$

$$2. \quad \text{for } \omega = \frac{1 + \sqrt{m}}{2}, \quad x = -b, \quad y = 2b;$$

and from these results it is seen that (1),  $(\sqrt{m})$  are the only ambiguous principal ideals of the realm.

If  $m \equiv 1 \pmod{4}$  or if  $m \equiv 2 \pmod{4}$ , the product of all the ambiguous ideals of the realm is  $I_1 \cdot I_2 \cdot \dots \cdot I_t = (\sqrt{m})$ ; if, however,  $m \equiv 3 \pmod{4}$  and if  $I_1$  is the ambiguous ideal-factor of 2, then is

$$I_2 \cdot I_3 \cdot \dots \cdot I_t = (\sqrt{m}).$$

In both cases any one of the ambiguous ideals, say  $I_t$ , may be expressed through  $(\sqrt{m})$  and the rest of the ambiguous ideals. Hence in either case there are at most  $t - 1$  independent ambiguous classes.

It must also be observed that there can never be an equivalence of the form  $I_1 \sim I_2 \cdot I_3 \cdot \dots \cdot I_\nu$ , where  $m \equiv 1 \pmod{4}$  or  $m \equiv 2 \pmod{4}$ ; nor one of the form  $I_2 \sim I_3 \cdot I_4 \cdot \dots \cdot I_\nu$ , for the case  $m \equiv 3 \pmod{4}$ , where  $\nu \geq t - 1$ . For it would

then follow that in the first case

$$I_1 \cdot I_2 \cdots I_p \sim I_2^2 \cdot I_3^2 \cdots I_p^2 \sim 1$$

and in the second case,

$$I_2 \cdot I_3 \cdots I_p \sim 1$$

which is not true, as it was shown above that (1) and  $(\sqrt{m})$  were the only ambiguous principal ideals of the realm. It follows that associated with the  $t-1$  ideals,  $I_1, I_2, \dots, I_{t-1}$ , there are  $t-1$  independent ambiguous classes. If these prime ideals are taken two at a time, three at a time,  $\dots$ , there exists a system of  $2^{t-1}-1$  ambiguous ideals, in which system no two ideals are equivalent and no ideal is a principal ideal. If then the principal class is included, there exists in the realm  $\mathfrak{R}(\sqrt{m})$ ,  $2^{t-1}$  classes that are different from one another and which contain ambiguous ideals.

II. Suppose next that the realm  $\mathfrak{R}(\sqrt{m})$  is *real*. The real quadratic realms are to be treated differently according as the norm of the fundamental unit is  $+1$  or  $-1$ .

1. In the *first* case, that is, when  $N(\epsilon) = +1$ , there is in the realm (see Art. 234) an algebraic integer  $\alpha$ , say, different from 1, and from  $\pm\sqrt{m}$ , such that  $\epsilon = \frac{\alpha}{\alpha'}$ . And from this relation it follows that

$$(\alpha) = (\alpha')$$

and consequently  $(\alpha)$  is an ambiguous principal ideal which is different from (1) and from  $(\sqrt{m})$ . Besides (1),  $(\sqrt{m})$ ,  $(\alpha)$  and  $(\alpha\sqrt{m})$ , where the last ideal is freed of rational factors, there is in the realm  $\mathfrak{R}(\sqrt{m})$  no other ambiguous principal ideal that is independent of the four ideals just mentioned. For if  $(\beta)$  is an arbitrary ambiguous principal ideal of the realm there is necessarily a rational integer  $f$  such that  $\beta = \pm\epsilon^f\beta'$ . On the other hand

$\alpha^f = \epsilon^f \alpha'^f$ . Hence if we write

$$(1) \quad \gamma = \frac{\beta}{\alpha^f}, \quad \text{when} \quad \beta = +\epsilon^f \beta',$$

and

$$(2) \quad \gamma = \frac{\beta}{\sqrt{m}\alpha^f}, \quad \text{when} \quad \beta = -\epsilon^f \beta',$$

it is seen that  $\gamma$  is a number, such that  $\frac{\gamma}{\gamma'} = +1$ . Since

this can be true only when  $\gamma$  is a rational number, there can be no other independent ambiguous ideals in  $\mathfrak{R}(\sqrt{m})$  besides the four principal ideals (1),  $(\sqrt{m})$ ,  $(\alpha)$  and the ideal  $(\alpha\sqrt{m})$  freed from rational factors.

2. If *secondly* the norm of the principal unit is  $N(\epsilon) = -1$ , the quadratic realm has only (1) and  $(\sqrt{m})$  as ambiguous principal ideals.

For, if  $(\alpha)$  is an ambiguous ideal which is different from (1) and  $(\sqrt{m})$  and does not contain  $(\sqrt{m})$  as a factor, we may write

$$\frac{\alpha}{\alpha'} = \pm \epsilon^f, \quad \text{so that} \quad N(\pm \epsilon^f) = N\left(\frac{\alpha}{\alpha'}\right) = +1.$$

It follows that  $f$  is an even integer, for by hypothesis  $N(\epsilon) = -1$ .

Hence if we choose  $\beta$  in such a way that

$$(1) \quad \beta = \frac{\alpha}{\epsilon^{f/2}} \begin{cases} \text{if } f/2 \equiv 0 \pmod{2} & \text{and } \frac{\alpha}{\alpha'} = +\epsilon^f, \\ \text{or if } f/2 \equiv 1 \pmod{2} & \text{and } \frac{\alpha}{\alpha'} = -\epsilon^f; \end{cases}$$

while

$$(2) \quad \beta = \frac{\alpha}{\sqrt{m}\epsilon^{f/2}} \begin{cases} \text{if } f/2 \equiv 0 \pmod{2} & \text{and } \frac{\alpha}{\alpha'} = -\epsilon^f, \\ \text{or if } f/2 \equiv 1 \pmod{2} & \text{and } \frac{\alpha}{\alpha'} = +\epsilon^f; \end{cases}$$

then it is clear that  $\beta$  is a number such that  $\frac{\beta}{\beta'} = +1$ , and



consequently,  $\beta$  is a rational number. It follows therefore that  $(\alpha) = (1)$  and  $(\alpha) = (\sqrt{m})$  are the only ambiguous principal ideals. (See Sommer, *Vorlesungen*, p. 154.)

ART. 259. Having determined all the ambiguous principal ideals that exist in a real realm, the system of non-equivalent ambiguous ideals and the ambiguous classes that are independent of one another may be determined in the same manner as in the preceding case of the imaginary realms. And it is seen that for a real realm with fundamental unit  $\epsilon$  such that  $N(\epsilon) = -1$ , one of the prime ideals  $l_1, l_2, \dots, l_t$  may be expressed through  $(\sqrt{m})$  and the remaining  $t-1$  of these ambiguous ideals; if however,  $N(\epsilon) = +1$ , of the ambiguous ideals  $l_1, l_2, \dots, l_t$ , that are factors of  $(\sqrt{m})$  or of  $(\alpha)$ , two may be expressed through  $(\sqrt{m})$  and  $(\alpha)$  and the remaining  $t-2$  inequivalent ambiguous ideals that are not principal ideals. Thus it has been shown that there are either  $t-1$  or  $t-2$  independent ambiguous classes and as in the case of the imaginary realms it is seen that there are in all  $2^{t-1}$  or  $2^{t-2}$  different ideal-classes which contain ambiguous ideals.

It remains yet to determine in what realms there exist ambiguous classes where such classes do *not* contain ambiguous ideals and to determine the number of such classes.

Observe first that if  $i$  is an ideal of an ambiguous class, then  $i \sim i'$ , or

$$(\gamma)i = i'.$$

If further  $N(\gamma) = +1$ , then the ambiguous class certainly contains an ambiguous ideal. For since  $N(\gamma) = +1$ , there is an integer  $\beta$  of the realm such that (see Art. 234)

$$\gamma = \frac{\beta}{\beta'}.$$

Hence,  $\beta i = \beta' i'$ ; so that  $\beta i$  is either an ambiguous ideal, or is an ambiguous ideal multiplied by a rational factor. Hence an ambiguous class without ambiguous ideals can exist only when  $N(\gamma) = -1$ . And this is possible only for real realms. If for such a real realm  $N(\gamma) = -1$ , and if further the fundamental unit  $\epsilon$  of this realm is such that  $N(\epsilon) = -1$ , then is  $N(\epsilon\gamma) = +1$  and consequently  $\epsilon\gamma = \beta/\beta'$ .

Here again  $(\beta)i = (\beta')i'$  and the class contains an ambiguous ideal.

Due to the above observation, there remains still the possibility which is expressed in the theorem:

**THEOREM.** *In the quadratic realm  $\mathfrak{K}(\sqrt{m})$  there exists an ambiguous class which does not contain ambiguous ideals only in the case where the character-system of  $-1 [= N(\gamma)]$  consists solely of positive units and where the norm of the fundamental unit of the realm is equal to  $+1$ . The number of such classes is had by taking one such class and multiplying it by all the different ambiguous classes which contain ambiguous ideals.*

Due to a previous theorem (Art. 248, end) the character-system of  $-1$  consists solely of positive units if  $-1$  is the norm of an integral or fractional number of the realm. The above conditions may be brought about as follows: Let  $m$  contain besides the possible factor 2 only prime factors of the form  $4n+1$ . The character-system of  $-1$  will contain in this event only positive units, since

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}};$$

and further (Art. 246)  $m$  may be expressed as the sum of two squares in the form

$$m = u^2 + v^2.$$

If we write this equation in the form

$$-1 = \frac{u^2 - m}{v^2} = N(\gamma),$$

say, it is seen that  $-1$  is the norm of an integral or fractional number of the real realm  $\mathfrak{R}(\sqrt{m})$ . This number is evidently fractional, otherwise it would be a unit and the norms of the units of the realm are by hypothesis equal to  $+1$ . Next write  $\gamma$  equal to the quotient of two ideals  $i$  and  $i_1$  that are relatively prime, so that

$$\gamma = \frac{i}{i_1} \quad \text{or} \quad i = (\gamma)i_1.$$

Since  $N(\gamma) = -1$ , it follows necessarily that

$$ii' = i_1i_1'.$$

As  $i$  and  $i_1$  are by hypothesis relatively prime and consequently also  $i'$  and  $i_1'$  it follows that  $i' = i_1$ ; and since  $i = (\gamma)i_1$ , it is seen that  $i = (\gamma)i'$  or  $i \sim i'$ . Thus it is seen that  $i$  determines an ambiguous class. This class cannot however contain an ambiguous ideal. For were  $a$  an ideal of this class, we would have  $a = \alpha i$  where  $\alpha$  is a number of  $\mathfrak{R}(\sqrt{m})$ , or  $a = (\alpha)(\gamma)i'$ . If  $a$  were an ambiguous ideal it would also follow that  $(\alpha')(\gamma')i = (\alpha)(\gamma)i'$ , or  $\alpha = (\alpha')(\gamma')$ . It would follow that  $\gamma' = \frac{\alpha}{\alpha'}$  and  $N(\gamma) = +1$ , which is not true. Neither is  $N(\epsilon\gamma) = +1$ , since  $N(\epsilon) = +1$ . And with this the first part of the above theorem is proved.

**ART. 260.** If next  $i$  is an ideal which is not ambiguous, but which determines an ambiguous class of the realm, and if  $a_1, a_2, \dots$ , denote ambiguous ideals taken as representatives of the different ambiguous classes which were presented in the preceding theorem, then as proved below, the ideals  $ia_1, ia_2, \dots$ , determine (1) different ideals; and (2) they determine *all* the ambiguous classes, which do not contain ambiguous ideals.

It is easily seen that no two of these ideals are equivalent. For, if

$$ia_\nu \sim ia_\mu,$$

then is  $a_\nu \sim a_\mu$ , which is contrary to the assumption.

Next let  $\mathfrak{I}$  be an ideal that is not ambiguous which is taken from one of the ambiguous classes. There are then two fractional numbers of the realm, say  $\gamma$  and  $\gamma_1$  such that  $N(\gamma) = -1$ ,  $N(\gamma_1) = -1$ , where  $\gamma = \frac{i}{i'}$ ,  $\frac{\mathfrak{I}}{\mathfrak{I}'} = \gamma_1$ , and consequently  $\frac{i\mathfrak{I}}{i'\mathfrak{I}'} = \gamma\gamma_1$ . Since  $N(\gamma\gamma_1) = +1$ , it is seen (Art. 234) that  $\gamma\gamma_1$  may be expressed as the quotient of an integer  $\alpha'$  and its conjugate in the form

$$\frac{i\mathfrak{I}}{i'\mathfrak{I}'} = \frac{\alpha'}{\alpha}, \quad \text{or} \quad (\alpha)i\mathfrak{I} = (\alpha')i'\mathfrak{I}'.$$

It is thus proved that  $(\alpha)i\mathfrak{I}$  is an ambiguous ideal, and consequently is one of the ideals  $a_1, a_2, \dots$ , above. Writing  $(\alpha)i\mathfrak{I} = a$ , it follows that

$$\mathfrak{I} \sim i'a \sim ia.$$

And with this it is shown that besides the classes that contain the ideals  $ia_1, ia_2, \dots$ , above, there are no ambiguous classes that contain ideals that are not ambiguous.

A combination of the theorems just proved gives rise to the following fundamental theorem:

**THEOREM.** *In every quadratic realm there exist  $2^{r-1}$  different ambiguous classes.*

This theorem *in extenso* includes the following results that have been derived above:

For the imaginary realms, it was seen that  $r=t$  and further that every ambiguous class contained necessarily ambiguous ideals. Hence, for imaginary realms the number of ambiguous classes is  $2^{t-1} = 2^{r-1}$ .

When the realm is real, there are three different cases to consider according to the nature of the character-system of  $-1$  and the value of the norm of the fundamental unit.

(a) Suppose that the character-system of  $-1$  contains once at least the unit  $-1$ . In this case  $r=t-1$ . The norm of the fundamental unit must be necessarily  $+1$ . Every ambiguous class of the realm contains ambiguous ideals. Their number is  $2^{t-2} = 2^{r-1}$ .

(b) The character-system of  $-1$  contains only positive units while the norm of the fundamental unit is  $-1$ . It is seen that  $r=t$  and that every ambiguous class contains at least one ambiguous ideal. Their number is therefore  $2^{t-1} = 2^{r-1}$ .

(c) The character-system of  $-1$  consists of positive units only and the norm of the principal is  $+1$ . In this case  $r=t$ . The realm contains  $2^{t-2}$  ambiguous classes which contain ambiguous ideals and in addition  $2^{t-2}$  ambiguous classes which do not contain ambiguous ideals, in all,  $2 \cdot 2^{t-2} = 2^{t-1} = 2^{r-1}$  ambiguous classes.

Thus it is shown that  $2^{r-1}$  is the maximum number of possible ambiguous classes. This correspondence gives rise to the conjecture that there is an intrinsic relation between the number of ambiguous classes and the number of genuses. This is shown to be true in the next article. It will be shown that every class of the principal genus may be expressed as the square of a class of the realm.

**ART. 261. The Existence of the Genuses. THEOREM.<sup>1</sup>**

*If  $m$  and  $n$  are two rational integers which have no squared factors and if for every prime integer  $p$  the value of the symbol  $\left(\frac{n, m}{p}\right)$  is  $+1$ , then is  $n$  equal to the norm of an*

<sup>1</sup> See Hilbert, § 71.



integral or fractional number of the realm  $\Re(\sqrt{m})$ .

*Proof.* If for all prime numbers  $p$ , the equation

$$\left(\frac{n, m}{p}\right) = +1,$$

is satisfied, then as has already been shown, at least one of the two numbers  $n$  or  $m$  must be positive.

We may assume that neither  $n$  nor  $m$  has a squared factor. Observe that if  $n = a \cdot b$ , then (Art. 251)

$$\left(\frac{n, m}{p}\right) = \left(\frac{a, m}{p}\right) \left(\frac{b, m}{p}\right).$$

Consider the exceptional cases that may arise: If  $p_1$  is a prime integer that divides  $n$  and also the discriminant of  $\Re(\sqrt{m})$ , then, as seen in the different cases considered above,  $p_1$  is the norm of an ideal in  $\Re(\sqrt{m})$ ; if  $p_2$  is an odd prime divisor of  $n$  but not of  $m$  and accordingly

$$\left(\frac{n, m}{p_2}\right) = \left(\frac{m}{p_2}\right),$$

and when this expression = +1, then  $p_2$  is the norm of an ideal in  $\Re(\sqrt{m})$ ; finally if 2 is a divisor of  $n$  but not of the discriminant of  $\Re(\sqrt{m})$ , and as

$$\left(\frac{2, m}{2}\right) = (-1)^{\frac{m^2-1}{8}},$$

it is seen (Art. 216, Case III), that when this expression = +1, then also 2 is the norm of an ideal in  $\Re(\sqrt{m})$ .

We may accordingly write  $n = \pm N(\mathfrak{i})$ , where  $\mathfrak{i}$  is an ideal of the realm  $\Re(\sqrt{m})$ . Since (Art. 218) there is an ideal  $\mathfrak{h}$  in the class determined by  $\mathfrak{i}$ , such that, if we put  $n_1 = N(\mathfrak{h})$ , then is  $|n_1| \leq |D_m|$ , where  $D_m$  is the discriminant of the realm  $\Re(\sqrt{m})$ . As  $\mathfrak{i}$  and  $\mathfrak{h}$  belong to the same class, it follows that  $\mathfrak{i} = (\alpha)\mathfrak{h}$  where  $\alpha$  is an integral or fractional number of  $\Re(\sqrt{m})$ . It follows that  $n = N(\mathfrak{i}) = \pm N(\alpha) \cdot N(\mathfrak{h}) = N(\alpha)n_1$ . If  $n_1 = +1$ , the correctness of the theorem is manifest.

Observe that  $n_1$  being the norm of an integral ideal is always a rational integer and in the further consideration of the theorem that we may assume  $n_1$  to be an integer without a squared factor such that

$$\left(\frac{n_1, m}{p}\right) = +1$$

for all prime integers  $p$ .

It is seen that if the theorem were proved for  $m$  and every integer  $n_1$ , where  $|n_1| \leq |\sqrt{D_m}|$ ,  $D_m$  being the discriminant of the realm  $\Re(\sqrt{m})$ , then it is true for every  $n$ ; and it is evident that no restriction upon the theorem has been made, when it is assumed that  $|n_1| \leq |\sqrt{D_m}|$ .

Suppose that the theorem has been proved for the two numbers  $n_1$  and  $m$ , and consequently that  $n_1 = \frac{x^2 - my^2}{u^2 - mv^2}$ .

In this expression,  $x, y$ , cannot be zero simultaneously, nor can  $u, v$  be simultaneously zero. Observe further that  $x, u$  cannot both be zero at the same time nor can  $y$  and  $v$  be both simultaneously zero, for in either of these cases  $n_1$  would be a perfect square. Solving the above expression for  $m$ , it is seen that

$$m = \frac{x^2 - n_1 u^2}{y^2 - n_1 v^2} \tag{i}$$

Due to the fact that

$$\left(\frac{n_1, m}{p}\right) = \left(\frac{m, n_1}{p}\right),$$

the meaning of the expression (i) is: If the theorem to be proved is correct for two numbers  $n_1$  and  $m$  then it is also true when these two numbers are interchanged, and that is, the theorem holds for  $m$  and  $n_1$ . Observe however that  $|n_1| \leq D_1$ . The inverse of this theorem is also true. In this discussion, if  $|m| \geq 4$ , then is  $|\sqrt{D_m}| < |m|$  and therefore *a fortiori*  $|n_1| < |m|$ .

Due to the first fact shown above the theorem is correct for  $m$  and  $n_1$ , where  $|n_1| \leq |\sqrt{D_m}|$  in case it is true for two numbers  $m_1$  and  $n_1$  where  $|m_1| \leq |\sqrt{D_{n_1}}|$  and  $D_{n_1}$  is the discriminant of  $\mathfrak{R}(n_1)$ . With this the proof of the theorem for two arbitrary numbers  $n, m$  is reduced to the proof of two new numbers  $\bar{n} = m_1$ , and  $\bar{m} = n_1$  which in absolute value are less than  $|m|$ , provided  $|\sqrt{D_m}| \leq |m|$  and that is, if  $|m| \geq 4$ .

Since we may reason backward from the truth of the theorem for the two numbers  $n, m$  to the truth of the theorem for the two numbers  $\bar{n}, \bar{m}$ , which are greater in absolute value, it is seen that the theorem is proved in general if its correctness is shown for the realms  $\mathfrak{R}(\sqrt{-1})$ ,  $\mathfrak{R}(\sqrt{\pm 2})$ ,  $\mathfrak{R}(\sqrt{\pm 3})$  and that is for the realms where  $m < 4$ . For all these realms the number of classes is  $h=1$ , and further note that the following eight are the only cases in which  $|m| \leq 4$  and at the same time  $|n| \leq |\sqrt{D_m}|$ . It is proved below that  $\left(\frac{n, m}{p}\right) = +1$  for all prime numbers  $p$  in each of the cases:

$$\begin{array}{ll} 1 = N(\sqrt{-1}), & -2 = N(\sqrt{2}), \\ 2 = N(1 + \sqrt{-1}), & 2 = N(\sqrt{-2}), \\ 2 = N(2 + \sqrt{2}), & -2 = N(1 + \sqrt{3}), \\ -1 = N(1 + \sqrt{2}), & -3 = N(\sqrt{3}). \end{array}$$

For note that in the realm  $\mathfrak{R}(\sqrt{-1})$ ,

$$\begin{array}{ll} \left(\frac{1, -1}{p}\right) = +1, & \left(\frac{2, -1}{p}\right) = +1; \\ 1 = N(-1), & 2 = N(1 + \sqrt{-1}), \end{array}$$

while in the realm  $\mathfrak{R}(\sqrt{2})$

$$\left(\frac{\pm 1, 2}{p}\right) = +1, \quad -1 = N(\epsilon),$$

where

$$\epsilon = 1 + \sqrt{2}, \quad +1 = N(\epsilon^2);$$

$$\left(\frac{\pm 2, 2}{p}\right) = +1, \quad -2 = N(\sqrt{2}), \quad 2 = N(2 + \sqrt{2}).$$

In the realm  $\mathfrak{R}(\sqrt{-2})$

$$\left(\frac{1, -2}{p}\right) = +1 \quad \text{and} \quad 1 = N(-1),$$

$$\left(\frac{2, -2}{p}\right) = +1 \quad \text{and} \quad 2 = N(\sqrt{-2}).$$

In the realm  $\mathfrak{R}(\sqrt{3})$

$$\left(\frac{1, 3}{p}\right) = +1, \quad 1 = N(-1), \quad \left(\frac{-2, 3}{p}\right) = +1,$$

$$-2 = N(1 + \sqrt{-3}), \quad \left(\frac{-3, 3}{p}\right) = +1, \quad -3 = N(\sqrt{3}),$$

while in the realm  $\mathfrak{R}(\sqrt{-3})$ ,

$$\left(\frac{1, -3}{p}\right) = +1 \quad \text{and} \quad 1 = N(-1).$$

In all these cases the theorem is found to be true and from the above considerations it is true in general.

ART. 262. THEOREM. *Every class of the principal genus in a quadratic realm  $\mathfrak{R}(\sqrt{m})$  may be expressed as the square of a class of this realm.*

*Proof.* Let  $H$  be a class of the principal genus in the realm  $\mathfrak{R}(\sqrt{m})$  and let  $\mathfrak{h}$  be an ideal of this class which is relatively prime to the discriminant  $D$  of this realm and let  $n$  be the norm of  $\mathfrak{h}$  with the  $\pm$  sign assigned as in Art. 252. Then is

$$\left(\frac{n, m}{p}\right) = +1,$$

for all prime integers  $p$ .

Due to the theorem just proved, we have  $n = N(\alpha)$ , where  $\alpha$  is an integral or fractional number of the realm  $\mathfrak{R}(\sqrt{m})$ .





then is also

$$K_{\lambda}^2 = K_{\nu}^2,$$

since the square of an ambiguous class belongs to the principal class  $K=1$ . The  $K$ 's however are all classes different from one another.

On the other hand, if  $C$  is any class of the realm, then  $C^2$  belongs to the principal genus. For if  $i$  is an ideal of  $C$ , so that  $i^2$  is an ideal of  $C^2$ , then is

$$\left(\frac{N(i^2), m}{p}\right) = \left(\frac{N(i), m}{p}\right) \left(\frac{N(i), m}{p}\right) = +1.$$

Hence, there is a class  $K_{\nu}$ , say, such that

$$C^2 = K_{\nu}^2,$$

where  $\nu$  is one of the integers  $1, 2, \dots, f$ . Hence  $\frac{C}{K_{\nu}}$  is an ambiguous class since its square is equal to  $K$ , where  $K$  denotes the principal class; and we may write  $\frac{C}{K_{\nu}} = A$ ,  $A$  denoting one of the ambiguous classes above. And that is,  $C = AK_{\nu}$ , which class is found among the classes (i). Thus it is seen that on the one hand  $h = gf$  and on the other hand  $h = af = 2^{r-1}f$ , so that

$$g = 2^{r-1}.$$

It was proved in Art. 256 that the product of the units which constitute a character-system is always equal to  $+1$ , and consequently there existed at most  $2^{r-1}$  genuses. In conclusion, it is seen that a system of  $r$  units  $\pm 1$ , *always* represents a character system, when and only when the product of the  $r$  units is equal to  $+1$ .

#### APPLICATION<sup>1</sup> OF THE EXISTENCE THEOREM OF THE GENUSES

ART. 263. 1. If the number of classes of a realm is odd, all the classes belong to one and the same genus. For,  $h = g \cdot f = 2^{r-1}f$ , and if  $h$  is odd,  $2^{r-1}$  must equal unity.

<sup>1</sup>Sommer, *Vorlesungen*, p. 164.

2. Let  $m = p$  be a positive or negative prime integer and let  $m \equiv 1 \pmod{4}$ . In this case  $D = m = p$ , so that  $t = 1 = r$ . The number of genuses is  $2^0 = 1$ . The realm contains only one ambiguous principal ideal and only one ambiguous class, namely, the principal class. When the discriminant contains only the one prime factor, the number of classes is odd (Art. 235) and if the realm is real, the norm of the fundamental unit (Art. 235) is equal to  $-1$ .

3. Let  $m = p$  be a positive prime integer of the form  $4n + 3$ . In this case  $D = 4p$ ,  $l_1 = 2$ ,  $l_2 = p$ , and therefore,  $t = 2$ . The character-system of  $-1$  is

$$\left(\frac{-1, p}{2}\right) = -1, \quad \left(\frac{-1, p}{p}\right) = -1,$$

so that  $r = t - 1 = 1$ . The number of ambiguous classes as well as the number of genuses is  $2^0 = 1$ . In particular,  $2$  is factorable (Art. 216) in such a realm. For  $i = (2, 1 + \sqrt{p})$  is an ambiguous ideal  $= (2, 1 - \sqrt{p}) = i'$ . And as the norm of any principal ideal in this realm is of the form  $x^2 - py^2$ , it is clear that

$$\pm 2 = x^2 - py^2.$$

Writing the equation  $2 = x^2 - py^2$  in congruence form  $x^2 \equiv 2 \pmod{p}$ , it is seen that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1, \quad \text{when} \quad p = 4(2n+1) + 3 = 8n+7$$

(Art. 216, Case III). Hence,  $+2 = x^2 - py^2$  admits solution for  $p = 8n + 7$ , and similarly,  $-2 = x^2 - py^2$  admits solution for  $p = 4(2n) + 3 = 8n + 3$ . The solution of such equations may be done by trial. Observe that often the solution may be effected in a similar manner as that of the equation (Art. 246)

$$\pm 1 = x^2 - my^2$$

by first determining the roots of the congruence

$$x^2 \mp 2 \equiv 0 \pmod{p}.$$

If  $w$  is a solution of this congruence, the required value of  $x$  is to be found among the numbers  $x = w + pg$ , where  $g$  is a positive or negative rational integer. We may write for  $g$  the values  $1, 2, \dots, p-1$ , and observe when  $\frac{x^2 \pm 2}{p}$  is a perfect square, say,  $y^2$ .

4. Let  $m = -p$  be a negative prime integer of the form  $m \equiv 3 \pmod{4}$ . In this case  $r = t = 2$ . The number of classes is *even* and the realm contains two ambiguous classes in which appear the two ambiguous prime ideals

$$a = (\sqrt{m}), \quad b = (2, 1 + \sqrt{m}),$$

whose norms are  $N(a) = -m = p$ ,  $N(b) = +2$ . The character-systems of  $a$  and  $b$  in the realm  $\mathfrak{R}(\sqrt{m})$  are accordingly,

$$\begin{aligned} \left(\frac{-m, m}{2}\right) &= +1, & \left(\frac{-m, m}{m}\right) &= +1; \\ \left(\frac{2, m}{2}\right) &= \pm 1, & \left(\frac{2, m}{m}\right) &= \pm 1, \end{aligned}$$

where in the two last expressions the upper or the lower signs occur according as  $p \equiv 1 \pmod{8}$  or  $p \equiv 5 \pmod{8}$  (Art. 216, Case III). If the two upper (plus) signs occur, then the class  $B$  determined by  $b$  belongs to the principal genus. And since every class of the principal genus may be expressed through the square of another class, it is evident that  $B = K^2$ . But  $B$  being an ambiguous class,  $B^2 = 1$  and consequently  $K^4 = 1$ . In this case it is seen that the number of classes is divisible by 4 and that is, at least equal to 4.

If however the lower (minus) signs occur in the expressions in question, then  $B$  cannot be equal to the

square of a class, and the number of classes is divisible by 2 but by no higher power of 2.

In this case, if  $H_1, H_2, \dots, H_f$ , are the classes of the principal genus, where  $f$  is an odd number, then the remaining classes are  $H_1B, H_2B, \dots, H_fB$ . Due to the fact that  $B^2=1$ , it follows that  $H_l=H_k^2, H_l=H_sH_t$ , where  $l, k, s, t$  are integers of the series  $1, 2, \dots, f$ .

5. Let  $m=p \cdot p_1$  be a positive integer where  $p$  and  $p_1$  are both positive prime integers of the form  $4n+1$ . In this case  $t=2=r, g=2$ . The number of the ambiguous classes is accordingly 2 as is also the number of the genuses. The number of classes is *even*. The ambiguous ideals are

$$(p, \sqrt{m}), \quad (p_1, \sqrt{m}), \quad (\sqrt{m}).$$

Further note that

$$\left(\frac{-1, pp_1}{p_1}\right) = \left(\frac{-1}{p_1}\right) = (-1)^{\frac{p_1-1}{2}} = +1 = \left(\frac{-1, pp_1}{p}\right).$$

Hence, see theorem in Art. 259, if the norm of the fundamental unit  $\epsilon$  of the realm is  $=+1$ , there exists an ambiguous class which does not contain an ambiguous ideal.

In this case the three ideals above must all be principal ideals. And that is, one or the other of the two equations

$$\pm p = \left(x + \frac{y}{2}\right)^2 - \frac{pp_1}{4}y^2$$

as well as one or the other of the equations

$$\pm p_1 = \left(x_1 + \frac{y_1}{2}\right)^2 - \frac{pp_1}{4}y_1^2$$

admits integral solutions.

If we write  $x + \frac{y}{2} = \frac{z}{2}p$ , it follows also that the equation

$$\pm 1 = p \left(\frac{z}{2}\right)^2 - p_1 \left(\frac{y}{2}\right)^2$$

admits integral solutions.

Reciprocally, if this equation can be solved in integers, then the norm of the fundamental unit  $\epsilon$  is equal to  $+1$ .

A necessary condition for the above Diophantine equation is that

$$(p/p_1) = +1.$$

The above result may be expressed in the theorem:

**THEOREM.** *If  $m = pp_1$ , where  $p$  and  $p_1$  are positive prime integers of the form  $4n+1$ , then the norm of the fundamental unit  $\epsilon$  of  $\mathfrak{K}(\sqrt{m})$  is equal to  $-1$ , if  $\left(\frac{p}{p_1}\right) = -1$ .*

If  $\left(\frac{p}{p_1}\right) = +1 = \left(\frac{p_1}{p}\right)$ , the fundamental unit  $\epsilon$  may have the norm  $\pm 1$ , as is seen in the case of the two realms  $\mathfrak{K}(\sqrt{145})$ , where  $\epsilon = 11 + 2\omega$ , and  $N(\epsilon) = -1$ , and in the realm  $\mathfrak{K}(\sqrt{221})$ , where  $\epsilon = 7 + \omega$  and  $N(\epsilon) = +1$ .

The question when is  $N(\epsilon) = +1$  and when is  $N(\epsilon) = -1$ , is discussed further from a different standpoint by P. G. Lejeune Dirichlet, *Ges. Werke*, Vol. I, p. 288, in a paper: "Einige neue Sätze über unbestimmte Gleichungen."

**EXAMPLE.** Write  $p = 2$ ,  $p_1 = 1 + 4n$  and derive similar results as those just proved.

6. Let  $m = qq_1$  be a positive integer, where  $q$  and  $q_1$  are positive prime integers of the form  $4n+3$ . (See Art. 243, third case.) In this case  $m \equiv 1 \pmod{4}$  and  $t = 2$ . Observe that

$$\left(\frac{-1, qq_1}{q}\right) = \left(\frac{-1}{q}\right) = -1 = \left(\frac{-1, qq_1}{q_1}\right).$$

Hence  $r = t - 1$  and  $g = 2^0 = 1$  (Art. 262). The number of classes is *odd*, since the ambiguous ideals are all principal ideals (Sommer, p. 119), and no ambiguous classes can exist which do not contain ambiguous ideals.



The equivalence  $(q, \sqrt{qq_1}) \sim 1$  has the signification here that one or the other of the two equations

$$\pm q = (x+y/2)^2 - \frac{qq_1}{4}y^2$$

admits solution; and that is, one of the equations

$$\pm 4q = (2x+y)^2 - qq_1y^2$$

may be solved in integers.

Writing  $2x+y = zq$ , these equations become

$$\pm 4 = z^2q - y^2q_1.$$

Further, observe that the equation with the upper or the lower sign admits solution, according as

$$(q/q_1) = +1 \quad \text{or} \quad (q/q_1) = -1.$$

Note that if one solution of the equation  $\pm 4 = qx^2 - q_1y^2$  is known, an infinite number of other solutions may be determined by means of the units of the real realm  $\mathfrak{R}(\sqrt{qq_1})$ . And it is further seen that the equations  $\pm 1 = qx^2 - q_1y^2$  admit solution according as  $(q/q_1) = \pm 1$ .

7. If  $m = \pm pq$  is a positive or negative integer,  $p$  and  $q$  being prime numbers such that  $p \equiv 1 \pmod{4}$  and  $q \equiv 3 \pmod{4}$ , then is  $t = 3$  or  $t = 2$ , and in either case,  $r = 2$  and  $g = 2$ . The number of classes of the realm is clearly even.

If the special cases above are taken into consideration, the results may be expressed in the theorem:

**THEOREM.** *The number of classes of a realm is odd: (1) if  $m$  is a positive or negative prime integer and  $m \equiv 1 \pmod{4}$ ; (2) if  $m$  is a positive prime integer of the form  $4n+3$ ; (3) if  $m = qq_1$  is a positive integer, being the product of two positive prime integers  $q$  and  $q_1$  of the form  $4n+3$ . In these and only in these cases is the number of classes of the realm equal to one; in all other cases the number of classes of a realm is an even number.*

## CHAPTER XI

### APPLICATIONS OF THE THEORY OF IDEALS OF QUADRATIC REALMS TO A DIS- CUSSION OF FERMAT'S THEOREM

ART. 264. L. E. Dickson in his *History of the Theory of Numbers*, Vol. II, pp. 731-776 devotes forty-five pages to the discussion of this remarkable theorem. In the preface of this volume, p. XIX he writes: "Fermat's last theorem is not of special importance in itself and the publication of a complete proof of it would deprive it of its chief claim to attention for its own sake. But the theorem has acquired an important position in the history of mathematics on account of its having afforded the inspiration which led Kummer to his invention of ideal numbers, which is one of the most important branches of modern mathematics." False proofs and erroneous deductions are noted by Dickson, in particular those of Cauchy, Lamé, Wantzel, and Kummer.

In his *Observations sur Diophante Fermat* (Vol. III, p. 241) calls attention to the fact that the equation  $a^2 + b^2 = c^2$  is satisfied by  $a = p^2 + q^2$ ,  $b = p^2 - q^2$ ,  $p > q$ ,  $c = 2pq$ , and says that he has a "truly marvelous proof," which the "margin of his book is too narrow to contain, that it is impossible to solve  $a^n + b^n = c^n (n > 2)$  in rational integers." Kronecker (*Vorlesungen über allgemeine Arithmetik*, p. 23) says that mathematicians have probably worked on this theorem more than upon any other and that no problem has caused so many false and erroneous

deductions. As stated by Dickson,<sup>1</sup> the study of the theory of ideals grew up out of the study of this problem combined with the study of the general reciprocity law (see Art. 240).

Kummer's fundamental discovery consisted in the proof that all complex integers defined by the  $n$ th roots of unity could, by the introduction of ideals, be factored uniquely into primes which obey the usual laws of arithmetic as regards multiplication and division. And he wished to apply this immediately to Fermat's theorem and the higher reciprocity law in a similar manner as Gauss, by the introduction of an  $i$  into the realm of rationality, had done for the biquadratic residues as well as by the introduction of  $\omega = \frac{-1 + \sqrt{-3}}{2}$  in the realm of rationality for the study of the cubic residues. See, for example, Bachmann, *Die Lehre von der Kreistheilung*, 14<sup>th</sup> Vorlesung; or Jacobi, *Works*, Vol. 6, p. 223.

Legendre in the beginning of the second volume of the *Théorie des nombres* writes: "The method, of which we are going to make several applications, is deserving of particular attention in that up to the present time (1830) it is the only one through which certain negative propositions relative to powers of numbers may be proved." This method consists in showing that if a theorem is true for certain numbers, it may be proved to be true for smaller numbers. This being done, the proposition (negative) is proved. For in order that the proposition be true, it would be necessary that a series of positive integers decrease indefinitely. Fermat is the first who indicated this method (of *infinite descent*) in one of his

<sup>1</sup>Dickson, "Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers." (*Annals of Math.*, Vol. 18, p. 161, Series 2.) Also read the excellent account of this theorem by H. J. S. Smith, *Collected Works*, pp. 131 et seq.

notes on Diophantus, where he proves that the area of a right angle triangle whose sides are integers can not be a square integer.

Later Euler extended these applications and treated the theory with great clearness in the second volume of his *Algebra*.

ART. 265. Following Legendre (see also Sommer, p. 177) we may give the Fermat proof that the equation

$$(1) \quad x^4 + y^4 = z^2$$

cannot be solved in integers. A zero value for one of the variables is excluded once for all. It is clear that no two of the integers can have a common factor, otherwise it must occur in the third integer and may be factored from the equation (1). If this equation admitted a solution, this solution could be expressed through

$$x^2 = r^2 - s^2, \quad y^2 = 2rs, \quad z^2 = r^2 + s^2,$$

where  $r$  and  $s$  are positive integers that are relatively prime, and where  $y$  is an even integer. Further, since  $2rs$  is a perfect square, it follows that either  $r$  and  $2s$  or  $2r$  and  $s$  are perfect squares.

If  $r = u^2$  and  $2s = 4v^2$ , we have

$$(2) \quad x^2 = u^4 - 4v^2.$$

This Diophantine equation admits solution on the assumption that (1) may be solved. We may accordingly write

$$(3) \quad u^2 = a^2 + b^2, \quad v^2 = ab,$$

where  $a$  and  $b$  are positive integers that are relatively prime. Since their product is a square, it follows that we may write

$$a = f^2, \quad b = g^2,$$

where  $f$  and  $g$  are positive integers that are relatively prime. These values substituted in (3) give the Dio-

phantine equation

$$(4) \quad u^2 = f^4 + g^4$$

which is the same as equation (1). Observe, however, that of the two integers  $x$  and  $y$ , one must be the smaller, say  $y$ . On the one hand we have

$$r = \frac{y^2}{2s} \leq \frac{y^2}{2},$$

and on the other  $r^2 = u^2$ , so that  $u \leq \frac{y}{2}$  and  $2rs = 4v^2r = y^2$ ,

so that  $v \leq \frac{y}{2}$ . Due to the relation  $ab = v^2$ , it is seen that

$$a = f^2 \leq \frac{y^2}{4}, \quad b = g^2 \leq \frac{y^2}{4}.$$

It follows that both  $f$  and  $g$  are less than  $y$  and this causes  $u$  to be less than  $z$ . Accordingly it is seen that equation (4) admits solution in smaller positive integers than the solution  $x, y$ , assumed for (1). This method could be continued indefinitely, contrary to the fact that there are only a finite number of positive integers that are less than a fixed integer  $z$  in (1).

As corollaries to this theorem it is seen that:

(A) Equations of the form

$$\begin{aligned} x^4 + y^4 = t^4 = z^2, & \quad (z = t^2), \\ s^8 + r^8 = t^4 = z^2, & \quad (s = x^2, r = y^2), \\ x^{2n} + y^{2n} = t^4 = z^2, & \end{aligned}$$

do not admit solution.

(B) No two of the relations

$$x^2 = r^2 - s^2, \quad y^2 = 2rs, \quad z = r^2 + s^2$$

can exist simultaneously, otherwise equation (1) would admit solution. Since  $(r+s)(r-s) = x^2$ , where  $r$  and  $s$  have no common factor, it would follow that

$$r+s = u^2, \quad \text{and} \quad r-s = v^2;$$



and consequently

$$2r = u^2 + v^2, \quad 2s = u^2 - v^2.$$

We would thus have

$$2y^2 = 4rs = u^4 - v^4,$$

which, as thus stated, can not exist simultaneously with  $x^2 = r^2 - s^2$ , and that is, equations of the form

$$2z^2 = x^4 - y^4$$

do not admit solution in integral form.

(C) Since the equation

$$x^4 + y^4 = z^4$$

does not admit solution, there do not exist two integers  $r$  and  $s$  such that

$$x^2 = r^2 - s^2, \quad z^2 = r^2 + s^2, \quad \text{or} \quad x^2 z^2 = r^4 - s^4.$$

(D) The last result has the following geometric interpretation. The area of a right-angled triangle whose sides are integers, can not equal to a squared integer.

For were  $xy = 2f^2$  and  $x^2 + y^2 = z^2$ , we would have

$$(x - y)^2 = z^2 - 4f^2, \quad (x + y)^2 = z^2 + 4f^2,$$

so that

$$(x^2 - y^2)^2 = z^4 - (2f)^4,$$

which from (C) is not possible. Numerous examples are given by Fermat. Dickson, *Annals of Math.*, Vol. 18, p. 163, gives an interesting reference to Leibniz in this connection.

ART. 266. The proofs which Kummer used for the Fermat Theorem rest upon the following principle that was introduced by Legendre, Vol. II, p. 357. Legendre made the impossibility of the solution of the equation  $x^3 + y^3 = z^3$ , for example, depend upon the three propositions:

1. If this equation is possible, one of the integers  $x, y, z$  must be divisible by 3.

2. That variable which is an even integer, must at the same time be divisible by 3.

3. If one of the variables is divisible at the same time by  $2^m$  and by  $3^n$ , the equation to which it belongs, may be changed into another where the corresponding variable will only be divisible by  $3^{n-1}$ . Then by making use of a series of transformations an equation is derived, in which no term is divisible by 3. And the solution of this equation is impossible by proposition 1.

To prove proposition 1, observe that if neither  $x$  nor  $y$  is divisible by 3, then is

$$x \equiv \pm 1 \pmod{3} \quad \text{and} \quad y \equiv \pm 1 \pmod{3}.$$

Further if  $t \equiv \pm 1 \pmod{3}$ , it is seen that

$$(t \mp 1)^3 = t^3 \mp 3t^2 + 3t \mp 1 = t^3 \mp 3(t \mp 1)t \mp 1,$$

so that  $t^3 \equiv \pm 1 \pmod{9}$ . It follows that

$$x^3 + y^3 \equiv 2, 0, -2 \pmod{9}.$$

Hence if  $z$  is not divisible by 3, then also is  $z^3 \equiv \pm 1 \pmod{9}$ , so that

$$x^3 + y^3 - z^3 \equiv \pm 1 \quad \text{or} \quad \pm 3 \pmod{9}.$$

And accordingly we can never have

$$x^3 + y^3 = z^3.$$

*The Proof of Proposition 2.* Observe that 3 is an odd integer, and if a solution were possible, then by giving to one of the variables the negative sign, it could be transposed to the other side of the equation, which would accordingly also admit solution.

Let  $z$  be the variable which is divisible by 2. Writing

$$(1) \quad x^3 + y^3 = 2^{3m}u^3,$$

we will prove that  $u$  must be divisible by 3. For observe that  $x^3 + y^3$  admits the two factors  $x + y$  and  $(x + y)^2 - 3xy$ , which factors have only 3 as a common divisor; and if 3 does not divide the right-hand side of (1), then are the

two factors just written relatively prime. Since  $x$  and  $y$  are both odd integers it follows that

$$\begin{aligned}x + y &= 2^{3m}a^3, \\x^2 - xy + y^2 &= b^3,\end{aligned}$$

and  $u = ab$ , where  $b$  is positive and prime to  $a$ . Writing  $b^3$  in the form

$$b^3 = \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2,$$

it is seen that  $b^3$  is of the form  $p^2 + 3q^2$  and is accordingly the norm of an integer of the realm  $\Re(\sqrt{-3})$ .

We may therefore write

$$b = f^2 + 3g^2 \quad \text{and} \quad (f + \sqrt{-3}g)^3 = F + \sqrt{-3}G,$$

where

$$\begin{aligned}F &= f(f^2 - 9g^2), \\G &= 3g(f^2 - 9g^2), \\b^3 &= F^2 + 3G^2.\end{aligned}$$

It follows that

$$\frac{x+y}{2} = F, \quad \frac{x-y}{2} = G,$$

or

$$\begin{aligned}x &= f^3 + 3f^2g - 9fg^2 - 3g^3, \\y &= f^3 - 3f^2g - 9fg^2 + 3g^3.\end{aligned}$$

Further as shown above, on the assumption that  $z$  is not divisible by 3, either  $x$  or  $y$  must be divisible by 3. It would follow that  $f$  is divisible by 3 and therefore both  $x$  and  $y$  and therefore also  $z$ . This is contrary to the assumption that the three variables had no common factor.

The *third* proposition consists in proving that the equation

$$(1) \quad x^3 + y^3 = 2^{3m}3^{3n}z^3$$

is impossible. Suppose for the moment it is satisfied without one of the variables being zero. Observe that

the two factors of the left-hand side, namely,  $x+y$  and  $(x+y)^2-3xy$  have no common factor save 3 and no higher power of 3 can be a common factor. Also note that  $x^2-xy+y^2$  is an odd integer. We may accordingly write

$$\begin{aligned}x+y &= 2^{3m}3^{3n-1}a^3, \\x^2-xy+y^2 &= 3b^3, \\z &= ab.\end{aligned}$$

Writing  $b^3$  in the form

$$b^3 = \left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2,$$

we have as above

$$b = f^2 + 3g^2, \quad b^3 = F^2 + 3G^2,$$

where

$$F = \frac{x-y}{2}, \quad G = \frac{x+y}{6}.$$

It follows that  $6G = x+y$ , or

$$(2) \quad 2^{3m-1}3^{3n-2}a^3 = g(f^2 - g^2).$$

Since  $3b^3 = x^2 - xy + y^2$  is an odd integer, it follows that  $b = p^2 + 3q^2$  is also odd and therefore also  $f^2 - g^2$ . It follows from (2) that  $g$  must be divisible by  $2^{3m-1}$ . Hence writing  $g = 2^{3m-1}A$ ,  $f+g = B$  and  $f-g = C$ , we have

$$(3^{n-1}a)^3 = ABC,$$

where  $A$ ,  $B$ , and  $C$  are relatively prime. We may accordingly write

$$f+g = M^3, \quad f-g = N^3, \quad g = 2^{3m-1}L^3, \quad LMN = 3^{n-1}a,$$

where one of the integers  $L$ ,  $M$ ,  $N$  is divisible by  $3^{n-1}$ .

We further have

$$M^3 - N^3 = 2g = 2^{3m}L^3.$$

Due to proposition 2 the solution of the equation just written necessitates that  $L$  be divisible by 3. Accordingly putting  $L = 3^{n-1}T$ , it follows that

$$(3) \quad M^3 - N^3 = (2^m 3^{n-1} T)^3.$$

Comparing this equation with (1) it is seen that through the repetition of similar transformations the solution of (1) necessitates the solution of an equation of the form

$$x^3 + y^3 = (2^m z)^3,$$

where  $z$  is not divisible by 3, and this in virtue of proposition 1 is impossible.

With this it is also proved that the solution of the equation  $x^3 + y^3 = 2^k z^3$ , for integral values of  $k$ , is impossible. (See also Legendre, II, 9.)

ART. 267. It may also be proved that the equation

$$(1) \quad \alpha^3 - \beta^3 = \gamma^3$$

does not admit solution in the realm  $\Re(\sqrt{-3}) = \Re(\omega)$ ,  $\omega = \frac{-1 + \sqrt{-3}}{2}$ . The units of this realm (Art. 99) are

1,  $\pm i$ ,  $\pm \omega$ ; and all the ideals are principal ideals.

Following Kummer (see Sommer, p. 184) write

$$\lambda = 1 - \omega = \frac{3 - \sqrt{-3}}{2} = \sqrt{-3} \left( \frac{-1 + \sqrt{-3}}{2} \right) = \sqrt{-3}\omega,$$

so that  $(\lambda) = (\sqrt{-3})$ . If a solution of (1) is possible it may be proved *first* that one of the quantities  $\alpha$ ,  $\beta$  or  $\gamma$  is divisible by  $(\lambda)$ . For suppose that neither  $\alpha$  nor  $\beta$  is divisible by  $\lambda$ . Since  $\alpha$  is an integer in  $\Re(\sqrt{-3})$ , it may be written

$$\alpha = a + b\omega = a + b - b(1 - \omega),$$

where  $a$  and  $b$  are rational integers. It would then follow that  $a + b$  is not divisible by  $(\lambda)$  and consequently 3 is not a factor of  $a + b$ .

We accordingly must have

$$\alpha \equiv \pm 1 \pmod{(\lambda)},$$

and similarly

$$\beta \equiv \pm 1 \pmod{(\lambda)},$$

and therefore

$$\alpha^3 - \beta^3 \equiv -2, 0, \text{ or } 2 \pmod{(\lambda^3)}.$$



If then  $\gamma$  is also not divisible by  $(\lambda)$ , we must have

$$\gamma \equiv \pm 1 \pmod{(\lambda)}$$

and

$$\alpha^3 - \beta^3 - \gamma^3 \equiv \pm 3, \quad \text{or} \quad \pm 1 \pmod{(\lambda^3)}.$$

The solution of  $\alpha^3 - \beta^3 - \gamma^3 = 0$  is accordingly impossible. Hence for a possible solution of this equation, one of the quantities  $\alpha$ ,  $\beta$ , or  $\gamma$  must be divisible by  $\lambda$ . Writing  $\gamma = \lambda^n \gamma_1$ ,  $n \geq 1$ , it may be shown that  $n \geq 2$ . For if  $\lambda$  is prime to  $\alpha = a + b\omega$ , then *either*

$$a \equiv \pm 1 \pmod{3}, \quad b \equiv 0 \pmod{3},$$

so that  $\alpha = \pm 1 + \lambda^2 \tau$ , where  $\tau$  is an integer; or  $a \equiv \pm 1 \pmod{3}$  and simultaneously  $b \equiv \pm 1 \pmod{3}$  so that  $\alpha = (1 + \omega) + \lambda^2 \sigma$ ,  $\sigma$  being an integer in  $\mathfrak{R}(\sqrt{-3})$ . Observe that  $1 + \omega = \eta$ , say, is a unit of the realm. It follows that in either case  $\alpha \equiv \eta \pmod{(\lambda^2)}$  and similarly  $\beta \equiv \eta_1 \pmod{(\lambda^2)}$ , where  $\eta$  and  $\eta_1$  are units of the realm.

Since  $\alpha^3 - \beta^3 \equiv 0 \pmod{(\lambda^3)}$ , it follows that  $\eta^3 - \eta_1^3 = 0$ , and with this it is proved that  $\alpha^3 - \beta^3 \equiv 0 \pmod{(\lambda^4)}$ , and that is,  $\gamma^3$  is divisible by  $\lambda^4$  or  $\gamma = \lambda^n \gamma_1$ , where  $n \geq 2$ . It may be shown *next* that the more general equation

$$(2) \quad \alpha^3 - \beta^3 = \eta \lambda^{3n} \gamma^3,$$

where  $\eta$  is a unit of  $\mathfrak{R}(\omega)$ , does not admit solution.

Due to the conditions

$$(3) \quad \alpha \equiv \pm 1 \pmod{(\lambda)}, \quad \beta \equiv \pm 1 \pmod{(\lambda)}$$

and  $\alpha^3 - \beta^3 \equiv 0 \pmod{(\lambda^3)}$ , it is seen that  $\alpha$  and  $\beta$  must satisfy the conditions in (3) simultaneously. And from these we further have the simultaneous congruences:

$$(4) \quad \alpha - \beta \equiv 0 \pmod{(\lambda)}, \quad \alpha - \omega\beta \equiv 0 \pmod{(\lambda)}, \\ \alpha - \omega^2\beta \equiv 0 \pmod{(\lambda)},$$

of which the difference  $\alpha - \beta$  is divisible by a higher power of  $\lambda$ , but neither of the other two.

For observe that  $\alpha = 1 + \lambda\tau$ ,  $\beta = 1 + \lambda\sigma$ ,  $\tau$  and  $\sigma$  integers,

so that  $\alpha - \beta = \lambda(\tau - \sigma)$ . Since  $\alpha - \beta \equiv 0 \pmod{\lambda^2}$ , it follows that  $\tau - \sigma \equiv 0 \pmod{\lambda}$  or  $\tau = \sigma + \lambda\gamma$ . Then also

$$\alpha - \omega\beta \equiv (1 - \omega) \pmod{\lambda}, \quad \text{or} \quad \frac{\alpha - \omega\beta}{\lambda} \equiv 1 \pmod{\lambda}.$$

And were  $\alpha - \omega\beta \equiv 0 \pmod{\lambda^2}$ , it would follow that 1 was divisible by  $\lambda$ . It is further seen that the three congruences (4) have no further divisor save  $\lambda$ .

Hence from (2) we may write

$$(5) \quad \begin{cases} \alpha - \beta = \epsilon_1 \lambda^{3n-2} \tau^3, \\ \alpha - \omega\beta = \epsilon_2 \lambda \mu^3, \\ \alpha - \omega^2\beta = \epsilon_3 \lambda \nu^3, \end{cases}$$

where  $\epsilon_1, \epsilon_2, \epsilon_3$  are units and  $\tau, \mu, \nu$  are integers in  $\mathfrak{R}(\sqrt{-3})$ . Observing that

$$\omega(\alpha - \beta) + \omega^2(\alpha - \omega\beta) + (\alpha - \omega^2\beta) = 0,$$

it follows from (5) that

$$\omega \epsilon_1 \lambda^{3n-2} \tau^3 + \epsilon_2 \omega^2 \lambda \mu^3 + \epsilon_3 \lambda \nu^3 = 0,$$

an equation, which, divided by  $\omega^2 \epsilon_2 \lambda$ , offers

$$(6) \quad \mu^3 - \zeta \nu^3 = \eta_1 \lambda^{3(n-1)} \tau^3,$$

where  $\zeta$  and  $\eta_1$  are two new units. Write this equation in the form of a congruence

$$(7) \quad \mu^3 - \zeta \nu^3 \equiv 0 \pmod{\lambda^3}$$

and note that neither  $\mu$  nor  $\nu$  is divisible by  $\lambda$ . As proved at the beginning of this article, we therefore have  $\mu \equiv \pm 1 \pmod{\lambda}$  and  $\nu \equiv \pm 1 \pmod{\lambda}$  so that

$$\mu^3 \equiv \pm 1 \pmod{\lambda^3} \quad \text{and} \quad \nu^3 \equiv \pm 1 \pmod{\lambda^3}.$$

These values substituted in (7) show that of the six units mentioned above we can only have  $\zeta = \pm 1$ . Hence on the supposition that (1) may be solved, it follows that an equation of the form (6), that is

$$\alpha_1^3 - \beta_1^3 = \eta_1 \lambda^{3(n-1)} \gamma_1^3$$

may be solved.

Continuing this process, it is seen that an equation of the form

$$\alpha_k^3 - \beta_k^3 = \eta_k \lambda^3 \gamma_k^3$$

could be solved, in which none of the integers  $\alpha_k$ ,  $\beta_k$  or  $\gamma_k$  is divisible by 3. And this as already proved is impossible.

ART. 268. It may also be proved that *the equation*

$$(1) \quad \alpha^4 + \beta^4 = \gamma^2$$

*can not be solved in integers of the realm  $\mathfrak{R}(i)$ .*

Here again all the ideals are principal ideals, and the units are 1,  $i$ . Writing  $\lambda = 1 - i$ , it may be proved that either  $\alpha$  or  $\beta$  must be divisible by  $\lambda$ . Note that  $2 = N(\lambda) = (1 - i)(1 + i)$  and that  $1 + i = i(1 - i) = i\lambda$ . It follows that  $2 = (1 - i)^2 i$ . Observe that  $1 \equiv i \pmod{\lambda}$ . It is clear that every integer  $\alpha$  that is prime to  $\lambda$  satisfies the congruence

$$(2) \quad \alpha \equiv i \pmod{\lambda}.$$

Every integer that is prime to 2 satisfies one or the other of the congruences

$$(3) \quad \alpha \equiv i \pmod{2} \quad \text{or} \quad \alpha \equiv 1 \pmod{2}.$$

From (3) it is seen that

$$\alpha^4 \equiv +1 \pmod{\lambda^6, \text{ or } \pmod{2^3}};$$

and that is, the fourth power of every integer  $\alpha$  that is relatively prime to  $\lambda$  is congruent to  $+1 \pmod{\lambda^6, \text{ or } 8}$ .

We may assume *first* that both  $\alpha$  and  $\beta$  in (1) are relatively prime to  $\lambda$ . It follows that

$$\alpha^4 \equiv 1 \pmod{\lambda^6}, \quad \beta^4 \equiv 1 \pmod{\lambda^6}$$

and therefore

$$\alpha^4 + \beta^4 - 2 \equiv 0 \pmod{\lambda^6}.$$

The equation (1) is

$$(4) \quad \alpha^4 + \beta^4 - 2 = \gamma^2 - 2.$$

And it is seen that  $\gamma^2$  is divisible by  $2 (= i\lambda^2)$ . We may

accordingly write  $\gamma = \lambda\gamma_1$ , where  $\gamma_1$  is relatively prime to  $\lambda$ . It follows that

$$\gamma^2 - 2 = \lambda^2\gamma_1^2 - 2 = -i2(\gamma_1^2 - i),$$

and therefore from (4)

$$\gamma_1^2 - i \equiv 0 \pmod{\lambda^4}.$$

This, however, is not possible; for from above, since  $\gamma_1$  is relatively prime to  $\lambda$ , it is seen that

$$\gamma_1^4 - 1 = (\gamma_1^2 - 1)(\gamma_1^2 + 1) \equiv 0 \pmod{\lambda^6},$$

so that  $\gamma_1^2$  is congruent to either 1 or  $-1 \pmod{\lambda^4}$ .

We may assume *secondly* that the integers  $\beta$  and  $\gamma$  are prime to  $\lambda$ . Then from (3)  $\gamma^2 \equiv -1 \pmod{2}$  or  $\gamma^2 \equiv +1 \pmod{2}$ ; and since  $-1 \equiv 1 \pmod{2}$ , we have in either case  $\gamma^2 \equiv 1 \pmod{2}$ . Since  $\beta^4 \equiv 1 \pmod{\lambda^2}$ , it is seen that  $\gamma^2 - \beta^4$  is divisible by  $\lambda^2$ . Hence from (1)  $\alpha$  is divisible by  $\lambda$ , and it follows that this equation can be solved only if

$$\lambda^{4n}\alpha^4 = \gamma^2 - \beta^4$$

admits solution, and *vice versa*. We may accordingly determine whether or not the more general equation

$$(5) \quad \epsilon\lambda^{4n}\alpha^4 = \gamma^2 - \beta^4, \quad n \geq 1,$$

may be solved. This equation when written in the form

$$(6) \quad \gamma^2 - 1 = \epsilon\lambda^{4n}\alpha^4 + \beta^4 - 1,$$

shows that  $\gamma^2 - 1$  is divisible by  $\lambda^4$  at least. From (3)  $\gamma \equiv i \pmod{\lambda^2}$ , or  $\gamma \equiv +1 \pmod{\lambda^2}$ . And it is evident in the case before us that the latter congruence must be taken so that  $\gamma - 1 = \lambda^2\tau$  and therefore  $\gamma + 1 = \lambda^2(\tau + i)$ ; and as either  $\tau$  or  $\tau + 1$  is divisible by  $\lambda$ , it is seen that

$$\gamma^2 - 1 \equiv 0 \pmod{\lambda^6}.$$

Since  $\beta^4 - 1 \equiv 0 \pmod{\lambda^6}$ , it follows from (6) that  $n > 1$ .

Next write the equation (5) in the form

$$(5) \quad \epsilon\lambda^{4n}\alpha^4 = (\gamma - \beta^2)(\gamma + \beta^2)$$

and observe that  $\gamma - \beta^2$  and  $\gamma + \beta^2$  can have no common

factor save  $\lambda^2$ , otherwise such a factor would be common to  $2\gamma$  and  $2\beta$ .

We may accordingly write

$$\gamma - \beta^2 = \eta\lambda^2\sigma^4 \quad \text{and} \quad \gamma + \beta^2 = \eta_1\lambda^{4n-2}\tau^4,$$

where  $\sigma$  and  $\tau$  are integers without a common divisor and  $\eta, \eta_1$  are units in  $\mathfrak{R}(i)$ . It follows through subtraction that

$$2\beta^2 = \eta_1\lambda^{4n-2}\tau^4 - \eta\lambda^2\sigma^4.$$

Divide this equation by 2 and write for  $\frac{-\eta\lambda^2}{2}$  and  $\frac{\eta_1\lambda^2}{2}$  the units  $\zeta$  and  $\zeta_1$ . It is seen that

$$\beta^2 - \zeta\sigma^4 = \zeta_1\lambda^{4(n-1)}\tau^4.$$

As  $n \geq 2$ , we may write

$$\beta^2 - \zeta\sigma^4 \equiv 0 \pmod{\lambda^4} \quad \text{or} \quad \beta^2 - \zeta \equiv 0 \pmod{\lambda^4},$$

and since  $(\beta^4 - 1) = (\beta^2 - 1)(\beta^2 + 1) \pmod{\lambda^6}$ , it follows that

$$\beta^2 \equiv 1 \quad \text{or} \quad -1 \pmod{\beta^4}$$

and therefore the unit  $\zeta$  is  $\pm 1$ .

Accordingly we have

$$\zeta_1\lambda^{4(n-1)}\tau^4 = \beta^2 - \sigma^4.$$

Compare this equation with (5). It is seen that a series of analogous substitutions will reduce it to the form

$$\epsilon_k\lambda^4\tau_k^4 = \rho^4 - \bar{\omega}^2,$$

a solution of which is not admissible, since it was shown above that  $\lambda$  must occur to a power greater than 4.

With this proof it is also evident that neither of the equations

$$z^2 = x^4 + y^4, \quad z^2 = x^4 - y^4$$

may be solved for rational integral values of the variables, that are different from zero.

ART. 269. A consequence of the theorems just proved, as remarked by Hurwitz, is that the quantities  $\sqrt[3]{1 \pm x^3}$ ,



$\sqrt[4]{1 \pm x^4}$  are irrational for all rational values of  $x$ . Geometrically interpreted, the meaning of these theorems is that the curves

$$x^3 \pm y^3 = c^3, \quad x^4 \pm y^4 = c^2,$$

where  $c$  is a rational number, never pass through any point whose coördinates  $x, y$  are rational numbers.

Further it is evident that the equation

$$x^3 + y^3 = z^3$$

is not satisfied by the square roots of any rational numbers. For were  $a, b, c$  three numbers that are not perfect squares and which have no common factor, and if

$$a^{3/2} + b^{3/2} = c^{3/2},$$

it would follow that

$$a^3 + b^3 - c^3 = -2(ab)^{3/2}$$

and this is impossible, since the right hand side is an irrational number.

And this means, geometrically interpreted, there is no point whose coördinates may be expressed through the square roots of rational numbers, upon the cubic

$$x^3 \pm y^3 = c^3,$$

where  $c$  is a rational number.

In Art. 298 an important consequence due to Kronecker (*Works*, Vol. I, p. 121) is made of the fact that the equation

$$(1) \quad x^3 + y^3 = 1$$

admitted solution in rational integers, only when either  $x$  or  $y$  was zero.

For writing

$$x = \frac{2a}{3b-1}, \quad y = \frac{3b+1}{3b-1},$$

where  $a$  and  $b$  are two rational numbers, it is seen that

$$x^3 + y^3 - 1 = \frac{2(4a^3 + 27b^3 + 1)}{(3b-1)^3}.$$

It is clear that every rational solution of

$$(2) \quad 4a^3 + 27b^2 + 1 = 0$$

offers a solution of (1) and vice versa. The latter equation admits solution only for  $x=1, y=0$ ; or  $x=0, y=1$ . Accordingly the only solutions of (2) are  $a=-1, b=1/3$ .

Further it is seen that the discriminant of the equation

$$x^3 + ax + b = 0$$

is (Art. 104)

$$\Delta = -(4a^3 + 27b^2).$$

With this is proved the theorem:

**THEOREM.** *The equations  $x^3 - x \pm 1/3 = 0$  are the only ones of the third degree whose discriminant is  $+1$ , in which at the same time the sum of the three roots is zero.*

**ART. 270.** An important theorem due to Kummer<sup>1</sup> is the following. By cyclotomic realms we understand (Art. 105) those realms which result from adjoining a root of unity to the usual realm.

**THEOREM.** *If  $p$  is a prime integer ( $> 2$ ) and  $\alpha, \beta, \gamma$  are any integers of the cyclotomic realm, which exists through the adjunction of a  $p^{\text{th}}$  root of unity to the usual realm, the equation*

$$\alpha^p + \beta^p + \gamma^p = 0$$

*admits no solution other than where one of the variables is zero.* See for example, Hilbert, p. 517 and an interesting article by Th. Got, which appears as an appendix to the translation into French of Hilbert's *Treatise*, by Levy and Got, and Dickson's *History*, Vol. II, p. 757. Prof. H. S. Vandiver is doing much work in this direction. Methods of solving the equation  $\zeta^2 + \eta^2 = \zeta^2$  in quadratic realms are given by the author (Liouville's *Journ.*, Vol. 4, Series 6 (1921), pp. 327 et seq.).

<sup>1</sup> Kummer, *Crelle*, Vols. 16, 17, and 40.

## CHAPTER XII

### CORRELATION BETWEEN THE THEORY OF QUADRATIC FORMS AND THE IDEALS OF QUADRATIC REALMS

ART. 271. In Arts. 240-2 we have determined whether or not a rational integer  $g$  may be expressed through one or the other of the special quadratic forms

$$x^2 + y^2, \quad x^2 - 2y^2, \quad x^2 \pm 3y^2, \quad x^2 - my^2.$$

The more general quadratic form is

$$f = ax^2 + 2bxy + cy^2,$$

in which  $a, b, c$  are rational integers, while  $x$  and  $y$  are variable integers. The middle coefficient  $2b$  is usually taken *even*. The greater part of the third volume of Dickson's *History of the Theory of Numbers* has to do with the treatment of such forms.

If  $a, 2b, c$  have no common divisor save unity, the form is said to be *properly primitive*, and *improperly primitive* if these three coefficients have 2 to the first power only as a common factor. The quantity  $b^2 - ac = D$  is called the *discriminant of the form*. We shall assume that  $D \neq 0$  and that  $D$  has no square factor.

If in the form with determinant (discriminant)  $D$  we make the substitution

$$S = \begin{cases} x = rx_1 + sy_1, \\ y = tx_1 + uy_1, \end{cases}$$

with determinant  $\Delta = ru - st$ , where all the quantities are rational integers, we have a new form

$$f_1 = a_1x_1^2 + 2b_1x_1y_1 + c_1y_1^2,$$

whose determinant  $D_1 = D\Delta^2$ . If  $\Delta = \pm 1$ , the forms  $f$  and  $f_1$  are said to be *equivalent*, *properly equivalent* if  $\Delta = +1$ , and *improperly equivalent* if  $\Delta = -1$ .

If in the form  $f_1$  we make the substitution

$$S_1 = \begin{cases} x_1 = r_1x_2 + s_1y_2, \\ y_1 = t_1x_2 + u_1y_2, \end{cases} \quad \Delta_1 = r_1u_1 - s_1t_1,$$

the form  $f_1$  becomes  $f_2 = a_2x_2^2 + 2b_2x_2y_2 + c_2y_2^2$ , whose determinant  $D_2 = D_1\Delta_1^2 = D\Delta^2\Delta_1^2$ .

In general, if we put  $SS_1 = \Sigma$ ,  $S_1S_2 = \Sigma_1$ , etc., it is seen that the associative principle is applicable, and that is,

$$\Sigma S_2 = S\Sigma_1 \quad \text{and} \quad \Sigma_1 S_3 = S_1\Sigma_2;$$

while

$(\Sigma S_2)S_3 = (S\Sigma_1)S_3 = S(\Sigma_1 S_3) = S(S_1\Sigma_2) = \Sigma\Sigma_2 = SS_1S_2S_3$ , etc. If  $D \neq 0$ , it follows from the substitutions  $S$  that

$$S^{-1} = \begin{cases} x_1 = \frac{ux - sy}{\Delta}, \\ y_1 = \frac{-tx + ry}{\Delta}. \end{cases}$$

Two substitutions  $S$  and  $S^{-1}$  are called *reciprocal* when

$$SS^{-1} = \begin{cases} x = x_2, \\ y = y_2. \end{cases}$$

We shall next consider only such substitutions in which  $r, s, t, u$  are rational integers and where the determinant  $ru - st = 1$ . Such a substitution is called *unimodular*. Its reciprocal has like properties.

If  $f$  is transformed into  $f_1$  by a unimodular substitution, we say that  $f$  and  $f_1$  are *equivalent*, and this property is denoted symbolically by

$$f \sim f_1.$$

It is evident that  $f \sim f$ . If further  $f \sim f_1$  and  $f_1 \sim f_2$ , then is  $f \sim f_2$ , as is readily proved, since  $\Delta = \Delta_1 = 1$  and  $D_2 = D_1 = D$ .

All equivalent forms constitute a *class*. It may be

proved that all possible forms with the same determinant  $D$  may be distributed into a finite number of classes (Dirichlet-Dedekind, *Zahlentheorie*, §§ 67 and 75). It is clear that any form of a class determines that class.

The fundamental problems of the Theory of Quadratic Forms are the following:

1. Determine whether a given integer may be expressed through a given form; and when this can be done, determine the values of  $x$  and  $y$ , so that the form may present the integer.

2. Determine that form as representative of a class, which will express the given integer with the least numerical calculation.

3. Determine whether two forms with the same determinant are equivalent, and if so, derive the substitutions through which they may be transformed into each other.

4. Prove that the infinite number of forms with the same determinant, may be distributed into a finite number of classes. In Art. 218 it was shown that the infinite number of ideals that belong to a definite realm, may be distributed into a finite number of classes. In this realm the discriminant is a fixed integer.

5. Show that the classes may be distributed into genuses.

ART. 272. Kummer in his first communication regarding the ideal numbers (*Crelle*, Vol. 35, p. 325) called attention to the fact that the Theory of Quadratic Realms was identical with that of the Theory of Quadratic Forms. In this same paper Kummer writes as follows: "The ideal factors of the complex numbers appear as factors of complex numbers that have a real existence." In other words the Kummer factors (Art. 205) are divisors of the integers of a fixed realm. "And



consequently," he says "when multiplied by other (Kummer) ideal factors, they produced integers of this fixed realm."

The two most important results, he emphasizes, are the following:

1. There is always a finite definite number of these Kummer numbers which are necessary and sufficient when multiplied with one another, to produce all existing integers of the realm.

We have seen that the ideals of a fixed realm were distributed into a finite number of classes.

In another form the above theorem was proved by Kronecker in his Berlin dissertation (1845), *De unitatibus complexis*. Observe that Kummer, the teacher and friend of young Kronecker, produced the above mentioned results about this time (1845), and a study of them greatly influenced the entire trend of Kronecker's mathematical endeavors, notably his introduction of modular systems already considered in Chapter VIII, and the general Theory of Forms in which he attempted (see Vol. II, Chapt. 4 of the present treatise) to generalize the Kummer results already mentioned in Art. 205.

2. *Every ideal (Kummer) number  $\mathfrak{f}$  has the property that when raised to a definite integral power it becomes an integer of the realm.* (See Art. 205.)

In Art. 218 it was seen that the  $h$  power of every ideal was a principal ideal (that is, an integer) of the realm. And we may accordingly prove the following:

**THEOREM.** *Corresponding to every ideal  $\mathfrak{a}$  of a fixed realm  $\Omega$  there exists an integer  $\kappa$  which in general does not belong to  $\Omega$ , and is such that the integers of  $\mathfrak{a}$  are identical with those integers of  $\Omega$  which are divisible by  $\kappa$ .*

For observe that  $\mathfrak{a}^h = (\omega)$ , say, where  $\omega$  is an integer of  $\Omega$ . Writing  $\kappa = \sqrt[h]{\omega}$ , it is seen that  $\kappa$  has the property

required. For if  $\alpha$  is any integer of  $\mathfrak{a}$ , then  $\alpha^h$  is divisible by  $\mathfrak{a}^h (= (\omega))$ . It follows that  $\frac{\alpha^h}{\omega}$  is an integer, as is also  $\frac{\alpha}{\sqrt[h]{\omega}} = \frac{\alpha}{\kappa}$ . Reciprocally, if  $\alpha$  is an integer of  $\Omega$  so that  $\frac{\alpha}{\kappa}$  is integral, then is  $\frac{\alpha^h}{\omega}$  integral and therefore also  $\frac{(\alpha^h)}{\mathfrak{a}^h}$  is an integral ideal as is also  $\frac{(\alpha)}{\mathfrak{a}}$ . And this means that  $\alpha$  is an integer of the ideal  $\mathfrak{a}$ . These numbers  $\kappa$  are clearly Kummer numbers which belong to a realm of degree  $h$  above  $\Omega$ . (See Smith's *Report*, p. 111.)

Let  $\mathfrak{p} = (p, b + \sqrt{m})$  denote a prime ideal of the realm  $\Re(\sqrt{m})$ . All numbers of this ideal are expressed in the form  $xp + y(b + \sqrt{m})$ , where  $x$  and  $y$  go over all rational integers. And the norm of such numbers is (Art. 205)

$$p \left( px^2 + 2bxy + \frac{b^2 - m}{p} y^2 \right).$$

Observe that the determinant of the form

$$f = px^2 + 2bxy + \frac{b^2 - m}{p} y^2$$

is  $m$ . The problem before us is the investigation of the correlation between  $\mathfrak{p}$  and  $f$ . (See Sommer, p. 197.)

ART. 273. CASE I. *The real realm  $\Re(m)$ , where  $m \not\equiv 1 \pmod{4}$ .* This case is presented in Articles 273 to 280. The discriminant is  $d = 4m$ , the basis being  $1, \omega = \sqrt{m}$ . Denoting by  $p$  any positive prime rational integer, we saw that the question of its factorization into ideal factors presented three possibilities (Art. 216).

1. If  $\left(\frac{d}{p}\right) = +1$ , then in  $\Re(\sqrt{m})$  it was possible to factor  $(p)$  into the product of two ideals, which may or may not be principal ideals.

2. If  $\left(\frac{d}{p}\right) = -1$ , then  $(p)$  is itself a prime ideal in  $\mathfrak{R}(\sqrt{m})$ . But if  $p$  is not factorable in this realm, it is not of the form  $pp' = x^2 - my^2$ . And this means that  $p$  can not be expressed through a form  $ax^2 + 2bxy + cy^2$ , with determinant  $m = b^2 - ac$ . For since  $\left(\frac{d}{p}\right) = \left(\frac{m}{p}\right) = -1$ , it follows that both  $a$  and  $c$  are relatively prime to  $p$ . And if  $\pm p = ax^2 + 2bxy + cy^2$ , it is clear that

$$\pm ap = (ax + by)^2 - my^2, \quad \text{or} \quad (ax + b)^2 \equiv m \pmod{p},$$

which is contrary to the assumption that  $\left(\frac{m}{p}\right) = -1$ .

3. If  $\left(\frac{d}{p}\right) = 0$ , that is, if  $d$  is divisible by  $p$ , then is  $x^2 \equiv 0 \pmod{p}$ , and  $p$  is equal to the square of an ambiguous ideal  $\mathfrak{p} = (p, \sqrt{m})$ .

**ART. 274. Principal Ideals and Principal Forms.** If the ideal  $(p)$  can be factored into the product of two principal ideals,

$$(p) = (a + b\omega)(a + b\omega'), \quad (\text{i})$$

this is equivalent to the fact that the integer  $p$  may be expressed through one or the other or through both of the *principal forms* (Hauptformen)

$$(I) \quad f = x^2 - my^2,$$

$$(II) \quad f = -x^2 + my^2,$$

in which for  $x$  and  $y$  two rational integers  $a$  and  $b$ , which are relatively prime, may be written. If the norm of the fundamental unit  $\epsilon$  of the realm  $\mathfrak{R}(\sqrt{m})$  is  $+1$ , and that is, if

$$N(\epsilon) = N(r + \sqrt{m}s) = r^2 - ms^2 = +1,$$

then only *one* of the two relations

$$p = a^2 - mb^2 \quad \text{or} \quad -p = a^2 - mb^2$$

follows from the ideal equation (i).

If however  $N(\epsilon) = -1$ , and if for two definite integers  $a$  and  $b$ , we have from (i), say,

$$p = a^2 - mb^2, \tag{ii}$$

then also is

$$-p = (a^2 - mb^2)(r^2 - ms^2).$$

Observing that the latter expression is the norm of an integer in  $\mathfrak{R}(\sqrt{m})$ , we may write

$$(a^2 - mb^2)(r^2 - ms^2) = N(ar + bsm + (as + br)\sqrt{m}),$$

so that

$$-p = (ar + bsm)^2 - m(as + br)^2 = a_1^2 - mb_1^2.$$

In this case it is seen that  $p$  and  $-p$  may be expressed through the same quadratic form (I). If  $p = a^2 - mb^2$  and we write these same pairs of values, namely,  $x = a$ ,  $y = b$  and  $x = ar + bsm$ ,  $y = as + br$  in (I), we have  $p$  and  $-p$ ; and if we write these pairs of values in (II) we have  $-p$  and  $p$ . And thus when the  $N(\epsilon) = -1$ , we have both  $p$  and  $-p$  represented through the form (II).

In this case however, that is, if  $N(\epsilon) = r^2 - ms^2 = -1$ , if we put  $x_1 = rx + msy$ ,  $y_1 = -sx - ry$ , with determinant  $-r^2 + ms^2 = +1$ , we have

$$-x_1^2 + my_1^2 = -(r^2 - ms^2)(x^2 - my^2) = x^2 - my^2,$$

and that is the form (I) is equivalent to the form (II). If reciprocally there is a substitution with determinant  $\Delta = \pm 1$ , which transforms (I) and (II) into each other, then simultaneously  $p$  and  $-p$  may both be expressed through either of the forms  $x^2 - my^2$ , or  $-x^2 + my^2$ . If  $p = a^2 - mb^2$  and  $-p = a_1^2 - mb_1^2$ , there exists the ideal equation

$$(a + \sqrt{mb}) = (a_1 + \sqrt{mb_1})$$

and consequently also

$$\epsilon = \frac{a + \sqrt{mb}}{a_1 + \sqrt{mb_1}}, \quad N(\epsilon) = \frac{a^2 - mb^2}{a_1^2 - mb_1^2} = \frac{p}{-p} = -1.$$

Using the results derived above, as defining a "correlation" between an ideal and a form, we have the theorem:

**THEOREM.** *If  $\mathfrak{p} = (a + b\sqrt{m})$  is a principal prime ideal, then*

(A) *the two non-equivalent forms  $x^2 - my^2$  and  $-x^2 + my^2$  are correlated to  $\mathfrak{p}$  in the realm  $\mathfrak{R}(\sqrt{m})$  in which  $N(\epsilon) = 1$ ;*

(B) *the two equivalent forms  $x^2 - my^2$  and  $-x^2 + my^2$  are correlated to  $\mathfrak{p}$  in the realm  $\mathfrak{R}(\sqrt{m})$  in which  $N(\epsilon) = -1$ .*

**ART. 275.** If in (I) and (II) we make the substitutions

$$\begin{aligned}x &= rx_1 + sy_1, \\y &= tx_1 + uy_1,\end{aligned}$$

where the rational integers  $r, s, t, u$  satisfy the condition

$$\Delta = ru - st = +1,$$

and if we put  $r^2 - mt^2 = A$ ,  $rs - mtu = B$ ,  $s^2 - mu^2 = C$ , we have two infinite systems of quadratic forms

$$(I_a) \quad Ax_1^2 + 2Bx_1y_1 + Cy_1^2$$

equivalent to (I), and

$$(II_a) \quad -Ax_1^2 - 2Bx_1y_1 - Cy_1^2$$

equivalent to (II), with determinant  $D = B^2 - AC = m$ .

And clearly every integer  $p$  which may be expressed through (I) or (II) may also be expressed through the equivalent forms  $(I_a)$  or  $(II_a)$ .

In the realms in which  $N(\epsilon) = 1$ , the forms (I) and (II) are different, as are also  $(I_a)$  and  $(II_a)$ . These forms are, however, equivalent in those realms in which  $N(\epsilon) = -1$ . We may next prove the *inverse theorem*, namely, that if the prime integer  $p$  can be expressed through the quadratic form  $F = Ax^2 + 2Bxy + Cy^2$  with determinant  $D = (B^2 - AC) = m$ , then this form is equivalent to the form (I) when  $N(\epsilon) = 1$ , or to the equivalent forms (I) and (II) when  $N(\epsilon) = -1$ . In other words, if  $p$  can be expressed through  $f$  and also through  $F$ , then is  $f$  equivalent to  $F$ .



Due to the assumption that  $D$  can have no squared factor it follows that  $A$ ,  $B$ , and  $C$  can have no common factor except unity. We may further assume that any of the three integers  $A$ ,  $B$  or  $C$  is relatively prime to any given integer. For example, if  $A$  is not prime to  $p$ , we may, without loss of generality, derive a form equivalent to  $F$  in which the coefficient of the first term is prime to  $p$ . For if  $A$  is divisible by  $p$  and if  $C$  is prime to  $p$  (which includes the case  $p=2$ ), then applying to  $F$  the substitution

$$\begin{aligned} x &= px_1 + sy_1 \\ y &= qx_1 + uy_1, \quad pu - sq = 1, \end{aligned}$$

where  $q$  is prime to  $p$ , it is seen that the coefficient of  $x^2$  is  $Ap^2 + 2pqB + q^2C$ , which integer is prime to  $p$ .

If on the other hand  $C$  is also divisible by  $p$ , the substitution

$$\begin{aligned} x &= q_1x_1 + sy_1, \\ y &= q_2x + uy, \quad q_1u - q_2s = 1, \end{aligned}$$

where both  $q_1$  and  $q_2$  are prime to  $p$ , offers a form in which the coefficient of  $x^2$  is relatively prime to  $p$ .

Writing

$$p = Ax_1^2 + 2Bx_1y_1 + Cy_1^2, \tag{iii}$$

where  $x_1$  and  $y_1$  are relatively prime, it is seen that

$$Ap = (Ax_1 + By_1)^2 - my_1^2 = x^2 - my^2, \tag{iv}$$

where

$$x = Ax_1 + By_1, \quad \text{and} \quad y = y_1.$$

And that is,  $Ap$  may be expressed through the form  $x^2 - my^2$ .

From the equation (iii) it is seen that  $y_1$  is prime to  $p$ , and that  $A$  and  $y$  are relatively prime. And from (iv) it follows that both  $y$  and  $Ax_1 + By_1$  are relatively prime to  $Ap$ . The case before us assumes that  $p=f$ , and that is,  $p$  may be factored into two prime principal ideals, so that

$p = X^2 - mY^2$ . Equation (iv), when expressed in terms of ideal factors, is  $(A)(X - \sqrt{m}Y)(X + \sqrt{m}Y)$  on the one hand, and  $(Ax_1 + By_1 - \sqrt{m}Y)(Ax_1 + By_1 + \sqrt{m}Y)$  on the other hand. Since  $X - \sqrt{m}Y$  and  $X + \sqrt{m}Y$  are prime ideals they must divide one or the other of the ideal factors in the right hand side of the equation. We thus have  $(A)$  expressed as the product of integral principal ideals, say

$$A = r^2 - mt^2, \quad (\text{v})$$

where  $r$  and  $t$  are two integers that are relatively prime. Writing  $\alpha = r + \sqrt{m}t$ , it is seen that  $N(\alpha) = A$ . Further, observing that  $AC = B^2 - m \cdot 1$ , and writing  $\alpha\gamma = B - \sqrt{m}$ ,  $N(\alpha\beta) = AC$  and  $\gamma = s - \sqrt{m}u$ , we have

$$(r + \sqrt{m}t)(s - \sqrt{m}u) = B - \sqrt{m},$$

where  $s$  and  $u$  are rational (and as proved below) integral numbers.

From this we have at once

$$\left. \begin{aligned} rs - mtu &= B \\ ru - st &= 1 \end{aligned} \right\} \quad (\text{vi})$$

or

$$u = \frac{Bt + r}{A}, \quad s = \frac{Br + tm}{A}. \quad (\text{vii})$$

It follows that

$$\begin{aligned} Ap &= (r^2 - mt^2)(X^2 - mY^2) \\ &= [rX + tmY + (rY + tX)\sqrt{m}][rX + tmY - (rY + tX)\sqrt{m}]. \end{aligned}$$

This equation in connection with (iv) shows that the integers  $x, y$  may be so chosen that

$$\begin{aligned} Ax_1 + By_1 &= rX + tmY, \\ -y_1 &= tX + rY. \end{aligned}$$

And from the latter equations, it follows that

$$X = rx + sy, \quad Y = -tx - uy.$$

Observing in these equations that  $X, Y, r, t, x$  are integers, it is seen that  $sy$  and  $uy$  are integers. Hence from (vi) if  $s$  and  $u$  were rational numbers, their de-

nominators must be factors of  $A$  and  $y$ . But since  $A$  and  $y$  are relatively prime, the numbers  $s$  and  $u$  are integers. With this it is proved that the substitution

$$\begin{aligned} x &= rx_1 + sy_1, \\ -y &= tx_1 + uy_1, \quad ru - st = 1 \end{aligned}$$

is such that the form (I) is transformed into the form

$$F = Ax^2 + 2Bxy + Cy^2.$$

With this our inverse theorem is proved.

**ART. 276. Arbitrary Prime Ideals and Correlated Forms in the Realms  $m \not\equiv 1 \pmod{4}$ .** Let  $p$  be a prime rational integer such that  $\left(\frac{d}{p}\right) = +1$ , or  $\left(\frac{d}{p}\right) = 0$ . The ideal  $(p)$  accordingly is factorable in the realm  $\mathfrak{R}(\sqrt{m})$  as the product of two prime ideals which may or may not be principal ideals. When  $\left(\frac{d}{p}\right) = 0$ , the two ideals are equal (ambiguous) (see Art. 216).

Accordingly we may write

$$(p) = \mathfrak{p}\mathfrak{p}' = (p, b + \sqrt{m})(p, b - \sqrt{m}).$$

where  $b$  is a positive integer of zero. Again observe that all integers that are divisible by  $\mathfrak{p}$  are of the form  $px + (b + \sqrt{m})y$ , where  $x$  and  $y$  are rational integers.

With the ideal  $\mathfrak{p}$ , by definition, are correlated the forms

$$\begin{aligned} \text{(I)} \quad f_1 &= \frac{1}{p}(px + by + \sqrt{m}y)(px + by - \sqrt{m}y) \\ &= px^2 + 2bxy + \frac{b^2 - m}{p}y^2, \end{aligned}$$

or

$$\text{(II)} \quad f_2 = -px^2 - 2bxy - \frac{b^2 - m}{p}y^2;$$

and to the ideal  $\mathfrak{p}'$  the forms

$$\text{(III)} \quad f_3 = px^2 - 2bxy + \frac{b^2 - m}{p}y^2,$$

or

$$(IV) \quad f_4 = -px^2 + 2bxy - \frac{b^2 - m}{p}y^2.$$

Note that:

(a) The forms  $f_1$  and  $f_3$  on the one hand and  $f_2$  and  $f_4$  on the other are improperly equivalent, since the substitutions  $s = x$ ,  $y = -y_1$  with determinant  $\Delta = -1$  transform these forms respectively into each other.

(b) With definite values ascribed to  $x$  and  $y$  the forms  $f_1$  and  $f_2$  on the one hand and  $f_3$  and  $f_4$  on the other offer equal integers with contrary sign.

If the norm of the fundamental unit  $\epsilon$  of  $\mathfrak{K}(\sqrt{m})$  is  $-1$ , and only in this case are the forms  $f_1$  and  $f_2$  improperly equivalent as are the forms  $f_3$  and  $f_4$ .

For write

$$\epsilon = r + s\sqrt{m}, \quad r^2 - s^2m = -1;$$

and observe that

$$x = (r - bs)x_1 - \frac{b^2 - m}{p}sy_1,$$

$$y = psx_1 + (r + bs)y_1,$$

with determinant  $-1$ , transforms  $f_1$  into  $f_2$  and also  $f_3$  into  $f_4$ .

Writing

$$x = (r - bs)x_1 + \frac{b^2 - m}{p}sy_1,$$

$$y = psx_1 - (r + bs)y_1,$$

with determinant  $+1$ , it is seen that  $f_1$  and  $f_4$  are properly equivalent, as are also  $f_2$  and  $f_3$ .

Accordingly the results (a) and (b) may be expressed as follows: when  $N(\epsilon) = -1$ , we have  $f_1 \sim f_4$  and  $f_2 \sim f_3$ , these equivalences being improperly equivalent to each other.

ART. 277. **Ambiguous Ideals** <sup>1</sup> in Real Realms  $m \neq 1$  (mod. 4). If  $\mathfrak{p}$  is an *ambiguous ideal*, and that is, if

$$(p, b + \sqrt{m}) = (p, b - \sqrt{m}) = (p, b + \sqrt{m}, b - \sqrt{m}),$$

then is

$$b - \sqrt{m} = pr_1 + (b + \sqrt{m})s_1,$$

where  $r_1$  and  $s_1$  are rational integers. It follows that  $s_1 = -1$ ,  $2b = pr_1$ , so that  $2b$  is divisible by  $p$ .

It is evident at once that the substitution  $x = x_1 - \frac{2b}{p}y_1$ ,  $y = y_1$  with determinant  $\Delta = +1$ , transforms  $f_1$  into  $f_3$  and likewise  $f_2$  into  $f_4$ . If  $N(\epsilon) = +1$ , the two forms  $f_1$  and  $f_2$  are representative of the four forms of the preceding article. However, if  $N(\epsilon) = -1$ , it was shown in the preceding article that  $f_1 \sim f_4$ , so that in the case before us  $f_1 \sim f_2 \sim f_3 \sim f_4$ .

In (a) of the preceding article it was seen that  $f_1$  was also improperly equivalent to  $f_3$  and  $f_2$  to  $f_4$ . It is seen that the substitution

$$x = x_1 + \frac{2b}{p}y_1, \quad y = -y_1,$$

with determinant  $\Delta = -1$  transforms these forms into themselves. Such a form is improperly equivalent to itself and (see Dedekind, *Zahlentheorie*, § 58) is called *ambiguous* (*Zweiseitig*). See also Kummer (*Monatsb. d. Berliner Akad.*, Feb. 18, 1858).

Observe finally that if  $\mathfrak{p}$  is a principal ideal, the results of Art. 274 show that simultaneously, on the one hand the forms  $f_1$  and  $f_3$  and on the other  $f_2$  and  $f_4$  are equivalent to one of the forms  $x^2 - my^2$ ,  $-x^2 + my^2$  or to them both. And if the form  $f_1$  is both properly and improperly equivalent to  $f_3$  they are both improperly equivalent to themselves.

<sup>1</sup> See Smith's *Report*, p. 189; Dickson, Vol. III, p. 13; and see the remark by the author at the end of this chapter.



EXAMPLE. Let the ideal  $(p, b + \sqrt{m})$  degenerate into a principal ideal. Deduce, using the methods of Art. 276, the results of Art. 274. Consider also the case of *ambiguous* principal ideals.

ART. 278. An integer  $p$  which may be expressed through any of the forms  $f_1, f_2, f_3, f_4$ , say  $f_1$ , is also presented through any form that is equivalent to  $f_1$ . It remains to prove the inverse problem, namely:

Any form  $f = Ax^2 + 2Bxy + Cy^2$  with determinant  $D = m$  through which  $p$  may be expressed by giving to  $x, y$  definite values  $r$  and  $t$ , which are relatively prime, is equivalent to one of the four forms  $f_1, f_2, f_3, f_4$ .

Suppose for example, that  $p = Ar^2 + 2Brt + Ct^2$  where  $r$  and  $t$  are relatively prime. Let  $s$  and  $u$  be two other integers that are likewise relatively prime, such that

$$ru - st = 1.$$

Introducing the substitution

$$\begin{aligned} x &= rx' + sy', \\ y &= tx' + uy', \quad \Delta = 1, \end{aligned}$$

we observe that the form  $f$  is transformed into

$$F = px'^2 + 2\{(Ar + Bt)s + (Br + Ct)u\}x'y' + (As^2 + 2Bsu + Cu^2)y'^2$$

with determinant  $m$ ; or if we put

$$F = px'^2 + 2b_1x'y' + c_1y'^2,$$

we have

$$m = b_1^2 - c_1p.$$

It follows that  $b_1^2 - m \equiv 0 \pmod{p}$ ; and that  $b_1$  is a rational integer which satisfies the congruence

$$X^2 - m \equiv 0 \pmod{p}. \quad (i)$$

In a later article (Art. 280, end) it is seen that  $b_1$  depends upon the values for  $r$  and  $t$ , but is independent of the values  $u, s$ , which as seen above are not uniquely determined.

Since  $\frac{b^2 - m}{p}$  is an integer, it is seen that  $b$  satisfies the

congruence (i), so that  $b_1 = \pm b + gp$ , where  $g$  is an integer (including zero). The form  $F$  becomes

$$F = px'^2 + 2(gp \pm b)x'y' + cy'^2.$$

Making the substitution

$$x' = X - gY, \quad y' = Y, \quad \Delta = 1,$$

we have

$$F = pX^2 \pm 2bXY + c_2Y^2,$$

where  $c_2$  is a definite constant. And since the determinant of this form is  $m$ , and that is  $b^2 - c_2p = m$ , so that

$c_2 = \frac{b^2 - m}{p}$ , we have finally

$$F = pX^2 \pm 2bXY + \frac{b^2 - m}{p}Y^2.$$

And that is,  $f(\sim F)$  is one of the forms  $f_1$  or  $f_3$ ; and to these two forms were correlated, by definition, the ideals  $\mathfrak{p}$  and  $\mathfrak{p}'$ . The following rule expresses the results that have been derived above.

If  $\mathfrak{p} = (p, b + \sqrt{m})$  with its conjugate  $\mathfrak{p}' = (p, b - \sqrt{m})$  is an arbitrary ideal of  $\mathfrak{R}(\sqrt{m})$ , in which  $b$  is a positive integer (or zero) then with  $\mathfrak{p}$  are correlated.

(A) *the forms  $f_1$  and  $f_2$  and with  $\mathfrak{p}'$  the forms  $f_3$  and  $f_4$  if  $N(\epsilon) = 1$ , it being assumed that  $\mathfrak{p}$  is neither an ambiguous ideal nor a principal ideal;*

(B) *the quadratic form  $f_1$  and with  $\mathfrak{p}'$  the form  $f_3$ , when  $N(\epsilon) = -1$ , where  $\mathfrak{p}$  is neither an ambiguous nor a principal ideal. If, however  $\mathfrak{p}$  is an ambiguous or principal ideal, then  $f_1$  and  $f_3$  fall together as do  $f_2$  and  $f_4$  and are ambiguous forms.*

ART. 279. Instead of writing the ideal  $\mathfrak{p}$  in the normal form, any other basis  $\hat{\omega}_1$  and  $\hat{\omega}_2$  may be taken, where  $\hat{\omega}_1 = a_1 + b_1\sqrt{m}$ ,  $\hat{\omega}_2 = c_1 + d_1\sqrt{m}$ . The form corresponding

to  $f_1$  above, which is correlated to  $\mathfrak{p}$ , is

$$F = \frac{1}{p} [(a_1x + c_1y) + (b_1x + d_1y)\sqrt{m}] \\ \times [(a_1x + c_1y) - (b_1x + d_1y)\sqrt{m}]$$

or

$$F = \frac{a_1^2 - b_1^2m}{p}x^2 + 2\frac{(a_1c_1 - b_1d_1m)}{p}xy + \frac{c_1^2 - d_1^2m}{p}y^2.$$

Since  $N(\hat{\omega}_1)$  and  $N(\hat{\omega}_2)$  are both elements of  $\mathfrak{p}$ , these two integers can have no common factor. It is shown below that the determinant of the form  $F$  is  $m$ . Accordingly the quantities  $a_1^2 - b_1^2m$ ,  $a_1c_1 - b_1d_1m$ ,  $c_1^2 - d_1^2m$  are not all divisible by  $p^2$ , otherwise  $m$  would be divisible by the square of  $p$ , which case has been excluded. It follows that the coefficients of  $F$  have no common divisor save unity.

Since  $\mathfrak{p} = (\hat{\omega}_1, \hat{\omega}_2) = (p, b + \sqrt{m})$ , we may write  $\hat{\omega}_1 = rp + t(b + \sqrt{m})$ ,  $\hat{\omega}_2 = sp + u(b + \sqrt{m})$ , where  $ru - st = \pm 1$ .

Accordingly the form  $F$  may be written

$$F = \frac{1}{p} \cdot N[p(rx_1 + sy_1) + (tx_1 + uy_1)b + (tx_1 + uy_1)\sqrt{m}].$$

The form  $f$  correlated with  $\mathfrak{p}$  in Art. 276 was

$$f = \frac{1}{p} N(px + by + \sqrt{m}y).$$

It follows that by writing

$$x = rx_1 + sy_1, \\ y = tx_1 + uy_1, \quad ru - st = \pm 1 = \Delta,$$

that the form  $F$  is transformed into  $f_1$ , where  $\Delta = 1$ . If  $\Delta = -1$ , we have the same substitution as above where for  $r$  and  $s$  are written  $-r$  and  $-s$ ; and in this case  $F$  is transformed into  $f_3$ . Since the determinants of  $f_1$  and  $f_3$  are equal to  $m$ , it is seen that the determinant of  $F$  is  $m$ . We accordingly have the theorem:

*To the different pairs of elements which constitute bases*

of the ideal  $\mathfrak{p}$ , there correspond forms with determinant  $m$ , which are properly or improperly equivalent amongst themselves. And that is, the dependence of different pairs of elements among themselves leads to the equivalence of corresponding forms.<sup>1</sup>

ARBITRARY IDEALS AND FORMS

ART. 280. We saw in Art. 206, end, that an ideal reduced to its canonical form was  $i = (i_1, i_2 + i_3\omega)$ , where  $i_3$  divided both  $i_1$  and  $i_2$ . If then we assume that  $i$  has no rational factor, it may be written  $(a, b + \omega)$ , where  $a$  is the smallest rational integer that is divisible by  $i$ . Accordingly this factor may enter as an element of  $i$ .

Corresponding to the ideal  $i$  there exists a form, analogous to  $f_1$  of Art. 276, given by

$$f = ax^2 + 2bxy + \frac{b^2 - m}{a}y^2.$$

And it is clear that  $\pm a$  may be expressed through this form with three other forms analogous to  $f_2, f_3, f_4$  of Art. 276 and through every form that is equivalent to one of these four forms.

However, inversely it is *not* true that every form with determinant  $m$ , through which  $\pm a$  may be expressed, is equivalent to one of the four forms that are correlated with  $i$  and  $i'$ . For in general, there exist other ideals with norms  $\pm a$  which are not equivalent to  $i$  and with each of which may be correlated a new quadruple of quadratic forms.

If on the other hand

$$F = Ax^2 + 2Bxy + Cy^2$$

is a quadratic form with determinant  $m$ , through which an integer  $a$  may be expressed in the form

$$a = Ax_1^2 + 2Bx_1y_1 + Cy_1^2,$$

<sup>1</sup> Sommer, *Vorlesungen*, p. 207.

where  $x_1$  and  $y_1$  are relatively prime; and if  $s$  and  $u$  are two integers such that  $x_1u - y_1s = 1$ , then the unit substitution

$$(\sigma) = \begin{cases} x = x_1X + sY, \\ y = y_1Y + uY, \end{cases}$$

transforms  $F$  into its equivalent form

$$F' = aX^2 + 2b_1XY + c_1Y^2.$$

If the substitution  $(\sigma)$  is made on the form  $f$  and the resulting coefficients of  $X^2$  and  $2XY$  are equated to those of  $F'$ , we have

$$(1) \quad ax_1^2 + 2bx_1y_1 + \frac{(b^2 - m)y_1^2}{a} = a,$$

$$(2) \quad ax_1s + b(x_1u + sy_1) + uy_1 \frac{b^2 - m}{a} = b_1.$$

Multiplying (1) by  $u$  and (2) by  $y_1$ , and subtracting we have

$$(b + b_1)y_1 = a(u - x_1).$$

Since  $a$  and  $y_1$  are relatively prime, it follows that

$$b + b_1 \equiv 0 \pmod{a}.$$

From this it is seen that the form  $F'$  can only be equivalent to  $f$ , if  $b + b_1 \equiv 0 \pmod{a}$ .

To be able to determine whether  $F'$  and  $f$  are equivalent it is above all necessary to know how the integer  $b$  depends upon the quantities  $x_1, y_1, u, s$ .

Observe that the determinant of  $F'$  is  $b_1^2 - a_1c_1 = m$ , so that  $b_1$  is a root of the congruence  $x^2 - m \equiv 0 \pmod{a}$ . If  $a$  is a prime integer, this congruence may have two different roots; while there may be more than two such roots, if  $a$  is *not* a prime integer.

It may be proved that the coefficient of  $b_1$  depends, modulo  $a$ , only upon the values of  $x_1$  and  $y_1$  and does not change, modulo  $a$ , if for  $s, u$  any other pairs of values are taken which satisfy the congruence  $x_1u - y_1s = 1$ . Ob-



serve that if  $s, u$  and  $s_1, u_1$  are two solutions of this equation, then is

$$x_1(u - u_1) - y_1(s - s_1) = 0,$$

so that

$$u = u_1 + ky_1, \quad s = s_1 + kx_1,$$

where  $k$  is any integer.

The middle coefficients, see (2) above, are accordingly

$$b_1 = Ax_1s + B(x_1u + y_1s) + Cy_1u,$$

$$b_2 = Ax_1s_1 + B(x_1u_1 + y_1s_1) + Cy_1u_1.$$

Through subtraction and the substitutions  $u - u_1 = ky_1$ ,  $s - s_1 = kx_1$ , it is seen that

$$b_1 - b_2 \equiv 0 \pmod{a}.$$

It is thus shown that there exists a unique relation between  $x_1, y_1$  and  $b_1$ , and we may say that the expression of the integer  $a$  through the form  $F$  by means of the quantities  $x_1, y_1$  belongs to a definite root  $b_1$  determined through the congruence

$$x^2 - m \equiv 0 \pmod{a}.$$

We accordingly have the theorem:

**THEOREM.** *If an arbitrary<sup>1</sup> rational integer  $a$  may be expressed simultaneously through  $f$  and  $F$ , the form  $F$  is then and only then equivalent to the form  $f$ , if the expression of the integer  $a$  through  $F$  belongs to the congruence-root  $b$ .*

If finally  $\mathfrak{i}$  is an ideal which is divisible by a rational integer  $z$  and if  $\mathfrak{i}_1 = \frac{\mathfrak{i}}{z}$ , the correlated form corresponding to  $\mathfrak{i}_1$  is first derived, with determinant  $D = m$ .

The correlation of forms and ideals may be reversed: To a primitive quadratic form  $ax^2 + 2bxy + cy^2$  with determinant  $m$  there may be correlated the corresponding ideal  $(a, b + \sqrt{m})$  of the fixed realm. Hence one and the same ideal is correlated with equivalent forms (see Art. 275).

<sup>1</sup>Sommer, *Vorlesungen*, p. 209.

ART. 281. The first case, where real realms were considered and  $m \equiv 2$ , or  $m \equiv 3 \pmod{4}$ , occupied Articles 273 to 280. We shall now encounter the second case.

CASE II. The imaginary realm  $\mathfrak{K}(\sqrt{m})$ , where  $m \not\equiv 1 \pmod{4}$ . Again let  $d=4m$  be the discriminant;  $1, \omega = \sqrt{m}$ , the basis; and  $h \geq 1$  the number of classes of the realm.

If  $p$  is a rational prime integer, such that  $\left(\frac{d}{p}\right) = -1$ , and which accordingly does not admit factorization in  $\mathfrak{K}(\sqrt{m})$ , then  $p$  can not be expressed through a quadratic form with determinant  $D=m$  (Art. 273). See Sommer, bottom of p. 197.

Further observe that if

$$f = ax^2 + 2bxy + cy^2 = \frac{1}{a}[(ax + by)^2 - my^2]$$

is a form with negative determinant  $m$ , then clearly  $a$  and  $c$  must have the same sign; and the form  $f$  presents only *positive* or only *negative* integers according as  $a, c$  are positive or negative. If  $a, c$  are positive, the form is called a *positive* form, while it is called a *negative* form if  $a, c$  are negative, the determinant in either case being negative. In the consideration of such forms it is accordingly sufficient to consider the forms of one kind, say the positive, since the two kinds are completely distinct, however in all other details quite the same. Accordingly in the corresponding arrangement of forms and ideals in contrast with the first case, considered above, the only change to be made is that the discussion be limited to the forms  $f_1$  and  $f_3$  of Art. 276.

ART. 282. CASE III. If  $\mathfrak{K}(\sqrt{m})$  is a real realm where  $m \equiv 1 \pmod{4}$  and if we wish to make a similar correlation between the ideals and forms as has been done in

the preceding articles, it is seen that the two theories are not in agreement.

For let  $\mathfrak{R}(\sqrt{m})$  be such a real realm with basis: 1,  $\omega = \frac{1 + \sqrt{m}}{2}$  and discriminant  $d = m$ . Then, if as was done in Art. 274 for example in the correlation of a principal ideal  $\mathfrak{p} = (a + b\omega)$  and a principal (haupt) form, it is seen that

$$N(x + y\omega) = N\left(x + \frac{y}{2} + \frac{\sqrt{m}y}{2}\right),$$

and

$$f = x^2 + xy + \frac{1 - m}{4}y^2.$$

And in the form  $f$ , contrary to that which was found in the previous cases, the middle coefficient is not necessarily an even integer. While in Case I and Case II, the determinant of the forms was  $D = m = \frac{1}{4}d$ , we have here

$$D = \frac{1}{4} - \frac{1 - m}{4} = \frac{m}{4},$$

which is a fractional number.

Historical ground justify the wish of correlating forms of determinant  $D = m$  with the ideals of the realm. Accordingly we must first introduce an observation regarding the nature of the coefficients  $a, b, c$  of the forms with determinant  $D = m$  and of the integers which may be expressed through such forms. If  $f = ax^2 + 2bxy + cy^2$  is a quadratic form with the determinant  $D = (b^2 - ac) (\equiv 1, \text{ mod. } 4)$  and if the coefficients  $a, 2b, c$  have no common factor, in particular have *not* 2 as a common factor, then no integer which is divisible by 2 and not by  $2^2$  can be expressed through  $f$ . For if  $a$  is an odd coefficient of  $f$ , we have

$$af = (ax + by)^2 - my^2;$$

and from this it is evident that  $af$  and therefore  $f$  for

integral values of  $x, y$  is either an odd integer or  $f$  is divisible at least by  $2^2$ . Hence an integer divisible by 2 to the first and no higher power can only be expressed through  $f$  if  $a$  and  $c$  are even integers, or more exactly said, if  $a, 2b, c$  have as common factor 2 to the first power only. Forms whose coefficients  $a, 2b, c$  have 2 to the first power only and no other common factor, were called *improper primitive forms* of the determinant  $D$  (Art. 271), *proper primitive forms* being those in which  $a, 2b, c$  have only unity as a common factor. For determinants  $D(\equiv 1, \text{ mod } 4)$  which are free from quadratic factors and only for such do there exist primitive forms, improper as well as proper. (See Dirichlet-Dedekind, *Zahlentheorie*, § 61.)

An improper primitive form can never be derived through a transformation with integral coefficients from a proper primitive form. Hence, in the exposition of the present third case it is necessary at the beginning to make a distinction between the proper and improper forms. To effect this correlation of ideals and forms two ways are suggested:

*First.* Forms other than  $f$  may be put in correlation with  $\mathfrak{p}$ . For example, the improper primitive form

$$2f = 2x^2 + 2xy + 2 \cdot \frac{1-m}{4} y^2$$

together with the proper primitive forms with even middle term which may be derived from  $f$  through a substitution with determinant 2. To derive these forms differing from one another and from  $f$ , we may make the substitutions

$$(A) \begin{cases} x = x_1 \\ y = 2y_1 \end{cases} \quad (B) \begin{cases} x = -2y_1 \\ y = x_1 \end{cases} \quad (C) \begin{cases} x = x_1 + 2y_1 \\ y = -x_1 \end{cases}$$

offering, besides  $2f$ , the forms

$$f_a = x_1^2 + 2x_1y_1 + (1-m)y_1^2,$$

$$f_b = 4y_1^2 - 2x_1y_1 + \frac{1-m}{4}x_1^2,$$

$$f_c = 4y_1^2 + 2x_1y_1 + \frac{1-m}{4}x_1^2.$$

Any substitution with determinant 2 may be derived from one of the above substitutions with determinant 2 combined with another substitution with determinant unity. For if

$$x = r_1x^* + s_1y^*, \quad y = t_1x^* + u_1y^*$$

is a substitution with determinant  $r_1u_1 - s_1t_1 = 2$ , and if

$$x^* = rx_1 + sy_1, \quad y^* = tx_1 + uy_1$$

is a substitution with determinant  $ru - st = 1$ , then the combined substitution

$$x = (r_1r + s_1t)x_1 + (r_1s + s_1u)y_1$$

$$y = (t_1r + u_1t)x_1 + (t_1s + u_1u)y_1$$

has the determinant 2.

If reciprocally

$$x = Rx_1 + Sy_1, \quad y = Tx_1 + Uy_1$$

is any given substitution with determinant

$$\begin{vmatrix} R, & S \\ T, & U \end{vmatrix} = 2,$$

then integers  $r, s, t, u$ , such that  $ru - st = 1$ , may be determined so that

$$R = r_1r + s_1t, \quad S = r_1s + s_1u,$$

$$T = t_1r + u_1t, \quad U = t_1s + u_1u.$$

For example using (A) above write

$$\begin{cases} R = r, & S = s, \\ T = 2t, & U = 2u, \end{cases}$$



(with  $r_1=1$ ,  $s_1=0$ ,  $u_1=2$ ,  $t_1=0$ ); or with (B) write

$$\begin{cases} R = -2t, & S = -2u, \\ T = r, & U = s; \end{cases}$$

or with (C) write

$$\begin{cases} R = r + 2t, & S = s + 2u, \\ T = -r, & U = -s. \end{cases}$$

As a *second* method, instead of introducing proper and improper primitive forms in the realm  $\mathfrak{R}(\sqrt{m})$ , we may take certain quantities that belong to the ring  $r(\sqrt{m})$  which is contained in  $\mathfrak{R}(\sqrt{m})$ . Let  $\mathfrak{p} = (a + b\omega)$  be a principal ideal of the realm and in its place put  $(2)\mathfrak{p} = (2a + 2b\omega)$  and associate with this latter ideal the improper primitive forms

$$f_1 = 2x^2 + 2xy + 2\frac{(1-m)}{4}y^2,$$

$$f_2 = -2x^2 - 2xy - 2\frac{(1-m)}{4}y^2.$$

If further  $\mathfrak{p} = (a + b\sqrt{m})$  is a principal ideal of the ring  $r(\sqrt{m})$ , associate with it the proper primitive forms

$$f_a = x^2 - my^2,$$

$$f_b = -x^2 + my^2.$$

These two pairs of forms may be treated in detail as in the Case I, there being two additional observations to be made.

*First* it is seen that  $f_1$  and  $f_2$  are ambiguous, since they are transformed the one into the other by the substitution  $x = -x_1 - y_1$ ,  $y = y_1$  with determinant  $-1$ .

And in the *second* place as noted above in general a proper primitive form can never be equivalent to an improper primitive form as is seen at once through application of a unit substitution. The forms  $f_1$  and  $f_2$  otherwise expressed correspond to the ideal  $(2, 2\omega)$  of the

realm  $\mathfrak{R}(\sqrt{m})$ , while  $f_a$  and  $f_b$  correspond to the ideal  $(1, \sqrt{m})$  of the ring  $r(\sqrt{m})$ . If  $\mathfrak{p}$  is an arbitrary ideal different from (2) of the realm  $\mathfrak{R}(\sqrt{m})$ , there may be correlated four improper primitive forms corresponding to the ideals (2)  $\mathfrak{p}$  and (2)  $\mathfrak{p}'$ ; and to the ring ideals  $\mathfrak{p}_r$  and  $\mathfrak{p}'_r$  that may be associated with  $\mathfrak{p}$  and  $\mathfrak{p}'$  there may be correlated four proper primitive forms as in Art. 276. The essential difference between the treatment here and that in Art. 276 lies only in the introduction of two kinds of primitive forms.

CASE IV. Where  $\mathfrak{R}(\sqrt{m})$  is an imaginary realm and  $m \equiv 1 \pmod{4}$ . The distinction made here and in the third case consists in limiting the discussion once for all either to positive or negative forms of the determinant  $D = m$ .

### MULTIPLICATION OF IDEALS AND THE COMPOSITION OF FORMS

ART. 283. Through the reciprocal relations of quadratic forms<sup>1</sup> to the theory of ideals and *vice versa* a basis may be laid for the theory of quadratic forms. In the establishment of the theory, it is necessary to know in what relation the classes of forms stand to the classes of ideals. The multiplication of ideals in connection with the operations with forms is a question which will now be considered. The two cases must again be considered here: (1) where  $m \equiv 2 \pmod{4}$  or  $m \equiv 3 \pmod{4}$ , and (2)  $m \equiv 1 \pmod{4}$ .

We shall limit the discussion to cases  $m \equiv 2$  and  $m \equiv 3 \pmod{4}$ .

Let  $\mathfrak{p}$  and  $\mathfrak{q}$  be two ideals of the realm  $\mathfrak{R}(\sqrt{m})$  and put

$$\mathfrak{p} = (p, b + \sqrt{m}), \quad \mathfrak{q} = (q, b_1 + \sqrt{m}),$$

<sup>1</sup> See Sommer, *Vorlesungen*, p. 213.

whose product, being an ideal of  $\mathfrak{R}(m)$ , may be written

$$\mathfrak{p}q = (pq, B + \sqrt{m}).$$

Observe that it is always possible to determine two integers  $u$  and  $v$  such that

$$pu + b = B \quad \text{and} \quad qv + b_1 = B.$$

It follows that  $B + \sqrt{m}$  is an integer belonging both to the ideal  $\mathfrak{p}$  and to  $q$ . We may accordingly choose  $p, B + \sqrt{m}$  as basal elements of  $\mathfrak{p}$ , and likewise  $q, B + \sqrt{m}$  as basal elements of  $q$ .

Hence with the ideals  $\mathfrak{p}, q$  and  $\mathfrak{p}q$  may be correlated the forms

$$\begin{aligned} f &= px^2 + 2Bxy + \frac{B^2 - m}{p}y^2, \\ f_1 &= qx_1^2 + 2Bx_1y_1 + \frac{B^2 - m}{q}y_1^2, \\ F &= pqX^2 + 2BXY + \frac{B^2 - m}{pq}Y^2. \end{aligned}$$

Among these three forms there exists the following striking relation: since  $px + (B + \sqrt{m})y$ ,  $qx + (B + \sqrt{m})y$ ,  $pqX + (B + \sqrt{m})Y$  are integers respectively of the ideals  $\mathfrak{p}, q, \mathfrak{p}q$ , there exists through multiplication

$$[px + (B + \sqrt{m})y][qx_1 + (B + \sqrt{m})y_1] = pqX + (B + \sqrt{m})Y.$$

By equating coefficients in this expression we have

$$(\Sigma) \begin{cases} X = xx_1 - \frac{B^2 - m}{pq}yy_1, \\ Y = pxy_1 + qx_1y + 2Byy_1; \end{cases}$$

and it is clear that the form  $F$  is transformed into the product of two forms  $f$  and  $f_1$  through the substitution  $(\Sigma)$ ; and inversely the product of the two forms  $f$  and  $f_1$  is equal to  $F$ , if the variables  $x, y$  and  $x_1, y_1$  are connected through the relations  $(\Sigma)$ .

Further, correlating with the ideals  $\mathfrak{p}$  and  $\mathfrak{q}$  the forms

$$\begin{aligned}\varphi &= px'^2 + 2bx'y' + \frac{b^2 - m}{p}y'^2, \\ \varphi_1 &= qx_1'^2 + 2bx_1'y_1' + \frac{b^2 - m}{q}y_1'^2,\end{aligned}$$

it is seen that  $F$  may be expressed as the product of  $\varphi$  and  $\varphi_1$ . For the substitutions

$$\begin{aligned}x' &= x + uy, & x_1' &= x_1 + vy_1, \\ y' &= y, & y_1' &= y_1,\end{aligned}$$

change  $\varphi$  to  $f$ , and  $\varphi_1$  to  $f_1$ . For the multiplication of forms Gauss (*Disq. Arith.*, V, pp. 234 et seq.) used the notation *composition*.<sup>1</sup> The form  $F$  is said to be composed of the forms  $f$  and  $f_1$ , and can be written symbolically  $F = ff_1$ .

The same is true of the composition of forms if  $\mathfrak{p}$  and  $\mathfrak{q}$  are two ambiguous prime ideals. One may observe how the forms are related which are correlated with  $\mathfrak{p}$  and  $\mathfrak{p}^2$ . For let  $\mathfrak{p}$  be a prime ideal that is different from 2, such that, say  $\mathfrak{p} = (p, B + \sqrt{m})$ , and  $\mathfrak{p}^2 = (p^2, B + \sqrt{m})$ . If the correlated forms are

$$\begin{aligned}f &= px^2 + 2Bxy + \frac{B^2 - m}{p}y^2, \\ F &= p^2X^2 + 2BXY + \frac{B^2 - m}{p^2}Y^2,\end{aligned}$$

it is seen that  $F = f^2$ , where

$$(\Sigma_1) \begin{cases} X = x^2 - \frac{B^2 - m}{p^2}y^2, \\ Y = 2pxy + 2By^2. \end{cases}$$

By a comparison of the substitutions  $(\Sigma)$  and  $(\Sigma_1)$  observe that the special case may be derived directly from the general case.

<sup>1</sup> Smith's *Report*, pp. 231 et seq.; Dickson, Vol. III, pp. 60 et seq.

Such a composition fails only when  $p$  is a divisor of 2. For example if  $m \equiv 3 \pmod{4}$  and  $pp' = 2$ , it is seen that

$$p = (2, 1 + \sqrt{m}), \quad p^2 = (2, 2\sqrt{m}), \quad f = px^2 - \frac{m}{2}y^2,$$

where  $m$  is an odd integer.

If  $p$  is any other ambiguous ideal, we have

$$p = (p, \sqrt{m}), \quad p^2 = (p, p\sqrt{m});$$

and

$$f = px^2 - \frac{m}{p}y^2, \quad F = X^2 - mY^2.$$

It is clear that  $F = f^2$ , if the substitutions

$$X = px^2 + \frac{m}{p}y^2, \quad Y = 2xy$$

are made.

ART. 284. We must next observe how more generally two forms may be compounded, which are correlated with two ideals. Let these ideals be (see Art. 206, end)

$$i = (a, b + \sqrt{m}), \quad i_1 = (a_1, b_1 + \sqrt{m})$$

with the restriction  $(a, a_1) = 1$ , the theory being sufficiently general for the results given in the sequel. Their product is

$$ii_1 = (aa_1, a_1b + a_1\sqrt{m}, ab_1 + a\sqrt{m}, bb_1 + (b + b_1)\sqrt{m} + m).$$

Observe that

$$\begin{aligned} aa_1u + (a_1b + a_1\sqrt{m}) &= a_1(B + \sqrt{m}), \\ aa_1v + (ab_1 + a_1\sqrt{m}) &= a(B + \sqrt{m}), \end{aligned}$$

where  $B = au + b = a_1v + b_1$ .

Since  $(a, a_1) \sim 1$ , we may add  $B + \sqrt{m}$  as an element to the product just written, which becomes thereupon

$$ii_1 = (aa_1, B + \sqrt{m}).$$

Further note that  $i = (a, B + \sqrt{m})$  and  $i_1 = (a_1, B + \sqrt{m})$ .



If then with the ideals  $i$ ,  $i_1$  and  $ii_1$  are correlated the forms

$$f = ax^2 + 2Bxy + \frac{B^2 - m}{a}y^2,$$

$$f_1 = a_1x_1^2 + 2Bx_1y_1 + \frac{B^2 - m}{a_1}y_1^2,$$

$$F = aa_1X^2 + 2BXY + \frac{B^2 - m}{aa_1}Y^2,$$

we may regard  $F$  as the *product* of  $f$  and  $f_1$ . For through the multiplication of ideals it is seen that

$$[ax + By + \sqrt{m}y][a_1x_1 + By_1 + \sqrt{m}y_1] = aa_1X + (B + \sqrt{m})Y,$$

where

$$X = xx_1 - \frac{B^2 - m}{aa_1}yy_1,$$

$$Y = axy_1 + a_1x_1y + 2Byy_1.$$

These values written for  $X$  and  $Y$  offer at once the product of the two forms  $f$  and  $f_1$ .

If we correlate with the ideals  $i$  and  $i_1$ , instead of the forms  $f$  and  $f_1$ , the forms

$$\varphi = ax'^2 + 2bx'y' + \frac{b^2 - m}{a}y'^2,$$

$$\varphi_1 = a_1x_1'^2 + 2b_1x_1'y_1' + \frac{b_1^2 - m}{a_1}y_1'^2,$$

corresponding to the ideals in the original forms, namely

$$i = (a, b + \sqrt{m}), \quad i_1 = (a_1, b_1 + \sqrt{m}),$$

then on the one hand  $f$  and  $\varphi$  and on the other  $f_1$  and  $\varphi_1$  are equivalent, and it may be again shown, just as was done above in detail for  $p$  and  $q$ , that  $F$  may be expressed as the product of  $\varphi$  and  $\varphi_1$ .

It is to be observed in particular that not only the form  $F$  but also every form  $F'$  that is equivalent to  $F$  may be compounded of the same forms  $f$  and  $f_1$ .

The above treatment is also reversible: if a form  $F$  is compounded of two forms  $f$  and  $f_1$ , and if with the forms

$f$  and  $f_1$  are correlated the ideals  $i$  and  $i_1$ , then to  $F$  there corresponds the product  $ii_1$ .

ART. 285. The fundamental theorem of composition respecting the behavior of equivalent forms is the following:

THEOREM. *If two quadratic forms  $f$  and  $f_1$  are compounded into  $F$  and if two other quadratic forms  $\varphi$  and  $\varphi_1$  are compounded into  $\Phi$ , and if on the one hand  $f$  and  $\varphi$  and on the other  $f_1$  and  $\varphi_1$  are equivalent, then is  $F$  equivalent to  $\Phi$ .*

*Proof.* If any two integers  $a$  and  $a_1$  can be expressed through  $f$  and  $f_1$ , then also these integers may be expressed through  $\varphi$  and  $\varphi_1$  and the product  $a \cdot a_1$  can be expressed through both  $F$  and  $\Phi$ . Due to the following theorem, which for convenience is placed after the one we are now proving, there correspond to the forms  $f$  and  $\varphi$  equivalent ideals, as also to the forms  $f_1$  and  $\varphi_1$ . If, say,  $i$  and  $h$  correspond to the forms  $f$  and  $\varphi$ , while  $i_1$  and  $h_1$  to  $f_1$  and  $\varphi_1$ , then is  $i \sim h$ ,  $i_1 \sim h_1$  and consequently also (Art. 217)  $ii_1 \sim hh_1$ . To the ideals  $ii_1$  and  $hh_1$  there correspond, among others, the forms  $F$  and  $\Phi$ , which must be properly equivalent, since through them either positive or negative integers may be expressed.

Due to the relation between the composition of forms and multiplication of ideals there exists, as an important consequence, the relation between classes of forms and classes of ideals which is expressed through the following theorem.

THEOREM. *If  $i$  and  $i_1$  are two equivalent ideals of the realm  $\mathfrak{K}(\sqrt{m})$  each without a rational factor, the quadratic forms, which by definition are correlated with these ideals, are also equivalent in pairs.*

*Proof.* We may observe regarding the equivalence of two forms that, if two forms  $f$  and  $f_1$  may be compounded with the same principal form  $\varphi(=x^2 - my^2)$  so that the

two forms  $f\varphi = F$  and  $f_1\varphi = F_1$  are equal or equivalent in the sense of Art. 280, then are the forms  $f$  and  $f_1$  equivalent by definition in a somewhat more general sense. For it is clear that any integer  $a$  which may be expressed through  $f$  may also be expressed through  $f_1$  with both expressions belonging to the same congruence root (Art. 280).

Due to the assumption that  $i$  and  $i_1$  are two equivalent ideals, there exist two integers of the realm  $\alpha$  and  $\beta$  such that  $(\alpha)i = (\beta)i_1$ . If then the principal form  $\varphi$  is correlated with the principal ideal  $(\alpha)$  and therefore the form  $\pm\varphi$  with  $(\beta)$ , and if there is correlated with the ideals  $i, i_1, (\alpha)i = (\beta)i_1$  the forms  $f, f_1, F$ , then necessarily is  $F = \varphi f = \pm\varphi f_1$ . In fact, the forms  $\varphi, f$  on the one hand and  $\varphi, f_1$  on the other hand may be compounded by the general method above, since the coefficient  $a_1$  of  $\varphi$  is unity, thus satisfying the condition that was imposed, namely that  $a$  and  $a_1$  be relatively prime.

From the equation  $\varphi f = \pm\varphi f_1$  it follows that the forms  $f$  and  $\pm f_1$  are equivalent; and hence also the four forms which correspond to the ideals  $i$  and  $i_1$  are equivalent in pairs.

If further  $f$  and  $f_1$  are equivalent forms and if  $i$  and  $i_1$  are ideals that are correlated with these forms, then it follows *vice versa* that  $i \sim i_1$ .

With this it is also proved that to the finite number of ideal classes of the realm  $\mathfrak{K}(\sqrt{m})$  there corresponds a finite number of classes of quadratic forms with determinant  $D = m$ . This last number is at least equal, in general greater and at most four times as great as the number of classes of ideals (Gauss, *Disq. Arith.*, p. 196). With an ambiguous class of ideals (Art. 277) there corresponds an ambiguous class of forms.

It was proved (Art. 218) that in every class of ideals

there is an ideal  $\mathfrak{a}$ , say, such that  $N(\mathfrak{a}) \equiv |\sqrt{D}|$ . If  $\mathfrak{a} = (a, b + \sqrt{m})$ , then  $N(\mathfrak{a}) = a$ , while  $b$  may be reduced so that  $|b| \leq \frac{a}{2}$ . Observe that  $d = 4m$ , where  $m \equiv 1 \pmod{4}$ .

Accordingly in every class of forms with determinant  $D = m$ , there is at least one quadratic form, whose middle coefficient  $b$  and extreme coefficients  $a, c$  satisfy the conditions

$$|b| \leq |\sqrt{m}|, \quad |a| \leq 2|\sqrt{m}| \quad \text{and} \quad |a| \geq |c|.$$

These are the conditions of a so-called *reduced* form (Dirichlet-Dedekind, *Zahlentheorie*, pp. 176 et seq.) namely

$$0 < b < \sqrt{D}, \quad 0 < \sqrt{D} - b < |a| < \sqrt{D} + b, \quad |a| \geq |c|$$

(Gauss, *Disq. Arith.*, p. 196, Prob. 4).

With this the analogy of the quadratic forms with the theory of ideals is again put into evidence. And it is clear that all such conceptions as the multiplication of classes, distribution of classes into genera,<sup>1</sup> character-system of a genus have their prototypes in either theory.

**EXAMPLE.** Derive results analogous to the above for realms  $\mathfrak{R}(\sqrt{m})$ , where  $m \equiv 1 \pmod{4}$ .

*Remark.* On p. 66 of the *Evanston Colloquium Lectures* Felix Klein wrote: "It is true that we have here spoken only of complex numbers containing square roots, while the researches of Kummer himself and of his followers, Kronecker and Dedekind, embrace all possible algebraic numbers. But our methods are of universal application; it is only necessary to construct lattices in spaces of higher dimensions." Again on p. 58 of the *Evanston Lectures* Klein wrote: "Recent investigations have made it clear that there exists a very intimate correlation between the Theory of Numbers and other departments of Mathematics, not excluding geometry.

<sup>1</sup> See Smith's "Report on the Theory of Numbers," *Collected Works*, Vol. I, p. 202. See also Gauss, *Disq. Arithm.*, Arts. 153-233.

“As an example I may mention the theory of the binary quadratic forms as treated in the *Elliptische Modulfunctionen*. An extension of this method to higher dimensions is possible without serious difficulties. Another example is found in the paper of Minkowski, ‘Ueber Eigenschaften von ganzen Zahlen, die durch räumliche Anschauung erschlossen sind,’ *Collected Works*, Vol. I, p. 270. Here geometry is used directly for the development of new arithmetical ideas.”

The author believes that one will reap richly the fruits of his labor, if he will first read Minkowski, “Zur Theorie der quadratischen Formen,” *Works*, Vol. I, pp. 6–239, in connection with Minkowski, *Die Geometrie der Zahlen*. The theories of this wonderful mathematician, who died all too young, still remain to be fully developed.



## CHAPTER XIII

### GEOMETRIC PRESENTATION OF IDEALS

#### IMAGINARY REALMS

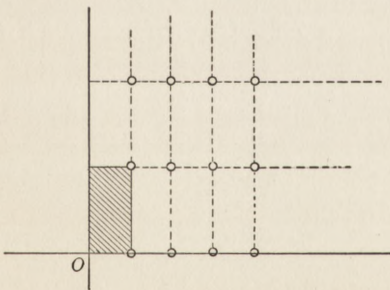
ART. 286. The theory of the ideals of the quadratic realms admits of interesting geometrical interpretations. These offer a close analogy with certain physical studies, for example mineralogy, in particular crystallography, etc. The sequence of analogies of pure analysis, geometry, etc., with physical subjects should never be lost sight of. They should always be emphasized. There are close analogies also with metaphysical subjects combined with physical subjects, for example, the analogy among ideals, the ideal numbers of Plato, chemistry, etc. See a paper by the author in *The American Math. Monthly*, Vol. 35, p. 282.

In the geometric treatment of ideals a distinction is to be made between the pure and imaginary realms, as has been done in their analytic development.

We shall first consider the imaginary realms and for this purpose we may employ the realm  $\mathfrak{R}(\sqrt{-5})$  which

has been repeatedly introduced. The number of ideal classes  $h$  is two.

Take two axes intersecting at right angles with the origin as usual at the intersection. On the real ( $x$ -axis) lay off unit distances and on the



imaginary axis ( $y$ -axis) lay off distances of length  $\sqrt{5}$ . The integers of the realm are those points of the plane expressed through the formula

$$a + b\sqrt{-5},$$

where  $a$  and  $b$  are any rational integers. The plane is thus covered with what may be called *unit rectangles* the vertices of which are algebraic integers in  $\mathfrak{R}(\sqrt{-5})$ . The points thus obtained constitute the *lattice-points*<sup>1</sup> of the realm. We shall call them the *fundamental set* of lattice-points. When a system of lines is made connecting these points we have what may be called a *lattice*.

Thus corresponding to the one system of points there may be drawn many different lattices. A parrellogram that contains no lattice points within its interior is called an *elementary parallelogram* of the lattice, or a *mesh*. A lattice is completely determined through a position and the dimension of a mesh. The meshes completely cover the plane.

**THEOREM.** *Through the lattice-points an indefinite number of different lattices may be laid.*

*Proof.* Take any lattice-point  $A$  and any other lattice-point  $B$ , so that the line  $AB$  does not go through a lattice-point between  $A$  and  $B$ . Continue the line in either direction through  $A$  and  $B$ . On this line at distances  $AB$  are situated an indefinite number of lattice-points. This line divides the plane into two halves. On either side of it draw parallel lines through the lattice-points. On these lines the lattice points are at distances  $AB$  from one another. On the line that is nearest to  $AB$  take any lattice point  $C$  and draw  $AC$ . Let  $D$  be the next point on this line parallel to  $AB$ . The distance  $CD$  is equal to  $AB$ . Join  $BD$  and it is seen that there can be no lattice-point in

<sup>1</sup> *Encyklopaedie der math. Wissenschaften*, Vol. I, pp. 606-616.

$ABCD$ , which accordingly is an elementary parallelogram or mesh. Extend the line  $AC$  in either direction from  $A$  and  $C$  and mark off the lattice-points at intervals  $AC$  on this line. Lines drawn through these points, parallel to the line  $AB$  will, with the first system of parallel lines, divide the entire plane into elementary parallelograms or meshes. It may be proved that were there a lattice-point within one of these meshes, there would also be one within  $ABCD$ .

By taking the lines through  $AB$  and  $AC$  as oblique axes, and denoting the lengths  $AB$  and  $AC$  by  $\omega_1$  and  $\omega_2$ , it is seen that all lattice-points may be had through the formula

$$x_1\omega_1 + x_2\omega_2,$$

where  $x_1$  and  $x_2$  take all positive and negative rational integral values; and that is,  $\omega_1, \omega_2$  from a basis of all the integers of the algebraic realm  $\mathfrak{R}(\sqrt{-5})$ , the lattice-points being geometric images of all algebraic integers of the realm. The arithmetic interpretation of what has just been given, is: there are an infinite number of ways of choosing two pairs of values  $\omega_1, \omega_2$  in every realm so that  $x_1\omega_1 + x_2\omega_2$  will, with rational integral values of  $x_1$  and  $x_2$ , give all the integers of the algebraic realm. And reciprocally, if  $\omega_1$  and  $\omega_2$  form a basis of the realm, then  $0, \omega_1, \omega_2, \omega_1 + \omega_2$  form the four vertices of the initial mesh. The quantities  $\omega_1, \omega_2$  give the direction of the coördinate axes and the unit lengths on these axes.

If  $\omega_1^*, \omega_2^*$  form another basis that is different from  $\omega_1, \omega_2$ , we saw (Art. 206, end) that

$$(S_1) \begin{cases} \omega_1^* = r\omega_1 + s\omega_2, \\ \omega_2^* = t\omega_1 + u\omega_2, \end{cases}$$

where  $ru + st = \pm 1$ .

Observing that

$$\omega_1^*x + \omega_2^*y = (rx + ty)\omega_1 + (sx + uy)\omega_2,$$

it is seen that the new variables

$$(S_2) \begin{cases} x_1 = rx + ty, \\ y_1 = sx + uy, \end{cases} \quad ru - st = \pm 1,$$

offer a transformation from one system to another. The coördinates  $x, y, x_1, y_1$  are in all cases rational integers. The direction of the coördinate axes are determined through  $\omega_1, \omega_2$  and  $\omega_1^*, \omega_2^*$ . With the exception of the origin, every lattice point is transformed into another lattice point. The transformations  $(S_1)$  and  $(S_2)$  are said to be *contragredient*. It is seen that the area of every mesh that determines a lattice is constant. The above results may be summarized as follows:

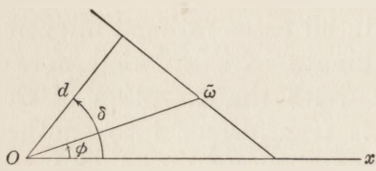
*To the integers of a quadratic realm there correspond the points of a lattice. These points we have called the fundamental set of lattice-points. Through the lattice-points an indefinite number of lattices may be laid, whose meshes are all of the same area. Every lattice corresponds to a definite basis of the realm. Any two lattices are analytically connected through a linear transformation with determinant  $\pm 1$ , and this transformation is contragredient to the one that connects the corresponding pairs of bases.*

The product, sum or difference of any two lattice-points is a lattice-point. To prove this we need only write a complex integer in place of the lattice-point and employ the usual rules for complex numbers.

ART. 287. If  $\alpha$  is an algebraic integer, the principal ideal  $(\alpha)$  consists of the collectivity of all the integers of the realm which are divisible by  $\alpha$ . And this means geometrically all those lattice-points which are obtained by the multiplication of the fundamental set of lattice-points by  $\alpha$ . It is clear that these points also form a system of lattice-points. Thus the lattice-points are merely the integers of the principal ideal  $(\alpha)$ . To

illustrate this take  $\alpha = 1 + \sqrt{-5}$ , an integer in  $\mathfrak{R}(\sqrt{-5})$ . Multiply the points that lie on a line of the fundamental set by  $\alpha$ . The resulting points also lie on a line. For denote the inclination that the quantity  $\alpha$  makes with the  $x$ -axis by  $\hat{\alpha}$ , so that

therefore  $\alpha = \bar{a}e^{i\hat{\alpha}}$ , where  $\bar{a}$  denotes the absolute value of  $\alpha$ . Observe that if  $\bar{\omega} = re^{i\varphi}$  is any point on a line, its co-



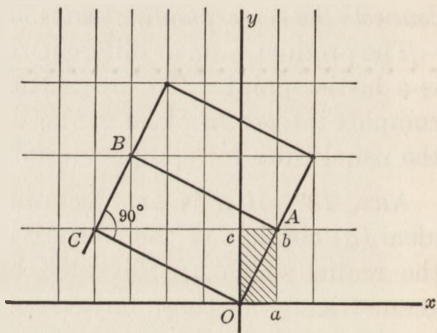
ordinates satisfy the equation

$$r \cos (\delta - \varphi) = d,$$

where  $d, \delta$  are the length and inclination of the perpendicular from the origin to the line. A similar equation may be had through the multiplication of  $\alpha$  and  $\bar{\omega}$ . It is further seen that points which lie in two parallel lines (in which therefore  $\delta$  is the same) when multiplied by  $\alpha$  offer points that lie on two parallel lines. Also observe, since  $\alpha\bar{\omega} = \bar{a}re^{i(\varphi+\hat{\alpha})}$ , that a vector drawn through the origin is turned through an angle  $\hat{\alpha}$  and stretched in the ratio

$\bar{a}r : r$ , so that therefore every figure is transformed into a similar figure. Since the ideal  $(\alpha)$  is derived from the ideal (1) through multiplication with  $\alpha$ , it is seen that the ideal  $(\alpha)$  with elementary

parallelogram  $ABCO$  is similar to the lattice (1) with parallelogram  $abco$ .



For observe that the complex quantities

$$o, a, b, c, \\ 0, 1, 1 + i\sqrt{5}, i\sqrt{5},$$



multiplied by  $\alpha = 1 + i\sqrt{5}$  are

$$\begin{array}{cccc} 0, & 1 + i\sqrt{5}, & -4 + 2i\sqrt{5}, & -5 + i\sqrt{5}, \\ O, & A, & B, & C. \end{array}$$

From this it is seen that *similar lattices correspond to all principal ideals, the ideal (1) being the fundamental lattice.*

Analytically it is seen that the derivation of the lattice ( $\alpha$ ) from the principal lattice (1) may be brought about by means of a linear transformation upon the latter.

For put  $\alpha = u + v\sqrt{-5}$ , where  $u$  and  $v$  are rational integers and denote points of the fundamental lattice by  $x + y\sqrt{-5}$  while those of the lattice ( $\alpha$ ) are expressed by  $X + Y\sqrt{5}$ , where  $x, y, X, Y$  are rational integers. It is seen that

$$\begin{aligned} X &= ux - 5vy, \\ Y &= vx + uy, \end{aligned}$$

with determinant

$$|\alpha| = u^2 + 5v^2.$$

Mark off the points that are the vertices of the lattice ( $\alpha$ ). Through these an infinite number of lattices may be laid whose meshes have a constant area precisely in the same way as was done for the indefinite number of lattice-points that were laid through the fundamental lattice-points. (Sommer, *Vorlesungen*, p. 227.)

Corresponding to every basis of the ideal ( $\alpha$ ), for example  $\alpha, \alpha\sqrt{-5}$ , there may be associated a lattice whose elementary parallelogram has as vertices the points  $O, \alpha, \alpha\sqrt{-5}, \alpha + \alpha\sqrt{-5}$ . To the different bases there correspond different lattices, that are connected through linear transformations with determinant 1. For example in the figure above  $OA = \omega_1 = 1 + i\sqrt{5}$ ,  $OC = \omega_2 = -5 + i\sqrt{5}$ ; and if we put

$$\begin{aligned} \omega_1^* &= r\omega_1 + s\omega_2, \\ \omega_2^* &= p\omega_1 + q\omega_2, \quad rq - sp = 1, \end{aligned}$$

we have a different lattice, the vertices of the elementary

parallelogram being  $O, \omega_1^*, \omega_1^* + \omega_2^*, \omega_2^*$ . The area of the meshes in both cases is  $6\sqrt{5}$ . Accordingly we have the theorem:

**THEOREM.** *With any ideal  $(\alpha)$  there may be associated a set of lattice-points that is similar to the fundamental set of lattice-points. Through this set of lattice points may be laid an indefinite number of lattices each defined by a basis of the ideal  $(\alpha)$ . Any two such lattices are connected by a linear transformation with determinant  $\pm 1$ . This transformation is contragredient to the transformation which connects the pair of bases, that correspond to the two lattices. All such lattices have meshes of constant area.*

**ART. 288.** The ideal (1) corresponds to the fundamental set of lattice points. The ideal  $(\alpha)$  corresponds to a similar set of lattice-points, there being fewer such points within the area which includes one or more meshes of the fundamental lattice. The question then is: how many lattice-points of the fundamental lattice lie on the sides and within a mesh of the lattice  $(\alpha)$ ?

In this enumeration we shall count as belonging to a definite mesh:

1. One vertex of the mesh, so that therefore every vertex belongs only to one mesh;
2. All those lattice points that lie on the two sides of the mesh that intersect at the vertex that is counted as belonging to the mesh;
3. All points on the interior of the mesh.

Since all the meshes contain the same number of lattice-points of the fundamental lattice, we shall take, for the determination of this number, that mesh which belongs to the normal basis of the ideal  $(\alpha)$ . Writing as above  $\alpha = u + v\sqrt{-5}$ , let  $t$  be the greatest common divisor of  $u$  and  $v$ , so that  $u = \bar{u}t, v = \bar{v}t$ . It is seen that

$$(\alpha) = (u + v\sqrt{-5}) = t(\bar{u} + \bar{v}\sqrt{-5}) = t(\bar{u} + \bar{v}\sqrt{-5}, \bar{u}^2 + 5\bar{v}^2),$$

since the norm of any basal element may be added as an element of an ideal. It follows that (see Art. 206, where  $i$  is divisible by  $i_2(=t)$ ),

$$(\alpha) = \left( u + v\sqrt{-5}, \frac{u^2 + 5v^2}{t} \right) = \left( \frac{u^2 + 5v^2}{t}, i_1 + t\sqrt{-5} \right).$$

If this mesh is so laid that the side  $\frac{u^2 + 5v^2}{t}$  lies on the  $x$ -axis, it is seen that this side contains  $\frac{u^2 + 5v^2}{t}$  of the initial lattice-points, while there are  $t$  such points on the other side. In all there are  $u^2 + 5v^2 = N(\alpha)$  such points. And these points constitute (mod.  $\alpha$ ) a complete system of incongruent integers that belong to the realm  $\mathfrak{R}(\sqrt{-5})$ . Accordingly we have:

**THEOREM.** *Every mesh of the lattice  $(\alpha)$  contains  $N(\alpha)$  of the fundamental lattice-points, and these points constitute a complete system of incongruent (mod.  $\alpha$ ) integers of the realm.*

**ART. 289.** Instead of the principal ideal  $(\alpha)$  consider next any arbitrary ideal  $i$  with basal elements  $\iota_1, \iota_2$  so that

$$i = (\iota_1, \iota_2, x\iota_1 + y\iota_2),$$

where  $x$  and  $y$  are any arbitrary rational integers. Corresponding to this ideal there is a lattice with mesh having  $O, \iota_1, \iota_2, \iota_1 + \iota_2$  as vertices. By giving to  $x$  and  $y$  all possible integral values, we derive lattice-points corresponding to the integers of  $i$ . Besides the lattice just written, an indefinite number of other lattices may be laid through these points corresponding respectively to the pairs of basal elements through which the ideal may be expressed. In all these lattices the meshes are of constant area.

The number of lattice points of the fundamental lattice (which corresponds to the ideal (1)), which lies within one of these lattices, is equal to the absolute value of the norm and that is  $|N(i)|$ . And the numbers that correspond to these points constitute (mod.  $i$ ) a complete system of incongruent integers of the realm.

Let  $i$  and  $i_1$  be two ideals of the realm  $\mathfrak{R}(\sqrt{-5})$  that are not principal ideals and which belong to the same class, so that  $(\alpha)i = (\alpha_1)i_1$ , where  $\alpha$  and  $\alpha_1$  are integers of the realm.

Write  $i$  in a form (Art. 206) free from rational integral factors  $i = (a, b + \sqrt{-5})$  and also write  $i_1 = (A, B + \sqrt{-5})$  so that  $N(i) = a$  and  $N(i_1) = A$ . Further let  $\alpha = c + \sqrt{-5}d$  and  $\alpha_1 = C + \sqrt{-5}D$  where  $c, d, C, D$  are rational integers, with the norms  $N(\alpha) = c^2 + 5d^2$ ,  $N(\alpha_1) = C^2 + 5D^2$ . Due to the relation

$$(1) \quad (\alpha)i = (\alpha_1)i_1,$$

we have

$$N(\alpha)N(i) = N(\alpha_1)N(i_1).$$

Writing

$$i = ax + by + \sqrt{-5}y, \quad i_1 = AX + BY + \sqrt{-5}Y,$$

where  $x, y, X, Y$  are arbitrary rational integers, we have from (1), when the real and imaginary forms are equated on either side of the equation,

$$(2) \quad \begin{cases} cax + (cb - 5d)y = CAX + (CB - 5D)Y, \\ dax + (bd + c)y = DAX + (BD + C)Y. \end{cases}$$

From these two relations it is seen that

$$x = \frac{A}{aN(\alpha)} \left\{ C(bd + c) - D(cb - 5d)X + \frac{1}{aN(\alpha)} \right. \\ \left. \times [(CB - 5D)(bd + c) - (cb - 5d)(BD + C)]Y \right\},$$

$$y = \frac{A}{N(\alpha)} [cD - dC]X + \frac{1}{N(\alpha)} [c(BD + C) - (CB - 5D)d]Y,$$

with determinant

$$\begin{aligned} \Delta &= \frac{A}{aN(\alpha)^2} \left\{ \begin{aligned} &[b(cD - dC) - 5(Dd + Cc)] \\ &\quad \times [B(Cd - Dc) - (5Dd + Cc)] \\ &\quad + (dC - cD)(CB - 5D)(bd + c) \\ &\quad - (BD + C)(cb - 5d) \end{aligned} \right\} \\ &= \frac{A}{aN(\alpha)^2} \left\{ \begin{aligned} &[b(cD - dC) - 5(dD + Cc)] \\ &\quad \times [B(Cd - Dc) - (5Dd + Cc)] + (dC - cD) \\ &\quad \times [Bb(Cd - Dc) + B(cC + 5Dd) \\ &\quad - b(cC + 5Dd) - 5(Dc - Cd)] \end{aligned} \right\} \\ &= \frac{A}{aN(\alpha)^2} [5(Dc - dC)^2 + (5Dd + Cc)^2] \\ &= \frac{A}{aN(\alpha)^2} [(C^2 + 5D^2)(c^2 + 5d^2)] = \frac{AN(\alpha_1)}{aN(\alpha)} = 1. \end{aligned}$$

Reciprocally, if from (2) we express  $X, Y$  in terms of  $x, y$ , which is done by changing the capitals above into small letters, and *vice versa* and then  $\alpha$  into  $\alpha_1$ , it is seen that the determinant of the resulting linear forms is

$$\Delta_1 = \frac{aN(\alpha)}{AN(\alpha_1)} = 1.$$

As in Art. 289, corresponding to the lattice that connects the integers of the ideal  $i$  there is a similar lattice that connects the points of  $(\alpha)i$ . The same is true of the ideals  $i_1$  and  $(\alpha_1)i_1$ . Hence if  $(\alpha)i = (\alpha_1)i_1$ , the lattices corresponding to  $i$  and  $i_1$  are similar. And due to the results of this article the meshes of the lattices that correspond to the ideals  $(\alpha)i$  and  $(\alpha_1)i_1$  are of equal area.

Observe that the lattice that corresponds to the product of the two ideals  $i$  and  $i_1$  contains all those lattice-points that are common to these ideals. If all the points that belong to both ideals  $i$  and  $i_1$  are formed into another ideal  $\mathfrak{J}$ , the greatest common divisor of the first two, the corresponding lattice is had by superposing one of the ideals  $i$  on the other  $i_1$ .



ART. 290. The preceding theorems are immediately applicable to all realms  $\mathfrak{R}(\sqrt{m})$  for which  $m \not\equiv 1 \pmod{4}$ . If  $m \equiv 1 \pmod{4}$ , the integers of the realm are obtained through  $\gamma = x + y \frac{(1 + \sqrt{m})}{2}$ , where  $x$  and  $y$  go over all rational integral values. The lattice-points of the fundamental lattice are the set of points of an oblique system of coördinates, so chosen that the origin is at the point  $O$  and the unit points lie on the coördinate axes at the points 1, and  $\frac{1 + \sqrt{m}}{2}$ .

Among the lattices that may be laid through the fundamental set of lattice-points (of the realm) there are none that offer a rectangular mesh. A fundamental mesh may be taken with vertices  $O, \frac{1 + \sqrt{m}}{2}, 1, \frac{1 - \sqrt{m}}{2}$ .

As seen in Art. 294, the units of the given realm that are different from  $\pm 1$  offer certain symmetric properties of the lattice-points. In all other respects, the results of the preceding articles apply literally for the present case where  $m \equiv 1 \pmod{4}$ .

ART. 291. The geometric interpretation that the number of classes  $h$  of an algebraic realm  $\mathfrak{R}(\sqrt{m})$  is finite, may be expressed as follows:

THEOREM. *The indefinite number of lattices that may be laid through the lattice-points of the realm may be distributed into  $h$  classes, so that all lattices of a class are similar to one another and only these may be transformed into one another by linear transformations.*<sup>1</sup>

We saw that the meshes of all the different lattices that could be laid through any one set of lattice-points were of constant area. This area for any ideal  $i = (i, i_1 + i_2\omega)$ ,

<sup>1</sup> See Klein, *Ausgew. Kapitel der Zahlentheorie*, Vol. II, pp. 94 et seq.

$N(i) = i\bar{i}$ , may be calculated as follows. From the figure it is seen that the area in question is

$$OA \cdot BD = i\bar{i}\omega = \frac{N(i) |\sqrt{d}|}{2}.$$

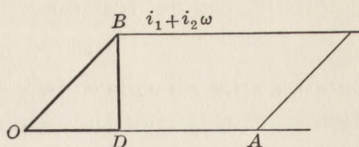
Since in every ideal-class there is at least one whose norm is less than  $|\sqrt{d}|$

(Art. 218), we have the theorem:

**THEOREM.** *In each of the  $h$  classes of similar lattices there is at least one lattice, whose area is less than  $\frac{|d|}{2}$ .*

As a lattice represents an ideal, and an ideal in normal form is as given above, it follows in every lattice whose mesh is  $< \frac{|d|}{2}$ , that an elementary parallelogram may be

laid whose sides are less than  $|d|$  and  $\frac{|\sqrt{d}|}{2}$ , respectively.



### REAL REALMS

**ART. 292.** To give a geometric meaning of the ideals in a real realm  $\Re(\sqrt{m})$  corresponding to the results established in the preceding Articles for the imaginary realms, we may introduce a *pseudometric*<sup>1</sup> geometry in the place of the Euclidian-Cartesian.

Corresponding to the Cartesian method we may introduce a rectangular system of coördinates with zero as the origin and lengths 1 and  $\sqrt{m}$  laid off on the  $x$ -axis and  $y$ -axis respectively. With this system of coordinates, we must define:

- (1) the *distance* between two points;
- (2) the *angle* between two straight lines;
- (3) the *area* of a finite closed figure.

<sup>1</sup> Klein, *loc. cit.*, pp. 50 et seq. and p. 71; and *Math. Annalen*, Vol. 48, p. 562. See also G. B. Matthews, *Theory of Numbers*, pp. 103-131.

1. First let  $x, y\sqrt{m}$  or  $(x, y)$  be any one of the lattice-points, say  $P$ , the origin  $O$  being the point  $(0, 0)$ . By definition the expression

$$r = +\sqrt{x^2 - my^2}$$

denotes the distance  $OP$ . All points which lie at a distance  $r=1$  from the origin satisfy the equation

$$1 = x^2 - my^2,$$

a real hyperbola, which has its real axis on the  $x$ -axis.

This hyperbola is the *standard curve* for the pseudo-metric distances. It defines a definite unit-length on every line that is drawn through the origin, cutting the hyperbola, the unit-length being constant for the line which determines it. This hyperbola corresponds to the Cartesian circle  $x^2 + y^2 = 1$ .

All points which lie on either of the asymptotes

$$x - \sqrt{m}y = 0, \quad \text{and} \quad x + \sqrt{m}y = 0$$

are at a distance zero from the origin, since for any point on an asymptote we have

$$r = \sqrt{x^2 - my^2} = 0.$$

The asymptotes play a peculiar rôle in this pseudo-metric geometry. They correspond to the lines  $x \pm iy = 0$  of the Cartesian geometry.

Due to the fact that any two points of an asymptote are at zero-distances apart, the asymptotes may be called *minimal* lines, which name is also applied to the lines

$$x + iy = 0.$$

All points which lie within the same angles included by the asymptotes as the hyperbola, have real distances from the origin. Points that lie in either of the other angles have imaginary distances, since for them  $x^2 - my^2$  is negative. However for these imaginary distances, the *real* hyperbola

$$x^2 - my^2 = -1$$

may be used as the standard curve of reference, the factor  $i$  being multiplied into any measurements derived from the first hyperbola.

If  $x, y\sqrt{m}$ , and that is  $(x, y)$ , are the coördinates of any point  $P$  and if  $(x_1, y_1)$  are the coördinates of a second point  $P_1$ , by definition the distance  $r$  between these points is

$$r = +\sqrt{(x-x_1)^2 - m(y-y_1)^2}.$$

2. To determine<sup>1</sup> the *inclination* of any radius  $r = OP$  with the  $x$ -axis, the following artifices may be used:

Introducing the hyperbolic functions, we may write

$$x + y\sqrt{m} = r(\operatorname{ch}\varphi + \operatorname{sh}\varphi),$$

where

$$x = r\operatorname{ch}\varphi, \quad \sqrt{m}y = r\operatorname{sh}\varphi.$$

By definition the angle  $\varphi$  thus determined is the inclination of the radius  $OP$  with the  $x$ -axis.

It may be well to insert here some of the fundamental relations among the *hyperbolic functions*. By definition

$$\operatorname{ch}\varphi = \frac{e^\varphi + e^{-\varphi}}{2}, \quad \operatorname{sh}\varphi = \frac{e^\varphi - e^{-\varphi}}{2},$$

so that

$$\operatorname{ch}(-\varphi) = \operatorname{ch}\varphi, \quad \operatorname{sh}(-\varphi) = -\operatorname{sh}\varphi.$$

It follows that

$$\operatorname{ch}\varphi + \operatorname{sh}\varphi = e^\varphi, \quad \operatorname{ch}\varphi - \operatorname{sh}\varphi = e^{-\varphi},$$

with the relations

$$\begin{aligned} (\operatorname{ch}\varphi + \operatorname{sh}\varphi)(\operatorname{ch}\varphi_1 + \operatorname{sh}\varphi_1) &= \operatorname{ch}(\varphi + \varphi_1) + \operatorname{sh}(\varphi + \varphi_1), \\ (\operatorname{ch}\varphi + \operatorname{sh}\varphi)(\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) &= \operatorname{ch}(\varphi - \varphi_1) + \operatorname{sh}(\varphi - \varphi_1), \\ (\operatorname{ch}\varphi - \operatorname{sh}\varphi)(\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) &= \operatorname{ch}(\varphi + \varphi_1) - \operatorname{sh}(\varphi + \varphi_1), \\ (\operatorname{ch}\varphi + \operatorname{sh}\varphi) \div (\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) &= \operatorname{ch}(\varphi - \varphi_1) + \operatorname{sh}(\varphi - \varphi_1), \\ (\operatorname{ch}\varphi + \operatorname{sh}\varphi) \div (\operatorname{ch}\varphi_1 + \operatorname{sh}\varphi_1) &= \operatorname{ch}(\varphi + \varphi_1) + \operatorname{sh}(\varphi + \varphi_1), \\ (\operatorname{ch}\varphi - \operatorname{sh}\varphi) \div (\operatorname{ch}\varphi_1 - \operatorname{sh}\varphi_1) &= \operatorname{ch}(\varphi - \varphi_1) - \operatorname{sh}(\varphi - \varphi_1). \end{aligned}$$

Due to these formulas the multiplication of two numbers

<sup>1</sup> Sommer, *Vorlesungen*, p. 236.

$x+y\sqrt{m}=r(ch\varphi+sh\varphi)$  and  $x_1+y_1\sqrt{m}=r_1(ch\varphi_1+sh\varphi_1)$  is accomplished in a manner analogous to that for the multiplication of two complex numbers.

To determine the inclination  $\varphi$  of the radius  $OP$  use may be made of the two equations

$$x+y\sqrt{m}=re^{\varphi}, \quad x-y\sqrt{m}=re^{-\varphi},$$

or

$$e^{2\varphi} = \frac{x+y\sqrt{m}}{x-y\sqrt{m}}.$$

It follows that

$$\varphi = \frac{1}{2} \log \frac{x+y\sqrt{m}}{x-y\sqrt{m}},$$

where the real value of the logarithm is here meant. Observe that imaginary values might enter since

$$e^{2\varphi} = e^{2\varphi+2\pi ik}.$$

Further, a distinction is to be made among the radii  $OP$  which lie within the angles made by the asymptotes and in which the hyperbola lies, and those radii which lie without these angles, and that is, those which do not cut the hyperbola  $x^2-my^2=1$ .

In the first case  $x^2-my^2$  is positive, so that the norm of the integer  $x+y\sqrt{m}$  is positive, and therefore  $r$  is real.

In this case

$$\varphi = \frac{1}{2} \log \frac{x+y\sqrt{m}}{x-y\sqrt{m}} = \frac{1}{2} \log \frac{(x+y\sqrt{m})^2}{N(x-y\sqrt{m})},$$

so that  $\varphi$  is a real angle.

In the second case, where  $x^2-my^2 < 0$ , it is seen that  $N(x+y\sqrt{m})$  is negative. It follows that

$$\begin{aligned} \varphi &= \frac{1}{2} \log \frac{(x+y\sqrt{m})^2}{N(x-y\sqrt{m})} \\ &= \frac{1}{2} \log \left[ -\frac{(x+y\sqrt{m})^2}{N(x-y\sqrt{m})} \right] + \frac{1}{2} \log (-1), \end{aligned}$$



or  $\varphi = |\varphi| + \frac{1}{2}i\pi$ , which is a complex quantity. The angle between two radii is by definition the difference between the inclinations  $\varphi - \varphi_1$ , a fixed sign  $\pm$  having been chosen to indicate a fixed direction. Two radii which are separated by an asymptote include a *complex* angle, while the included angle is real if no asymptote lies between the radii.

From the formula for  $\varphi$  it follows that every asymptote incloses with the  $x$ -axis, as well as with any arbitrary radius  $OP$ , an indefinitely large angle.

3. The area is defined by choosing for a surface unit a square whose side has the length unity in the ordinary sense, the surface area being computed by the usual methods of geometry and integration. For example the parallelogram, whose vertices are  $O$ ,  $a + b\sqrt{m}$ ,  $a_1 + b_1\sqrt{m}$ ,  $a + a_1 + (b + b_1)\sqrt{m}$ , has the area

$$S = \begin{vmatrix} a, & b\sqrt{m} \\ a_1, & b_1\sqrt{m} \end{vmatrix} = (ab_1 - a_1b)\sqrt{m}.$$

The mesh of the lattice points of the integers of the realm  $\Re(\sqrt{m})$ , which, as in the preceding case shall be called the fundamental lattice, has the area  $\sqrt{m}$ .

With these assumptions the fundamental operations of addition, subtraction, multiplication and division hold good for the points of the lattice as for the integers of the realm. For multiplication it is necessary to add the inclinations of the radii and multiply their radius-vectors  $r$  and  $r_1$ .

ART. 293. A principal ideal  $(\alpha)$  is represented through a set of points which consists of those points of the fundamental lattice that are divisible by  $\alpha$ .

The expression of the ideal  $(\alpha)$  through any basis, for example  $\alpha$  and  $\alpha\sqrt{m}$ , in the form

$$(\alpha) = (\alpha, \alpha\sqrt{m}, \alpha x + \alpha\sqrt{m}y),$$

where  $x$  and  $y$  are rational integers, shows again that an indefinite number of lattices may be drawn through any fixed set of lattice-points that cover the plane.

The set of points that express the ideal  $(\alpha)$  is had if each point of the fundamental lattice is multiplied by  $\alpha$ . Let  $\alpha = a + b\sqrt{m} = \bar{a}e^{\hat{\alpha}}$ , say, and let  $x + y\sqrt{m} = r \cdot e^{\varphi}$  be any arbitrary point of the fundamental lattice. Then for the product of these points we have

$$ax + bym + (bx + ay)\sqrt{m} = \bar{a}r \cdot e^{(\hat{\alpha} + \varphi)} = X + Y\sqrt{m}.$$

And from this follows the theorem:

*Every lattice-point of the principal ideal  $(\alpha)$  is had from one of the points of the fundamental lattice by a turning of the radius vector of the lattice-point through an angle  $\hat{\alpha}$  and a stretching of it in the ratio  $\bar{a} : 1$ .*

In other words, the set of lattice-points  $(\alpha)$  depends upon those of the fundamental lattice through a substitution

$$\begin{aligned} X &= ax + bym, \\ Y &= bx + ay, \end{aligned}$$

with determinant  $a^2 - b^2m = \bar{a}^2$ .

In this transformation a distinction must be made according as the determinant  $\bar{a}^2$  is positive, or negative. If  $\bar{a}^2$  is *positive*, in the theorem above the angle

$$\hat{\alpha} = \frac{1}{2} \log \frac{(a + b\sqrt{m})^2}{\bar{a}^2}$$

is *real* and we have to do with a turning in the usual sense.

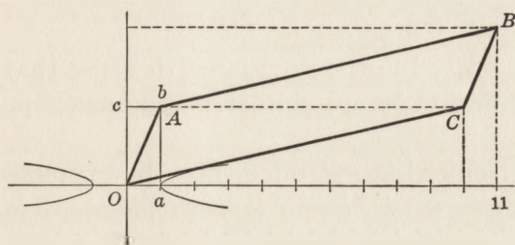
If, however,  $\bar{a}^2$  is *negative*, and therefore  $\bar{a}$  imaginary, we have

$$\hat{\alpha} = \frac{1}{2}i\pi + \frac{1}{2} \log \left[ -\frac{(a + b\sqrt{m})^2}{\bar{a}^2} \right],$$

which is a complex angle; and there is situated an asymptote between the initial and final positions of the radius.

This *improper* turning may be regarded as a combination of a *proper* turning through a real angle  $\frac{1}{2} \log \left[ -\frac{(a+b\sqrt{m})^2}{\bar{a}^2} \right]$  in which the radius does not pass out of the angle between two asymptotes and of a *reflection* about an asymptote.

As an example, consider the following figure which corresponds to the realm  $\Re(\sqrt{10})$  in which the number of



classes is  $h=2$ . From the points of the fundamental lattice  $O=0$ ,  $a=1$ ,  $b=1+\sqrt{10}$ ,  $c=\sqrt{10}$ , we have the corresponding points of the lattice  $(\alpha)=(1+\sqrt{10})$ , namely,  $O=0$ ,  $A=1+\sqrt{10}$ ,  $B=11+2\sqrt{10}$ ,  $C=10+\sqrt{10}$ , as shown in the figure. Observe that  $OA$  makes with the  $x$ -axis the angle

$$\varphi_A = \frac{1}{2} \log \frac{1+\sqrt{10}}{1-\sqrt{10}},$$

$OB$  makes with the  $x$ -axis,

$$\varphi_B = \frac{1}{2} \log \frac{11+2\sqrt{10}}{11-2\sqrt{10}},$$

$OC$  makes with the  $x$ -axis,

$$\varphi_C = \frac{1}{2} \log \frac{10+\sqrt{10}}{10-\sqrt{10}},$$

so that

$$\angle AOC = \frac{1}{2} \log (-1) = \angle aOc.$$

Similarly it is seen that

$$OAB = C_x + \pi - A_x = \pi - \frac{1}{2} \log(-1)$$

and

$$Oab = \pi - c_x = \pi - \frac{1}{2} \log(-1),$$

so that  $OAB = Oab$ , while  $ABC = abc$ , and  $BCO = bcO$ .

We further have the ratios

$$OA : OB = \sqrt{-9} : \sqrt{90} = \sqrt{-1} : \sqrt{10}$$

$$Oa : Ob = 1 : \sqrt{-10},$$

so that

$$OA : OB = Oa : Ob.$$

With this it is proved in the pseudometric sense that the figures  $OABC$  and  $Oabc$  are similar. (Sommer, *op. cit.*, p. 239.)

This result, somewhat extended, may be expressed as follows: *The lattice ( $\alpha$ ) is similar to the fundamental lattice and is derived therefrom through the turning about an angle*

$$\hat{\alpha} = \frac{1}{2} \log \frac{a+b\sqrt{m}}{a-b\sqrt{m}} \text{ and with a magnifying ratio } \bar{a} : 1.$$

Precisely as in the case of the imaginary realms, it may be shown that an indefinite number of lattices may be laid through the lattice-points of the ideal ( $\alpha$ ), and these lattices may be transformed into one another through linear transformations with determinant  $\pm 1$ .

ART. 294. To understand fully the significance of the structure of the set of points ( $\alpha$ ), it is necessary to consider the geometric meaning of the units of a real realm. We saw in Art. 99 that there were an indefinite number of such units. The images of these lie on the standard curve  $x^2 - my^2 = 1$ ; in fact, these are the points whose coördinates, integral in  $x$  and  $y$ , satisfy the equation just written. In particular that unit is to be considered whose radius vector makes the smallest angle with the  $x$ -axis.

Consider *first* a unit  $\epsilon$  whose norm  $N(\epsilon) = 1$ . The set of

points ( $\epsilon$ ) consists of *all* points of the fundamental lattice of the realm. For any definite unit  $\epsilon = a + b\sqrt{m}$ , the turning angle as shown above, is

$$\hat{\epsilon} = \frac{1}{2} \log \frac{a + b\sqrt{m}}{a - b\sqrt{m}} = \frac{1}{2} \log (a + b\sqrt{m})^2,$$

and since  $N(\epsilon) = +1$ , there is no magnifying. Similarly from the fundamental set of points of the realm, we may derive the set of points ( $\epsilon^k$ ),  $k$  any integer, by turning through an angle  $k \log (a + b\sqrt{m})$ , and also the set of points ( $-\epsilon^k$ ) is had through a turning through an angle  $k \log (a + b\sqrt{m}) + \pi i$ .

Since the set of points ( $\pm \epsilon^k$ ) is identical with the fundamental set of points of the realm, the existence of the indefinite number of units of the realm has the following geometric significance:

*The fundamental set of points of the real realm  $\mathfrak{R}(\sqrt{m})$  has the property of reverting into itself through a turning through an angle  $k\hat{\epsilon}$  or  $k\hat{\epsilon} + \pi i$ , where  $k$  is any rational integer. With this turning unit-points move along the hyperbolas  $x^2 - my^2 = \pm 1$ , while any arbitrary point of the fundamental set moves along the hyperbola  $x^2 - my^2 = C$ , where  $C$  has a definite value.*

Thus it is seen that the fundamental set of points of a real realm have certain symmetric properties analogous to those of regular polygons that are inscribed within a circle.

Next, let  $\epsilon$  be a unit with norm  $N(\epsilon) = -1$ . It is still true that the set of points ( $\epsilon$ ) is identical with the fundamental set of points and the first set is derived from the latter by an *improper* turning through the angle

$$\begin{aligned} \epsilon &= \frac{1}{2} \log \frac{a + b\sqrt{m}}{a - bm} = \log (a + b\sqrt{m}) - \frac{1}{2} \log (-1) \\ &= \log (a + b\sqrt{m}) - \frac{1}{2} i\pi; \end{aligned}$$



and that is, through a turning, together with a reflection through an asymptote by which a change in the radius-vectors in the ratio  $i : 1$  is brought about.

The set of points  $(-\epsilon)$  differs from the set  $(+\epsilon)$  only through a reflection through the origin.

The set of points  $(\epsilon^2)$  may be derived from the fundamental set by a *proper* turning.

Hence in the discussion of the unit-lattices, a distinction is to be made between the units  $\epsilon^{2k}$  and  $\epsilon^{2k+1}$ .

Geometrically formulated, the above results may be expressed as follows:

*If the real realm  $\Re(\sqrt{m})$  has a fundamental unit  $\epsilon$  with norm  $N(\epsilon) = -1$ , and if we put  $\epsilon = ie^{\frac{\pi}{2} + \hat{\epsilon}_1}$ , where  $\hat{\epsilon}_1$  is a real angle, then the fundamental set of units revert into themselves by a turning through an angle  $\hat{\epsilon}_1$ , and then a reflection through an asymptote of the standard curve.*

The geometric interpretation of the results of this article makes clear the distinction of the positive and negative norm of the fundamental unit of the real quadratic realm.

Treated analytically the knowledge of the units of the real realm is the knowledge of all linear transformations with integral coefficients (see Art. 293)

$$\begin{aligned} X &= ax + bmy, \\ Y &= bx + ay, \end{aligned}$$

through which the fundamental set of points are transformed into themselves. For it is clear that all transformations of this set have the determinant  $\pm 1$ .

#### EXAMPLES

(Excepting examples 1 and 2 the results are to be derived for real realms).

1. Determine the linear transformations with determinant 1 that transform into themselves the fundamental set of units of the

imaginary realm  $\Re(\sqrt{-3})$  and treat geometrically the ideals  $(\omega)$  and  $(\omega^2)$ , where  $\omega$  is a cube root of unity.

2. In the realm  $\Re(\sqrt{-1})$  the mesh of the fundamental lattice-points is a square. Show that these points revert into themselves with a turning through  $90^\circ$  and a reflection through the lines that bisect the angles included by the coördinate axes.

3. Give in detail a geometric treatment of the results given above for real realms where  $m \equiv 1 \pmod{4}$ .

4. To every ideal  $i$  of a real realm there corresponds a set of lattice-points through which an indefinite number of lattices may be laid. These lattices may be transformed into each other by means of linear transformations with determinant  $\pm 1$ .

5. Due to the fact that  $(\epsilon)(i) = i$ , show that every set of lattice-points may be transformed into themselves in an indefinite number of ways.

6. The meshes of a set of lattice-points of the ideal  $i$  contain those points of a fundamental set of lattice-points which  $(\text{mod. } i)$  form a complete set of incongruent integers of the real realm in question.

7. To equivalent ideals there correspond similar lattices which may be transformed into one another by linear transformations with determinant  $+1$ .

8. The lattices may be grouped into  $h$  classes. Each class contains at least one lattice the area of whose mesh is less than  $\frac{d}{2}$ .

*Remark.* Another method for the geometric representation of ideals of a quadratic realm was given by Poincaré, "Sur un mode nouveau de représentation géométrique des formes quadratiques définies ou indéfinies," *Journal de l'École Polytechnique*, Vol. 28 (1880), pp. 177 et seq. With him the lattice-points may be expressed through

$$\begin{aligned}x &= am + bn, \\y &= cm + dn,\end{aligned}$$

where  $m$  and  $n$  are indeterminates which may take all positive or negative integral values and  $a, b, c, d$  are constants; or through the notation

$$Am + Bn,$$

where  $A = a + c\sqrt{D}$ ,  $B = b + d\sqrt{D}$ , the quantity  $D$  being the determinant of the quadratic form.

Complex quantities of the form  $x + y\sqrt{D}$  are represented on a

plane  $P$  or through the projection of this plane on a plane  $Q$ . The planes  $P$  and  $Q$  cut along the  $x$ -axis, the angle between them being  $\cos^{-1} \sqrt{-D}$ . Observing that the modulus and argument of  $x+iy$  are  $\sqrt{x^2+y^2}$  and  $\tan^{-1} y/x$ , by analogy he (p. 200) calls the modulus and argument of  $x+y\sqrt{D}$  respectively  $\sqrt{x^2-y^2D}$  and  $\frac{1}{\sqrt{-D}} \tan^{-1} \frac{y}{x} \sqrt{-D}$ . When  $D$  is negative he introduces as a curve of reference the ellipse  $\zeta^2 - \eta^2 D = 1$ , and when  $D$  is positive the curve  $\zeta^2 - \eta^2 D = -1$  (hyperbola). Thus Poincaré was able (1880) to interpret geometrically all the results of the present chapter. The generalization of these results would lead to a geometric interpretation of ideals in the extended realms, the ellipse and hyperbola above being replaced by standard surfaces in a generalized space. See Minkowski's *Geometrie der Zahlen.*, pp. 9 and 73.

Bachmann, *Grundlehren der neueren Zahlentheorie*, p. 106, gives a geometric treatment of quadratic forms and their equivalence by means of lattice-points, the latter being the geometric images of the former, while the same lattice-points present the geometric image of two or more equivalent forms. On p. 129 is found the reduction of quadratic forms with negative discriminant geometrically interpreted through a method due to Gauss. On p. 219 a treatment of ideals and lattice-points is found and on p. 238 there is a geometric interpretation of the inner relation between "ideal (Kummer) numbers" and ideals of a fixed realm.

In the 45<sup>th</sup> volume of the *Mathematische Annalen* Hurwitz treats geometrically the reduction of quadratic forms for both positive and negative discriminants. His method may be extended to higher realms of rationality.

## CHAPTER XIV

### THE CUBIC<sup>1</sup> REALMS

ART. 295. In Arts. 87 and 101 a quantity  $\xi$  which satisfied an irreducible algebraic equation of the  $m$ th degree with rational coefficients was called an *algebraic number*; and if such a number  $\xi$  is added or adjoined to the realm of rational numbers, a *new realm of algebraic numbers* (Arts. 42 et seq.) is had through the operations of addition, subtraction, multiplication and division, and that is, a realm consisting of all integral and fractional functions of  $\xi$  with rational coefficients.

This realm has the following fundamental properties which may serve in their turn to define the realm:

1. *The sum or difference of any two numbers of the realm is a number of the realm.*

2. *The product or quotient of any two numbers of the realm is a number of the realm.*

Let  $\theta, \theta', \theta''$  be the roots of the irreducible equation of the third degree,

$$(1) \quad G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0,$$

whose coefficients are rational integers. Through definition (Art. 87)  $\theta, \theta', \theta''$  are *algebraic integers*. These three integers are different from one another and are *not* rational. The quantities  $\theta, \theta', \theta''$  are called *conjugate* (Art. 45) and when *adjoined* to the realm of rational numbers constitute the conjugate algebraic realms  $\mathfrak{R}(\theta), \mathfrak{R}(\theta'), \mathfrak{R}(\theta'')$ . Any number  $\nu$  of the realm  $\mathfrak{R}(\theta)$  may be

<sup>1</sup> *Report on Algebraic Numbers*, p. 12.

expressed in the form (see Art. 44)

$$\nu = a + b\theta + c\theta^2,$$

where  $a, b, c$  are definite rational numbers.

From equation (1) since  $-a_1 = \theta + \theta' + \theta''$ , or  $\theta' + \theta'' = -a_1 - \theta$ , it is seen that  $\theta' + \theta''$  is a number of the realm  $\Re(\theta)$  as is also  $\theta' \cdot \theta'' = -\frac{a_3}{\theta}$ .

**ART. 296. THEOREM.** *The sum, the difference, and the product of any two integers of  $\Re(\theta)$  is an integer of  $\Re(\theta)$ .*

This theorem has been proved for the general case in Arts. 88 and 162.

The following are simple proofs for the cubic realms.

Let  $\alpha$  and  $\beta$  be two algebraic integers of the realm  $\Re(\theta)$ , where  $\theta$  satisfies the irreducible equation

$$(1) \quad G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0,$$

$a_1, a_2, a_3$  being rational integers.

It follows from above that  $\alpha$  is of the form

$$\alpha = u + v\theta + w\theta^2, \quad (i)$$

where  $u, v, w$  are rational numbers.

If  $\theta$  is changed in this last expression to  $\theta'$  and  $\theta''$  respectively, we have the conjugate quantities  $\alpha'$  and  $\alpha''$ .

Similarly we may put

$$\beta = u_1 + v_1\theta + w_1\theta^2, \quad (ii)$$

where  $u_1, v_1, w_1$  are rational numbers.

It is further seen that  $\alpha$  satisfies the equation

$$(x - \alpha)(x - \alpha')(x - \alpha'') = 0,$$

or

$$x^3 + A_1x^2 + A_2x + A_3 = 0. \quad (iii)$$

In this expression  $A_1, A_2, A_3$  are rational integers, since by hypothesis  $\alpha$  is an algebraic integer.

In the same way  $\beta$  must satisfy an equation

$$x^3 + B_1x^2 + B_2x + B_3 = 0, \quad (iv)$$

where  $B_1, B_2, B_3$  are rational integers.



Forming the expression

$$S(t) = [t - (\alpha + \beta)][t - (\alpha' + \beta')][t - (\alpha'' + \beta'')],$$

it follows at once from (i) and (ii) that the sum  $\alpha + \beta$  satisfies an equation of the third degree with rational coefficients.

Since the coefficient of  $t^3$  in the expression just written is unity, it is only necessary to show that the other coefficients are rational integers. This may be done by forming the equation of the ninth degree:

$$\begin{aligned} T(t) = & [t - (\alpha + \beta)][t - (\alpha + \beta')][t - (\alpha + \beta'')] \\ & \times [t - (\alpha' + \beta)][t - (\alpha' + \beta')][t - (\alpha' + \beta'')] \\ & \times [t - (\alpha'' + \beta)][t - (\alpha'' + \beta')][t - (\alpha'' + \beta'')], \end{aligned}$$

an equation in which the coefficients are symmetric in both the  $\alpha$ 's and the  $\beta$ 's.

From (iii) and (iv) it is seen that these coefficients are rational integral functions of the  $A$ 's and the  $B$ 's.

It is evident that  $T(t)$  is divisible by  $S(t)$ , so that

$$T(t) = S(t)S_1(t).$$

From Art. 9 it follows that the coefficients of  $S(t)$  are rational integers.

In a similar manner it may be proved that the product  $\alpha \cdot \beta$  is an algebraic integer. Form the two quotients

$$\begin{aligned} \Phi(t) &= (t - \alpha\beta)(t - \alpha'\beta')(t - \alpha''\beta''), \\ Q(t) &= (t - \alpha\beta)(t - \alpha\beta')(t - \alpha\beta'')(t - \alpha'\beta)(t - \alpha'\beta') \\ &\quad \times (t - \alpha'\beta'')(t - \alpha''\beta)(t - \alpha''\beta')(t - \alpha''\beta''). \end{aligned}$$

It is clear that the coefficients of  $t$  in the latter expression are integral functions of the  $A$ 's and  $B$ 's; and since  $Q(t)$  is divisible by  $P(t)$ , it follows also that the coefficients of  $P(t)$  are rational integers and consequently  $\alpha\beta$  is an algebraic integer.

Through repetition of the above theorem it is seen that *every rational integral function in any number of algebraic*

integers of the realm  $\Re(\theta)$  with rational integral coefficients, is an integer of  $\Re(\theta)$ .

If  $\alpha$  is an algebraic integer, then also  $\alpha'\alpha''$  is an algebraic integer; and since  $\alpha'\alpha'' = \frac{N(\alpha)}{\alpha}$ , it is seen that  $\alpha' \cdot \alpha''$  is an algebraic integer in  $\Re(\theta)$ .

**THEOREM.** *If an algebraic integer  $\alpha$  in  $\Re(\theta)$  is a rational number, it must be a rational integer.*

For 1°, being an algebraic integer it satisfies an algebraic equation  $S(t) = 0$  in which the coefficient of the highest power is unity and the other coefficients are rational integers; and 2°, being a rational number, it follows from the theorem (Art. 10) since  $S(t)$  is divisible by  $t - \alpha$ , that  $\alpha$  must be a rational integer. (See also Art. 87.)

#### THE DISCRIMINANT OF AN INTEGER OF THE REALM

**ART. 297.** If  $\alpha$  is an arbitrary integer of  $\Re(\theta)$ , it was seen (Art. 44) that  $\alpha$  could be written in the form

$$\alpha = u + v\theta + w\theta^2,$$

where  $u, v$  and  $w$  are rational numbers. When  $\theta$  is changed to  $\theta'$  and  $\theta''$  respectively, there arise the quantities  $\alpha'$  and  $\alpha''$ , the *conjugates* of  $\alpha$ .

The product of the three quantities  $\alpha, \alpha', \alpha''$  is called the *norm* of  $\alpha$  and written  $N(\alpha) = \alpha \cdot \alpha' \cdot \alpha''$ . (Art. 59.)

The product

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'')$$

was called by Hilbert (*Bericht*, § 3) the *different* of the number  $\alpha$ .

The *discriminant* of  $\alpha$  is (see Arts. 63, 94, and 104)

$$\Delta(\alpha) = (\alpha - \alpha')^2(\alpha' - \alpha'')^2(\alpha'' - \alpha)^2 = \begin{vmatrix} 1, & \alpha, & \alpha^2 \\ 1, & \alpha', & \alpha'^2 \\ 1, & \alpha'', & \alpha''^2 \end{vmatrix}^2.$$

It is evident that  $N(\alpha)$  and  $\Delta(\alpha)$  are *rational* integers.

It is also seen that

$$\begin{aligned} -N[\delta(\alpha)] &= -(\alpha - \alpha')(\alpha - \alpha'')(\alpha' - \alpha'') \\ &\quad (\alpha' - \alpha)(\alpha'' - \alpha)(\alpha'' - \alpha') \\ &= (\alpha - \alpha')^2(\alpha' - \alpha'')^2(\alpha'' - \alpha)^2 = \Delta(\alpha) \quad (\text{Art. 95}). \end{aligned}$$

Since the equation

$$(1) \quad G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0,$$

which is satisfied by  $\theta$ , is by hypothesis irreducible, it cannot have a double root. (Art. 41.)

It follows that  $\Delta(\theta) \neq 0$ .

And (see Burnside and Panton, *Theory of Equations*, p. 83),

$$\Delta(\theta) = a_1^2a_2^2 + 18a_1a_2a_3 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2$$

(see Art. 104).

If  $a_1 = 0$ , this expression reduces to

$$\Delta(\theta) = -4a_2^3 - 27a_3^2.$$

The discriminant of a rational number is zero, since a rational number is its own conjugate; and reciprocally, if the discriminant of  $\alpha$  is zero, then is  $\alpha$  a rational number. For, if  $\alpha$  were an algebraic number, say

$$\begin{aligned} \alpha &= a + b\theta + c\theta^2 \quad \text{and} \\ \alpha' &= a + b\theta' + c\theta'^2, \end{aligned}$$

then is  $\alpha - \alpha' = b(\theta - \theta') + c(\theta^2 - \theta'^2)$ ;

and were  $\alpha = \alpha'$ , it would follow that  $0 = b + c(\theta + \theta')$  and consequently  $\theta'$  would be a rational number, contrary to the assumption that  $\theta$  satisfies an irreducible equation.

If  $\Delta(\theta)$  is a *positive* number, the roots of  $G(x) = 0$  are all real, and the three conjugate realms  $\Re(\theta)$ ,  $\Re(\theta')$ ,  $\Re(\theta'')$  contain only real quantities and are called *real* realms. If, however,  $\Delta(\theta)$  is negative, the roots of  $G(x) = 0$  are *one* real and *two* conjugate complex. One of the corresponding three realms is real and contains only real numbers, while the other two contain complex numbers and are called *imaginary* realms.

ART. 298. THEOREM I. *The discriminants of all algebraic numbers of  $\mathfrak{R}(\theta)$ , which are different from zero, have the same sign and that sign is the sign of  $\Delta(\theta)$ .*

For writing any number  $\alpha$  in the form

$$\begin{aligned}\alpha &= a_1 + b_1\theta + c_1\theta^2, \\ \alpha^2 &= a_2 + b_2\theta + c_2\theta^2,\end{aligned}$$

and substituting these values in the discriminant  $\Delta(\alpha)$ , it is evident that

$$\begin{aligned}\Delta(\alpha) &= \begin{vmatrix} 1, & \alpha, & \alpha^2 \\ 1, & \alpha', & \alpha'^2 \\ 1, & \alpha'', & \alpha''^2 \end{vmatrix}^2 \\ &= \begin{vmatrix} 1, & a_1 + b_1\theta + c_1\theta^2, & a_2 + b_2\theta + c_2\theta^2 \\ 1, & a_1 + b_1\theta' + c_1\theta'^2, & a_2 + b_2\theta' + c_2\theta'^2 \\ 1, & a_1 + b_1\theta'' + c_1\theta''^2, & a_2 + b_2\theta'' + c_2\theta''^2 \end{vmatrix}^2 \\ &= (b_1c_2 - b_2c_1)^2\Delta(\theta).\end{aligned}$$

THEOREM II. *The discriminant of every integer of  $\mathfrak{R}(\theta)$  which is not rational, is different from 0 and from  $\pm 1$ .*

If  $\alpha$  is an algebraic integer that is not rational, it satisfies an irreducible equation

$$x^3 + a_1x^2 + a_2x + a_3 = 0, \tag{i}$$

where  $a_1, a_2, a_3$  are rational integers.

In this equation  $a_1$  is either zero or different from zero. In the first case

$$\Delta(\alpha) = -4a_2^3 - 27a_3^2.$$

In the second case where  $a_1 \neq 0$ , write  $y = x + \frac{a_1}{3}$ .

The equation (i) becomes

$$y^3 + \frac{A_2}{3}y + \frac{A_3}{27} = 0,$$

where  $A_2$  and  $A_3$  are rational integers.

If  $a_1 \equiv 0 \pmod{3}$ , then is  $A_2$  divisible by 3 and  $A_3$  by 27 and here again the discriminant takes the form

$$\Delta(\alpha) = -4\bar{a}_2^3 - 27\bar{a}_3^2,$$

where  $\bar{a}_2, \bar{a}_3$  are rational integers.

If, however,  $a_1 \not\equiv 0 \pmod{3}$ , we have

$$\Delta(\alpha) = -\frac{1}{27}(4A_2^3 + A_3^2).$$

If, then,  $\Delta(\alpha) = -1$ , we must have an equation of one or the other forms

$$\begin{aligned} 4a_2^3 + 27a_3^2 &= 1, \\ 4A_2^3 + A_3^2 &= 27, \end{aligned}$$

where  $a_2, a_3; A_2, A_3$  are rational integers. It follows that either

$$27a_3^2 - 1 \equiv 0 \pmod{4},$$

or

$$A_3^2 - 27 \equiv 0 \pmod{4}.$$

Evidently neither of these congruences can be satisfied.

It may also be shown that  $\Delta(\alpha)$  is *not* equal to  $+1$ . For it was seen (Art. 269) in connection with the proof of the impossibility of solution of the Diophantine equation  $x^3 + y^3 = z^3$ , that the equation

$$(1) \quad y^3 - y \pm \frac{1}{3} = 0$$

is the only equation, the sum of whose roots is zero, for which  $\Delta(\alpha) = +1$ .

It is also seen that there is no substitution

$$y = x + \frac{a_1}{3},$$

which transforms (1) into an equation

$$x^3 + a_1x^2 + a_2x + a_3 = 0,$$

where  $a_1, a_2, a_3$  are rational integers.

**ART. 299. The Basis of All Integers of the Realm  $\mathfrak{K}(\theta)$ .**

In Art. 101 it was shown that three algebraic integers  $\omega_1, \omega_2, \omega_3$  of the realm  $\mathfrak{K}(\theta)$  might be derived in an infinite number of ways such that every arbitrary integer of the realm could be expressed in the form

$$x\omega_1 + y\omega_2 + z\omega_3,$$

where  $x, y, z$  are rational integers.



In Art. 102 a form for these three basal elements was

$$\omega_1 = 1, \quad \omega_2 = \frac{-(A - a_1) + \theta}{d},$$

$$\omega_3 = \frac{(A - a_1)^2 + a_1(A - a_1) + a_2 + A\theta + \theta^2}{d^2\delta_1},$$

where  $d, \delta_1$  are rational integers,  $d^6$  and  $\delta_1^2$  being divisors of  $\Delta(\theta)$ , and where the rational integer  $A$  was a root of the three congruences given in Art. 102, end.

**ART. 300. The Ideals of the Realm  $\mathfrak{R}(\theta)$ .** An algebraic integer  $\alpha$  is said to be divisible by another algebraic integer  $\beta$ , if there is a third algebraic integer  $\gamma$  of the realm  $\mathfrak{R}(\theta)$ , to which  $\alpha$  and  $\beta$  both belong, such that  $\alpha = \beta\gamma$ .

If we neglect the units (Art. 90) of the realm  $\mathfrak{R}(\theta)$ , it is seen by passing to the norms, since  $N(\alpha) = N(\beta)N(\gamma)$  (Arts. 59 and 89), that there are only a finite number of factors of  $\alpha$ . For  $N(\alpha)$  is a rational integer, and a rational integer admits only a finite number of divisors.

If, however, the factorization of the algebraic number  $\alpha$  is carried out until none of the factors admits further factoring, we meet with the same difficulty in the case of the cubic realms as was already had (Arts. 108, 203) in the case of the quadratic realms, namely, *the distribution of an algebraic integer  $\alpha$  of the realm  $\mathfrak{R}(\theta)$  into its irreducible factors of the same realm, is no longer unique; and that is, the factorization, as such, is no longer a unique process.*

To avoid this difficulty we must introduce the ideals of the cubic realms in a similar manner as has been done for the quadratic realms. Thus a realm is to be regarded as the collectivity of its rational numbers and its ideals. It is only necessary to extend the definitions given for ideals of quadratic realms (Arts. 206 et seq.) and to observe the properties of the ideals thus generalized.

These concepts will be further extended to the cases of the more extended realms in Vol. II, Chaps. 1, 2, and 3.

**DEFINITION.** An ideal  $i = (\alpha_1, \alpha_2, \alpha_3, \dots)$  is the totality or complex of the infinite number of algebraic integers of the realm  $\Re(\theta)$ , which has the property that every linear expression  $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \lambda_3\alpha_3 + \dots$  offers an algebraic integer that is found among this totality (complex); and that is, if  $\sigma = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \lambda_3\alpha_3 + \dots$ , then  $i = (\alpha_1, \alpha_2, \alpha_3, \dots) = (\alpha_1, \alpha_2, \alpha_3, \dots, \sigma, \dots)$ . The numbers  $\alpha_1, \alpha_2, \alpha_3, \dots$  are definite algebraic integers of  $\Re(\theta)$ , while  $\lambda_1, \lambda_2, \lambda_3, \dots$  are any algebraic integers of the same realm.

Note from this definition that every ideal contains the quantity zero.

It was seen in Art. 296 that if  $\alpha$  is an algebraic integer of  $\Re(\theta)$ , then  $\alpha'\alpha'' = \frac{N(\alpha)}{\alpha}$  is also an algebraic integer, say  $\lambda$ , of  $\Re(\theta)$ . Hence if  $\alpha$  is an element of an ideal, then is  $\lambda\alpha = N(\alpha)$  also an element of the same ideal. And as  $N(\alpha)$  is a rational integer, it is seen that every ideal contains an infinite number of rational integers. If, further, an ideal contains an algebraic integer  $\alpha$  which is a divisor of unity, so that, therefore,  $N(\alpha) = \pm 1$ , the ideal is called a *unit* ideal (Art. 211). In this case there is a system of integers  $\lambda_1, \lambda_2, \lambda_3, \dots$ , such that

$$1 = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots$$

If in an ideal  $i = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha, \dots)$  all the elements  $\alpha_1, \alpha_2, \alpha_3, \dots$  are divisible by  $\alpha$ , then is  $i = (\alpha)$ .

Such an ideal is called a *principal* ideal (Art. 206).

**ART. 301. THEOREM.** In every ideal  $i$  of the realm  $\Re(\theta)$  there may be derived in an infinite number of ways three integers  $\iota_1, \iota_2, \iota_3$ , such that every other integer of the ideal may be expressed in the form

$$x\iota_1 + y\iota_2 + z\iota_3,$$

where  $x, y, z$  are rational integers (Art. 94).

A *normal* basis of the ideal

$$\mathfrak{i} = (\alpha_1, \alpha_2, \alpha_3, \dots)$$

may be derived as follows: Let  $\omega_1 = 1$ ,  $\omega_2, \omega_3$  form a basis of all integers of the realm  $\mathfrak{K}(\theta)$  (Arts. 100 and 101). We may therefore write

$$\alpha_1 = a_1 + b_1\omega_2 + c_1\omega_3, \quad \alpha_2 = a_2 + b_2\omega_2 + c_2\omega_3,$$

etc.

If  $c$  is the greatest common divisor of  $c_1, c_2, c_3, \dots$ , we may always determine rational integers  $k_1, k_2, k_3, \dots$ , such that

$$k_1c_1 + k_2c_2 + k_3c_3 + \dots = c.$$

Further  $k_1\alpha_1 + k_2\alpha_2 + k_3\alpha_3 + \dots = \alpha$ , say, may be added as an element to the ideal  $\mathfrak{i}$  so that  $\mathfrak{i} = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha, \dots)$ .

If we put  $k_1a_1 + k_2a_2 + \dots = a$  and  $k_1b_1 + k_2b_2 + \dots = b$ , it is seen that

$$\alpha = a + b\omega_2 + c\omega_3.$$

Since  $c$  is a divisor of  $c_1, c_2, \dots$ , we may write  $c_1 = d_1c$ ,  $c_2 = d_2c$ ,  $c_3 = d_3c$ ,  $\dots$ , where  $d_1, d_2, d_3, \dots$  are rational integers.

It follows that  $\alpha_i - d_i\alpha = a_i - d_ia + (b_i - d_ib)\omega_2$  ( $i = 1, 2, 3, \dots$ ) are elements that may be added to  $\mathfrak{i}$ . Further write  $a_i - d_ia = A_i$  and  $b_i - d_ib = B_i$  and it is seen that  $\alpha_i = d_i\alpha + A_i + B_i\omega_2$  ( $i = 1, 2, 3, \dots$ ).

It follows that  $A_i + B_i\omega$  may be added as elements to  $\mathfrak{i}$ , and that the elements  $\alpha_i$  may be omitted.

The ideal takes the form

$$\mathfrak{i} = (A_1 + B_1\omega_2, A_2 + B_2\omega_2, A_3 + B_3\omega_2, \dots, \alpha, \dots).$$

Continuing as in Art. 206, it is seen that  $\mathfrak{i}$  may be reduced to the form

$$\mathfrak{i} = (i, i_1 + i_1^{(1)}\omega_2, \alpha),$$

where  $i$  is a rational integer that is the greatest common divisor of all rational integers that belong to  $\mathfrak{i}$ . The

numbers  $i_1$  and  $i_1^{(1)}$  are also rational integers,  $i_1^{(1)}$  being (Art. 206) a divisor of both  $i$  and  $i_1$ .

Writing for  $\alpha$  its value  $a + b\omega_2 + c\omega_3$  and noting that  $i\omega_3$  may be added as an element to  $i$ , it follows as above that  $\alpha$  may be replaced by an element  $\iota_3 = i_2 + i_2^{(1)}\omega_2 + i_2^{(2)}\omega_3$  where  $i_2^{(2)}$  is a divisor of  $i$ , where  $i_2^{(1)}$  is reduced (mod.  $i_1^{(1)}$ ), and  $i_2$  is reduced (mod.  $i$ ).

The normal basis of the ideal  $i$  is thus shown to be

$$i = (\iota_1, \iota_2, \iota_3),$$

where

$$\iota_1 = i, \quad \iota_2 = i_1 + i_1^{(1)}\omega_2, \quad \iota_3 = i_2 + i_2^{(1)}\omega_2 + i_2^{(2)}\omega_3.$$

If we put

$$\iota_r^* = a_{r1}\iota_1 + a_{r2}\iota_2 + a_{r3}\iota_3 \quad (r=1, 2, 3)$$

and choose (Art. 100) the rational integers  $a_{rs}$  ( $s=1, 2, 3$ ) such that  $|a_{rs}| = \pm 1$ , it is evident (Art. 94) that  $\iota_1^*, \iota_2^*, \iota_3^*$  also form a basis of all integers of  $i$ .

ART. 302. Whenever the question of *division* arises in the realms of rationality such as  $\mathfrak{R}(\theta)$ , the ideals take the place of the algebraic integers of the realm. Multiplication and division of algebraic integers are to be replaced by multiplication and division of ideals for such realms, the operations of addition and subtraction of algebraic integers being retained as such.

*Multiplication of Ideals.* Let  $\mathfrak{a} = (\alpha_1, \alpha_2, \dots, \alpha, \dots)$ ,  $\mathfrak{b} = (\beta_1, \beta_2, \dots, \beta, \dots)$  be two ideals of  $\mathfrak{R}(\theta)$ . Here  $\alpha$  is supposed to be any integer of  $\mathfrak{a}$ , say

$$\alpha = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots,$$

and similarly

$$\beta = \mu_1\alpha_1 + \mu_2\alpha_2 + \dots,$$

where  $\lambda_1, \lambda_2, \dots, \mu_1, \mu_2, \dots$  are any algebraic integers of  $\mathfrak{R}(\theta)$ . The product  $\mathfrak{a} \cdot \mathfrak{b}$  is an ideal, say  $\mathfrak{c}$ , whose elements

consist of the products as follows:

$$\begin{aligned}
 c = a \cdot b = & \alpha_1\beta_1, \alpha_1\beta_2, \alpha_1\beta_3, \dots, \alpha_1\beta, \dots, \\
 & \alpha_2\beta_1, \alpha_2\beta_2, \alpha_2\beta_3, \dots, \alpha_2\beta, \dots, \\
 & \alpha_3\beta_1, \alpha_3\beta_2, \alpha_3\beta_3, \dots, \alpha_3\beta, \dots, \\
 & \dots\dots\dots \\
 & \alpha\beta_1, \alpha\beta_2, \alpha\beta_3, \dots, \alpha\beta, \dots, \\
 & \dots.
 \end{aligned}$$

It is clear that the ideal  $c$  is constituted of algebraic number of the form

$$\begin{aligned}
 & \nu_{11}\alpha_1\beta_1 + \nu_{12}\alpha_1\beta_2 + \nu_{13}\alpha_1\beta_3 + \dots + \nu_{10}\alpha_1\beta + \dots \\
 & \quad + \nu_{21}\alpha_2\beta_1 + \nu_{22}\alpha_2\beta_2 + \nu_{23}\alpha_2\beta_3 + \dots + \nu_{20}\alpha_2\beta + \dots \\
 & \quad + \nu_{31}\alpha_3\beta_1 + \nu_{32}\alpha_3\beta_2 + \nu_{33}\alpha_3\beta_3 + \dots + \nu_{30}\alpha_3\beta + \dots \\
 & \quad + \dots \\
 & \quad + \nu_{01}\alpha\beta_1 + \nu_{02}\alpha\beta_2 + \nu_{03}\alpha\beta_3 + \dots + \nu_{00}\alpha\beta + \dots \\
 & \quad + \dots,
 \end{aligned}$$

where the  $\nu$ 's are any algebraic (including rational) integers of  $\mathfrak{R}(\theta)$ .

Reciprocally, an ideal  $c$  is said to be divisible by the ideal  $a$  when there is an integral ideal  $b$  such that  $c = a \cdot b$ , the three ideals, of course, belonging to the same realm  $\mathfrak{R}(\theta)$ .

Since  $\nu_{11}\beta_1, \nu_{12}\beta_2$ , etc. are algebraic integers of  $\mathfrak{R}(\theta)$  it is evident that if the ideal  $c$  is divisible by the ideal  $a$ , then every number of the ideal  $c$  (and consequently of the form just written) is also a number of the ideal  $a$  and that is every number that is divisible by  $c$  is also divisible by  $a$ .

An ideal that is not a unit in  $\mathfrak{R}(\theta)$  and which is divisible only by itself and such a unit is called a *prime* ideal.

ART. 303. Two ideals  $a$  and  $b$  of  $\mathfrak{R}(\theta)$  are said to be *equivalent* (Art. 217) when there are two integers  $\alpha$  and  $\beta$  of  $\mathfrak{R}(\theta)$  such that

$$\frac{a}{b} = \frac{\alpha}{\beta}.$$



The same properties of equivalent ideals obtain here, as are given in Arts. 217 et seq. All equivalent ideals form a class.

It may be proved next that the factorization of ideals is unique. An indirect proof of this theorem due to Hurwitz is given here.<sup>1</sup>

LEMMA I. *An integer  $\alpha$  of the realm  $\mathfrak{R}(\theta)$  whose norm  $N(\alpha) = \pm a$  is finite, can enter as an element in only a finite number of different ideals.*

For let

$$\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha, a, \dots)$$

and let  $1, \omega_2, \omega_3$  be a basis of all integers of  $\mathfrak{R}(\theta)$  and let  $\iota_1 = i, \iota_2 = i_1 + i_1^{(1)}\omega_2, \iota_3 = i_2 + i_2^{(1)}\omega_2 + i_2^{(2)}\omega_3$  be a normal basis of the ideal  $\mathfrak{a}$ . Since  $a, a\omega_2, a\omega_3$  may be added as elements of  $\mathfrak{a}$ , it follows from the derivation of the normal basis that  $i$  is a divisor of  $a$ , while  $i_1^{(1)}$  and  $i_2^{(2)}$  are divisors of  $i$ . There are only a finite number of ways of distributing the rational integer  $a$  into divisors. Further  $i_2^{(1)}$  is reduced mod.  $i_1^{(1)}$  and consequently is an integer  $< i_1^{(1)}$ ; while  $i_1$  and  $i_2$  are reduced (mod.  $i$ ).

It follows that *an ideal can have only a finite number of different ideals as divisors*. For as seen in the preceding article, every integer that appears in the dividend must also enter the divisor.

LEMMA II. *There are only a finite number of different ideal-classes of the realm  $\mathfrak{R}(\theta)$ . It is proved below that this lemma follows, when we prove that every arbitrary ideal of the realm is equivalent to at least one ideal, which depends only upon the discriminant of the realm.*

In the proof of this lemma a distinction must be made between the real and the imaginary realms.

In the case of the *real* realms, let  $\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3)$ , where

<sup>1</sup> See Hurwitz, *Nachr. von der Kgl. Ges. d. Wissensch. zu Gött.*, 1895, p. 323.

the three basal elements (Art. 93) may be written

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + a_{i3}\omega_3 \quad (i=1, 2, 3).$$

Form the norms of all the numbers of  $\alpha$ . Among all these norms there is one whose absolute value is as small as the norm of any other number of the ideal. Let  $\iota$  be this number. It is asserted that a finite rational integer  $A$  may be derived which depends only upon the discriminant  $D = D(\omega_1, \omega_2, \omega_3)$  of the realm, and is such that  $A\alpha$  is divisible by  $\iota$ , where  $\alpha$  is an arbitrary number of the ideal. (See also Sommer, *Vorlesungen*, p. 266.)

For let  $\alpha_i$  be any one of the three basal elements of the ideal in question. Then due to the Minkowski Theorem (Art. 26) four rational integers  $u, x, y, z$  which are *not* all zero, may be found such that

$$(1) \quad \alpha_i u + \omega_1 x + \omega_2 y + \omega_3 z \leq k_1,$$

$$(2) \quad \alpha'_i u + \iota' \omega'_1 x + \iota' \omega'_2 y + \iota' \omega'_3 z \leq k_2,$$

$$(3) \quad \alpha''_i u + \iota'' \omega''_1 x + \iota'' \omega''_2 y + \iota'' \omega''_3 z \leq k_3,$$

$$(4) \quad \left| \frac{\pm \alpha_i u}{\sqrt{D}} \right| \leq k_4,$$

where  $k_1, k_2, k_3, k_4$  are four positive quantities whose determinant is equal to the determinant of the four forms just written, and that is

$$k_1 k_2 k_3 k_4 = \frac{\pm \alpha_i}{\sqrt{D}} N(\iota) \begin{vmatrix} \omega_1 & \omega_2 & \omega_3 \\ \omega'_1 & \omega'_2 & \omega'_3 \\ \omega''_1 & \omega''_2 & \omega''_3 \end{vmatrix} = \pm \alpha_i N(\iota).$$

Since one of the  $k$ 's may be arbitrarily chosen, write  $k_4 = 2|\alpha_i|$ , so that from (4)  $u \leq |2\sqrt{D}|$ . It follows that

$$k_1 k_2 k_3 \leq \frac{1}{2} N(\iota).$$

Next put

$$\beta = \alpha_i u + \iota(\omega_1 x + \omega_2 y + \omega_3 z).$$

Hence from (1), (2), and (3)

$$|N(\beta)| \leq k_1 k_2 k_3,$$

or

$$|N(\beta)| \leq \frac{1}{2} |N(\iota)|.$$

Note that  $\beta = \alpha_i u + \iota(\omega_1 x + \omega_2 y + \omega_3 z)$  is a number of the ideal  $\mathfrak{a}$ , since  $u$  and  $\omega_1 x + \omega_2 y + \omega_3 z = \lambda$ , say, are integers of  $\Re(\theta)$ , while  $\alpha_i$  and  $\iota$  are elements of the ideal. Further,  $\lambda$  cannot be zero; for in that case there would be a linear relation among the basal elements of the realm. And  $u$  cannot be zero; for in that case it would follow from (1), (2), and (3) that

$$|N(\iota) \cdot N(\omega_1 x + \omega_2 y + \omega_3 z)| \leq \frac{1}{2} |N(\iota)|,$$

or

$$|N(\omega_1 x + \omega_2 y + \omega_3 z)| \leq \frac{1}{2},$$

which is not true, since the norm of an algebraic integer in absolute value is  $\geq 1$ .

Since

$$|N(\beta)| \leq \frac{1}{2} |N(\iota)|,$$

and since by hypothesis no number of  $\Re(\theta)$ , other than zero, has a norm which is less than  $|N(\iota)|$ , it is seen that  $\beta = 0$ . It follows that

$$\alpha_i u + \lambda \iota = 0;$$

or, expressed in words: *For each of the basal elements  $\alpha_i$  of the ideal  $\mathfrak{a}$ , there may be determined a rational integer  $|u| < |2\sqrt{D}|$  such that  $\alpha_i u$  is divisible by  $\iota$ .*

Of course, this integer  $u$  is not necessarily the same for the three basal elements  $\alpha_1, \alpha_2, \alpha_3$ .

Denote by  $A$  the product of all positive integers that are less than  $|2\sqrt{D}|$ . Then clearly the product of each of the numbers  $\alpha_1, \alpha_2, \alpha_3$  by  $A$  is divisible by  $\iota$ , or  $A\alpha_i = \iota\delta_i$ , where  $\delta_i$  is an algebraic integer of  $\Re(\theta)$ . It follows, since every number  $\alpha$  of the ideal  $\mathfrak{a}$ , is of the form  $\alpha_1\lambda_1 + \alpha_2\lambda_2 + \alpha_3\lambda_3$ , that  $A\alpha$  is divisible by  $\iota$ .

Note that

$$\begin{aligned} A\mathfrak{a} &= A(\alpha_1, \alpha_2, \alpha_3, \dots, \iota, \dots) = (A\alpha_1, A\alpha_2, \dots, A\iota, \dots) \\ &= \iota(\delta_1, \delta_2, \delta_3, \dots, A) = \iota\mathfrak{b}, \end{aligned}$$

say.

It follows that every ideal  $\mathfrak{a}$  is equivalent to an ideal  $\mathfrak{b}$  which contains the rational integer  $A$ . As there are (see Lemma I) only a finite number of different ideals in which  $A$  may enter as an element, it follows that there are only a finite number of different classes to which a real ideal  $\mathfrak{a}$  may belong. Ideals  $\mathfrak{b}_1, \mathfrak{b}_2, \dots, \mathfrak{b}_h$  may be determined such that each is a representative of a definite class.

Next suppose that  $\mathfrak{R}(\theta)$  is an *imaginary* realm and let  $\alpha, \alpha_i, \alpha, \iota$  have the same significance as above,  $\alpha_i$  and  $\alpha$  being complex quantities. Determine an integer  $\beta$  of  $\mathfrak{a}$ , say  $\beta = \alpha_i u + \iota(\omega_1 x + \omega_2 y + \omega_3 z)$ , such that  $|N(\beta)| < |N(\iota)|$ . We may again apply the Minkowski Theorem to the four linear forms:

$$\frac{1}{\sqrt{2}}(\beta + \beta'), \quad \frac{1}{\sqrt{-2}}(\beta - \beta'), \quad \beta'', \quad \frac{\pm |\alpha_i| u}{|\sqrt{D}|},$$

( $\beta$  and  $\beta'$  being conjugate imaginaries,  $\beta''$  real) and

$$\begin{aligned} \beta &= \alpha_i u + \iota(\omega_1 x + \omega_2 y + \omega_3 z), \\ \beta' &= \alpha'_i u + \iota'(\omega'_1 x + \omega'_2 y + \omega'_3 z). \end{aligned}$$

Note that  $\alpha_i$  and  $\alpha'_i$  are conjugate imaginaries, as are also  $\omega_1, \iota'\omega'_1$ , etc.

As in the case of the real realms above, rational integers  $u, x, y, z$  that are not all zero, may be determined such that

$$(1) \quad \left| \frac{1}{\sqrt{2}}(\beta + \beta') \right| \leq k_1,$$

$$(2) \quad \left| \frac{1}{i\sqrt{2}}(\beta - \beta') \right| \leq k_1,$$

$$(3) \quad |\beta''| \leq k_3,$$

$$(4) \quad \left| \frac{\alpha_i u}{\sqrt{D}} \right| \leq k_4,$$

where  $k_1^2 \cdot k_3 \cdot k_4$  is equal to the determinant of the left hand side of (1), (2), (3), and (4), which is  $|\alpha_i N(\iota)|$ .

Write  $k_4 = 2|\alpha_i|$ , so that

$$k_1^2 k_3 = \frac{1}{2} |N(\iota)|.$$

Observe from (4) that

$$|u| \leq 2|\sqrt{D}|.$$

Further, note that

$$\begin{aligned} |N(\beta)| = |\beta \cdot \beta' \cdot \beta''| &\equiv \left| \left\{ \frac{1}{2}(\beta + \beta')^2 + \left( \frac{1}{2i}(\beta - \beta') \right)^2 \right\} \beta'' \right| \\ &\equiv \left\{ \left( \frac{k_1}{\sqrt{2}} \right)^2 + \left( \frac{k_1}{\sqrt{2}} \right)^2 \right\} k_3 \end{aligned}$$

or

$$|N(\beta)| \leq \frac{1}{2} |N(\iota)|.$$

The proof from now on is the same as in the case of the real realms. And thus it has been proved that *the number of classes into which the ideals of every realm  $\mathfrak{R}(\theta)$  may be distributed, is finite. This number is denoted by  $h$ .*

ART. 304. The following theorem may now be proved.

THEOREM. *If  $\mathfrak{a}$  is an arbitrary ideal of the realm  $\mathfrak{R}(\theta)$ , which is not a principal ideal, another ideal  $\mathfrak{b}$ , which is also not a principal ideal, may be determined, such that the product  $\mathfrak{a} \cdot \mathfrak{b}$  is a principal ideal.*

Let  $\mathfrak{a}$  be an ideal that is not a principal ideal, and form the powers of  $\mathfrak{a}$ , the ideals  $\mathfrak{a}, \mathfrak{a}^2, \mathfrak{a}^3, \dots$ .

Due to the second lemma, these ideals may be distributed into a finite number of classes; and, as the most general case, it may be assumed that  $\mathfrak{a}^{m+h_1}$  is the first power of  $\mathfrak{a}$  that falls into a class that has been occupied by a preceding  $\mathfrak{a}$ , say the same class to which  $\mathfrak{a}^m$  belongs, so that

$$\mathfrak{a}^{m+h_1} \sim \mathfrak{a}^m,$$

or

$$\alpha \mathfrak{a}^{m+h_1} = \beta \mathfrak{a}^m,$$



or finally

$$\alpha^{m+h_1} = \lambda \alpha^m, \quad (i)$$

where  $\alpha, \beta$  are integers of  $\mathfrak{R}(\theta)$ .

It remains to show that  $\alpha^{h_1}$  is equal to a principal ideal  $(\lambda)$ .

It must be shown first that  $\lambda$  as defined through equation (i) is an integer of the realm. Observe that every number of the ideal  $\alpha^{m+h_1}$  is also a number of the ideal  $\alpha^m$ , since every integer of the first ideal is also one of the latter. If  $\alpha_1, \alpha_2, \alpha_3$  constitute a basis of the ideal  $\alpha^m$ , then  $\lambda \alpha_1$  is an integer, since it is a number of the ideal  $\alpha^{m+h_1}$ , and as every number of this latter ideal is also a number of the ideal  $\alpha^m$ , it is seen that

$$\lambda \alpha_1 = x_1 \alpha_1 + y_1 \alpha_2 + z_1 \alpha_3;$$

and similarly

$$\lambda \alpha_2 = x_2 \alpha_1 + y_2 \alpha_2 + z_2 \alpha_3,$$

$$\lambda \alpha_3 = x_3 \alpha_1 + y_3 \alpha_2 + y_3 \alpha_3,$$

where the  $x$ 's,  $y$ 's, and  $z$ 's are rational integers. Through elimination of  $\alpha_1, \alpha_2, \alpha_3$  from these equations, it is seen that  $\lambda$  satisfies the equation

$$\begin{vmatrix} x_1 - \lambda & y_1 & z_1 \\ x_2 & y_2 - \lambda & z_2 \\ x_3 & y_3 & z_3 - \lambda \end{vmatrix} = 0.$$

Hence  $\lambda$  (see Art. 87) is an algebraic integer.

If, further,  $\beta$  is any number of the ideal  $\alpha^{h_1}$ , then are  $\beta \alpha_1, \beta \alpha_2, \beta \alpha_3$  numbers divisible by the product of ideals  $(\lambda) \alpha^m$ , and it follows also as in the case of  $\lambda$  above, that  $\frac{\beta}{\lambda}$  is an algebraic integer. Hence every number of  $\alpha^{h_1}$  is divisible by  $\lambda$  and consequently the ideal  $\alpha^{h_1}$  is divisible by  $\lambda$ .

It follows that  $\alpha^{h_1} = (\lambda)i$ , where  $i$  is an ideal. We may therefore write

$$\alpha^{m+h_1} = \alpha^m \alpha^{h_1} = \alpha^m (\lambda) i$$

and from equation (ii) namely  $a^{m+h_1} = \lambda a^m$ , it is seen that

$$a^m(\lambda)i = \lambda a^m.$$

Since  $\lambda$  may be divided out of this equation, we have finally

$$a^m i = a^m. \quad (\text{ii})$$

It may be proved that  $i$  is a unit-ideal (Art. 206). For let  $\iota_1, \iota_2, \iota_3$  be a normal-basis of  $i$ ; and if  $\alpha_1, \alpha_2, \alpha_3$  are a basis of  $a$ , it is evident that every number of the ideal  $a^m$  on the righthand side of (ii) may be written in the form

$$\lambda_1 \alpha_1 (x_1 \iota_1 + y_1 \iota_2 + z_1 \iota_3) + \lambda_2 \alpha_2 (x_2 \iota_1 + y_2 \iota_2 + z_2 \iota_3) \\ + \lambda_3 \alpha_3 (x_3 \iota_1 + y_3 \iota_2 + z_3 \iota_3),$$

where  $\lambda_1, \lambda_2, \lambda_3$  are arbitrary integers of  $\mathfrak{R}(\theta)$  and  $x_i, y_i, z_i (i=1, 2, 3)$  are rational integers.

On the other hand all numbers of  $a^m$  may be expressed in the form  $u_1 \alpha_1 + u_2 \alpha_2 + u_3 \alpha_3$ , where  $u_1, u_2, u_3$  are any rational integers. Equating this last expression for  $a^m$  to the preceding one, it is seen that

$$u_i = \lambda_i (x_i \iota_1 + y_i \iota_2 + z_i \iota_3) \quad (i=1, 2, 3).$$

If for  $u_1, u_2, u_3$  we choose three rational integers that are relatively prime, it is seen that the integers

$$u_i = \lambda_i (x_i \iota_1 + y_i \iota_2 + z_i \iota_3) \quad (i=1, 2, 3),$$

may be added as elements to the ideal (i). As this ideal contains also the greatest common divisor of these three rational integers, it is seen that the ideal  $i$  is a unit-ideal. It was proved above that  $a^{h_1} = (\lambda)i$ , and as  $i$  is a unit ideal, it follows that  $a^{h_1} = (\lambda)$  is a principal ideal, or  $a^{h_1} \sim 1$ .

Hence also

$$a^{h_1+1} = a \cdot a^{h_1} \sim a, \\ a^{h_1+2} \sim a^2,$$

etc.

In other words, in the original assumption, we may take  $m=1$ ; and by hypothesis the ideals  $a, a^2, \dots, a^{h_1-1}$  must be necessarily *in-equivalent*.

If then  $\mathfrak{a}$  is an arbitrary ideal of the realm  $\mathfrak{R}(\theta)$ , which is not a principal ideal, it is always possible to determine another ideal  $\mathfrak{a}^{h-1} = \mathfrak{b}$ , say, which is also not a principal ideal and it is such that  $\mathfrak{a} \cdot \mathfrak{b}$  is a principal ideal.

ART. 305. The following consequences result from the theorem of the preceding article.

THEOREM. *If  $\mathfrak{a}$ ,  $\mathfrak{b}$ ,  $\mathfrak{c}$  are three ideals that are different from zero, and which satisfy the equation  $\mathfrak{ac} = \mathfrak{bc}$ , then is  $\mathfrak{a} = \mathfrak{b}$ .*

For if  $\mathfrak{b}$  is an ideal such that  $\mathfrak{cb} = (\lambda)$ , where  $(\lambda)$  is a principal ideal, we may multiply both sides of the equation  $\mathfrak{ac} = \mathfrak{bc}$  by  $\mathfrak{b}$ , and then divide by the algebraic integer  $\lambda$ .

FUNDAMENTAL THEOREM. *If all the numbers of the ideal  $\mathfrak{b}$  also belong to the ideal  $\mathfrak{a}$ , then is  $\mathfrak{b}$  divisible by  $\mathfrak{a}$ . And that is, if  $\mathfrak{b} > \mathfrak{a}$ , then is  $\mathfrak{b} = \mathfrak{af}$ , where  $\mathfrak{f}$  is an ideal.*

If  $\mathfrak{b} \equiv 0 \pmod{\mathfrak{a}}$ , then is  $\mathfrak{bm} \equiv 0 \pmod{\mathfrak{am}}$ , where  $m$  is any ideal.

Let  $m$  be an ideal such that  $\mathfrak{am} = (\alpha)$ . It follows that  $\mathfrak{bm} \equiv 0 \pmod{(\alpha)}$  or  $\mathfrak{bm} = \mathfrak{af}$ ,  $\mathfrak{f}$  an ideal. Hence  $\mathfrak{abm} = \mathfrak{aaf}$  or  $\mathfrak{ab} = \mathfrak{af}$  or  $\mathfrak{b} = \mathfrak{af}$ .

THEOREM. *If the product  $\mathfrak{ab}$  of two ideals is divisible by the prime ideal  $\mathfrak{p}$ , and if  $\mathfrak{a}$  is not divisible by  $\mathfrak{p}$ , then is  $\mathfrak{b}$  divisible by  $\mathfrak{p}$ . In other words, if the prime ideal  $\mathfrak{p}$  is a factor of the product  $\mathfrak{ab}$ , then  $\mathfrak{p}$  must be a divisor of at least one of the factors  $\mathfrak{a}$  or  $\mathfrak{b}$ .*

If  $\mathfrak{ab} = \mathfrak{pc}$ , and if  $\mathfrak{am} = (\alpha)$ , then is  $(\alpha)\mathfrak{b} = \mathfrak{pcm}$ ; and since  $\alpha$  and  $\mathfrak{p}$  can have no factor in common, it follows that  $\mathfrak{b}$  is divisible by  $\mathfrak{p}$ . This may be proved differently as follows. If  $\mathfrak{a}$  is not divisible by  $\mathfrak{p}$ , then is  $(\mathfrak{a} + \mathfrak{p} = \mathfrak{o})$  and that is, two integers  $\alpha_1$  and  $\bar{\omega}$  may be found such that  $\alpha_1 + \bar{\omega} = 1$ , since 1 is an integer in  $\mathfrak{o}$ .

And if  $\beta$  is any integer of  $\mathfrak{b}$ , then is  $\alpha_1\beta$  divisible by  $\mathfrak{p}$ ;

and since  $\alpha_1\beta + \bar{\omega}\beta = \beta$ , it follows that  $\beta \equiv 0 \pmod{\mathfrak{p}}$ , and that is,  $\mathfrak{b}$  is divisible by  $\mathfrak{p}$ .

It follows from the above theorem that *every ideal may be distributed into its prime ideal-factors in only one way, or the factorization of an ideal into prime ideal factors is a unique process.*

A fundamental consequence of the theorem by which the unique factorization of ideals is established, is the fact that every prime ideal of the realm  $\mathfrak{R}(\theta)$  must be a divisor of a rational prime integer; and that is, a rational prime integer must appear as an element in every prime ideal. For corresponding to every prime ideal  $\mathfrak{p}$  there exists an ideal  $\mathfrak{i}$  such that  $\mathfrak{p}\mathfrak{i} = (\alpha)$ , a principal ideal. Since  $\alpha\alpha'\alpha'' = N(\alpha) = a$ , say, is a rational integer, and as  $\frac{(\alpha)}{\mathfrak{p}} = \mathfrak{i}$ , it is seen that  $(\alpha)$  is divisible by  $(\mathfrak{p})$  and consequently  $\alpha$  is an element of  $\mathfrak{p}$ . It follows also that  $a$  is an element <sup>1</sup> of  $\mathfrak{p}$ . Since  $a$  is divisible by  $\mathfrak{p}$ , one of the prime factors of  $a$  is also divisible by  $\mathfrak{p}$ , and being divisible by  $\mathfrak{p}$ , appears as an element of  $\mathfrak{p}$ .

The following theorem is of peculiar importance for the numerical calculation of ideals which belong to a fixed realm. (See also Art. 215.)

**THEOREM.** *In every ideal  $\mathfrak{a}$ , which is not a principal ideal, there always may be found two numbers  $\alpha$  and  $\alpha_1$ , whose greatest common divisor is  $\mathfrak{a}$ , so that  $\mathfrak{a}$  may be written equal to  $(\alpha, \alpha_1)$ .*

For let  $\alpha$  be any number of  $\mathfrak{a}$ . Then choose an ideal  $\mathfrak{b}$ , such that  $\frac{(\alpha)}{\mathfrak{a}} = \mathfrak{b}$ , where  $\mathfrak{b}$  is relatively prime to  $\mathfrak{a}$ . Next choose a number, say  $\alpha_1$  of  $\mathfrak{a}$ , which is relatively prime to

<sup>1</sup> For  $\alpha'\alpha'' = \frac{a}{\alpha}$  is an integer of the realm to which  $\alpha$  belongs. It follows that if  $\alpha$  is divisible by  $\mathfrak{p}$ , then also  $\alpha'\alpha''$  is divisible by  $\mathfrak{p}$  and accordingly is an element of  $\mathfrak{p}$ .

$b$ , and let  $\frac{(\alpha_1)}{a} = i$ , so that  $(\alpha_1) = ai$ . It is evident that  $i$  is relatively prime to  $b$ , and it may be shown that  $a$  is the greatest common divisor of  $(\alpha)$  and  $(\alpha_1)$ , or  $a = (\alpha, \alpha_1)$ . Since  $b$  and  $i$  are relatively prime, observe that we may determine an integer  $\beta$  of  $b$  and an integer  $\gamma$  of  $i$  (see above) such that  $\beta + \gamma = 1$ . Hence, if  $\alpha_i$  is any integer of  $a$ , it follows that

$$\alpha_i = \alpha_i\beta + \alpha_i\gamma = \lambda\alpha + \lambda_1\alpha_1, \quad \text{or} \quad a = (\alpha, \alpha_1).$$

**ART. 306. The Norm of an Ideal.** An integer  $\alpha$  of the realm  $\mathfrak{R}(\theta)$  is said to be *congruent to an ideal  $i$  as modulus*, and written  $\alpha \equiv 0 \pmod{i}$ , if  $\alpha$  is divisible by  $i$ , and that is, if  $\alpha$  is an element of  $i$ . Two numbers  $\alpha$  and  $\beta$  of  $\mathfrak{R}(\theta)$  are said to be *congruent to each other* and written  $\alpha \equiv \beta \pmod{i}$ , if the difference  $\alpha - \beta$  is divisible by  $i$ . (Art. 209.)

It follows that, if  $\alpha$  and  $\beta$  are both congruent  $\pmod{i}$  to a third number  $\gamma$ , they are congruent to each other.

The totality (or collectivity, and that is, the complex of all the integers of  $\mathfrak{R}(\theta)$ ) may be distributed  $\pmod{i}$  into classes, if all numbers are counted as belonging to the same class, when they are congruent  $\pmod{i}$  to a definite number, and that is, every number of a class is congruent  $\pmod{i}$  to every other number of the class. Every number of  $\mathfrak{R}(\theta)$  belongs to a definite class, and every number of a class determines  $\pmod{i}$  that class.

The number of such classes as seen below is finite. If from each of this finite number of classes a definite number is selected, a system of integers is constituted which may be called a *complete system of incongruent residues*  $\pmod{i}$ . Every number of the realm  $\mathfrak{R}(\theta)$  is congruent to a definite one of the numbers of the complete system. The number of the integers which constitute a complete system is called the *norm* of the ideal  $i$  and is written  $N(i)$ . (Art. 209.)



**THEOREM.** Let  $\alpha$  be an ideal of the realm  $\Re(\theta)$  and let the basis of  $\alpha$  be the quantities  $\alpha_1, \alpha_2, \alpha_3$ , where

$$\left. \begin{aligned} \alpha_1 &= a_{11}\omega_1 + a_{12}\omega_2 + a_{13}\omega_3, \\ \alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2 + a_{23}\omega_3, \\ \alpha_3 &= a_{31}\omega_1 + a_{32}\omega_2 + a_{33}\omega_3, \end{aligned} \right\} \quad (a)$$

the  $a$ 's being rational integers. Then is

$$N(\alpha) = |(a_{11}, a_{22}, a_{33})|.$$

*Proof.* First take the normal basis  $\iota_1, \iota_2, \iota_3$  (Art. 301) of the ideal  $\alpha$ , where

$$\iota_1 = 1, \quad \iota_2 = i_1 + i_1^{(1)}\omega_2, \quad \iota_3 = i_2 + i_2^{(1)}\omega_2 + i_2^{(2)}\omega_3. \quad (b)$$

Every integer  $\beta$  of  $\Re(\theta)$  may be written

$$\beta = u + u_1\omega_2 + u_2\omega_3,$$

where  $u, u_1, u_2$  are rational integers. When considered with regard to the ideal  $\alpha$ , by making use of the normal basis it is seen that  $u$  may be reduced (mod.  $i$ ),  $u_1$  may be reduced (mod.  $i_1^{(1)}$ ) and  $u_2$  may be reduced mod.  $i_2^{(2)}$ . It follows that there are  $i \cdot i_1^{(1)} \cdot i_2^{(2)}$  numbers like  $\beta$  of  $\Re(\theta)$  that are different (mod.  $\alpha$ ).

Hence, since  $(\alpha_1, \alpha_2, \alpha_3) = (\iota_1, \iota_2, \iota_3)$ , it is clear (Art. 94) that if

$$\left. \begin{aligned} \alpha_1 &= A_{11}\iota_1 + A_{12}\iota_2 + A_{13}\iota_3, \\ \alpha_2 &= A_{21}\iota_1 + A_{22}\iota_2 + A_{23}\iota_3, \\ \alpha_3 &= A_{31}\iota_1 + A_{32}\iota_2 + A_{33}\iota_3, \end{aligned} \right\} \quad (c)$$

then

$$\left| \begin{array}{ccc} A_{11}, & A_{21}, & A_{31} \\ A_{12}, & A_{22}, & A_{32} \\ A_{13}, & A_{23}, & A_{33} \end{array} \right| = \pm 1;$$

and further in (c) substitute the values of  $\iota_1, \iota_2, \iota_3$  from

(b) and compare the result with (a), and we have

$$\begin{vmatrix} a_{11}, & a_{12}, & a_{13} \\ a_{21}, & a_{22}, & a_{23} \\ a_{31}, & a_{32}, & a_{33} \end{vmatrix} = \begin{vmatrix} A_{11}, & A_{12}, & A_{13} \\ A_{21}, & A_{22}, & A_{23} \\ A_{31}, & A_{32}, & A_{33} \end{vmatrix} \begin{vmatrix} i, & 0, & 0 \\ i_1, & i_1^{(1)}, & 0 \\ i_2, & i_2^{(1)}, & i_2^{(2)} \end{vmatrix} = \pm i \cdot i_1^{(1)} \cdot i_2^{(2)}.$$

It follows that the absolute value of the left-hand determinant is  $i \cdot i_1^{(1)} \cdot i_2^{(2)}$  as stated in the theorem.

Since  $i$  is a number that appears as an element of the ideal  $\mathfrak{a}$ , it is evident that  $N(\mathfrak{a}) = i \cdot i_1^{(1)} \cdot i_2^{(2)}$  is an element of the ideal  $\mathfrak{a}$ .

**ART. 307.** *The norm of the product of two ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  is equal to the product of the norms of these ideals, and that is,  $N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$ .*

*Proof.* Let  $\alpha$  be an integer of the realm  $\Re(\theta)$  which is divisible by  $\mathfrak{a}$  and is such that  $\frac{(\alpha)}{\mathfrak{a}}$  is prime to  $\mathfrak{b}$  (cf. Art. 215).

The form  $\alpha\eta + \xi$  presents only incongruent (mod.  $\mathfrak{a}\mathfrak{b}$ ) integers of the realm, when to  $\eta$  there are ascribed a complete system of incongruent numbers (mod.  $\mathfrak{a}$ ) and to  $\xi$  likewise a complete system of incongruent residues (mod.  $\mathfrak{b}$ ). There are in all  $N(\mathfrak{a}) \cdot N(\mathfrak{b})$  such numbers, and no two numbers of this system are congruent to each other, mod.  $\mathfrak{a}\mathfrak{b}$ , while every integer of  $\Re(\theta)$  is congruent, mod.  $\mathfrak{a} \cdot \mathfrak{b}$ , to a number of this system.

It follows that  $N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$ .

The norm of an ideal as shown above is a rational integer that may be adjoined as an element of the ideal, and that is  $N(\mathfrak{a})$  is divisible by the ideal  $\mathfrak{a}$ .

We may therefore write  $\frac{N(\mathfrak{a})}{\mathfrak{a}} = \bar{\mathfrak{a}}$ , where  $\bar{\mathfrak{a}}$  is an ideal

which may be called the reciprocal of the ideal  $\alpha$ . And for two ideals it is seen that  $N(\alpha \cdot \beta) = \alpha \bar{\alpha} \beta \bar{\beta}$ .

ART. 308. The theorem for the determination of the norm of an ideal may be applied to the special case of a prime ideal; say

$$\mathfrak{p} = (p, i_1 + i_1^{(1)}\omega_1, i_2 + i_2^{(1)}\omega_1 + i_2^{(2)}\omega_2).$$

Since (Art. 206)  $i_1^{(1)}$  and  $i_2^{(2)}$  are divisors of  $p$ , these ideals are of the form

$$\begin{aligned} &(p, i_1 + 1\omega_1, i_2 + i_2^{(1)}\omega_1 + 1\omega_2), \\ &(p, i_1 + p\omega_1, i_2 + i_2^{(1)}\omega_1 + 1\omega_2), \\ &(p, i_1 + 1\omega_1, i_2 + i_2^{(1)}\omega_1 + p\omega_2), \\ &(p, i_1 + p\omega_1, i_2 + i_2^{(1)}\omega_1 + p\omega_2). \end{aligned}$$

Corresponding to these four possibilities it is seen (Art. 306) that  $N(\mathfrak{p}) = p^e$ , where  $e = 1, 2$ , or  $3$ . This number  $e$  is called the *degree* of the prime ideal  $\mathfrak{p}$ .

We thus have prime ideals of the first, second, and third degrees. (See Art. 211.)

After the introduction of the norm of an ideal and the calculation of its numerical value through the coefficients of the basis, we are in a position to present the theorems which are necessary for the calculation of the ideal-classes of a realm.

ART. 309. **Theorems of Minkowski for the Presentation of the Ideal-Classes.** For the presentation of the ideal classes of the quadratic realms we had (Art. 218) the theorem that each of the different classes contained at least one ideal whose norm was less or at least equal to  $|\sqrt{D}|$ , where  $D$  was the discriminant of the realm.

To prove the same theorem for the cubic realms we must prove first the following lemma.

LEMMA. *Every arbitrary ideal  $\alpha$  of the realm  $\mathfrak{R}(\theta)$  contains a number  $\alpha$ , whose norm satisfies the inequality  $|N(\alpha)| \leq N(\alpha) |\sqrt{D}|$ .*

First let  $\mathfrak{R}(\theta)$  be a *real* realm and let  $\alpha_1, \alpha_2, \alpha_3$  be a basis of the ideal  $\mathfrak{a}$  which may be written in the form (Art. 94)

$$\alpha_\nu = a_{\nu 1}\omega_1 + a_{\nu 2}\omega_2 + a_{\nu 3}\omega_3 \quad (\nu=1, 2, 3),$$

where  $\omega_1, \omega_2, \omega_3$  constitute a basis of all integers of the realm  $\mathfrak{R}(\theta)$ .

Due to the Minkowski Theorem (Art. 26) three rational integers  $x, y, z$  that are not all zero may be found such that the absolute values of the three linear forms

$$\begin{aligned} f_1 &= \alpha_1 x + \alpha_2 y + \alpha_3 z, \\ f_2 &= \alpha'_1 x + \alpha'_2 y + \alpha'_3 z, \\ f_3 &= \alpha''_1 x + \alpha''_2 y + \alpha''_3 z, \end{aligned}$$

are less than the three positive quantities  $k_1, k_2, k_3$  whose product  $k_1 k_2 k_3$  is equal to the absolute value of the determinant of the three linear forms  $|(\alpha_1, \alpha'_2, \alpha''_3)|$  which in turn  $= |(a_{11}, a_{22}, a_{33})| \cdot |\sqrt{D}|$ .

Write  $f_1 = \alpha$ , so that  $f_2 = \alpha'$ , and  $f_3 = \alpha''$ .

It follows that  $N(\alpha) \leq k_1 k_2 k_3$  or  $|N(\alpha)| \leq (N(\mathfrak{a})) |\sqrt{D}|$ .

Suppose *next* that  $\mathfrak{R}(\theta)$  is an *imaginary* realm, and that  $\mathfrak{R}(\theta')$  is the conjugate imaginary realm, while  $\mathfrak{R}(\theta'')$  is the conjugate real realm.

Instead of the two forms  $f_1$  and  $f_2$  above consider the two real forms

$$F_1 = \frac{1}{\sqrt{2}} \{ (\alpha_1 + \alpha'_1)x + (\alpha_2 + \alpha'_2)y + (\alpha_3 + \alpha'_3)z \}$$

and

$$F_2 = \frac{1}{\sqrt{-2}} \{ (\alpha_1 - \alpha'_1)x + (\alpha_2 - \alpha'_2)y + (\alpha_3 - \alpha'_3)z \}$$

and of the quantities above let  $k_1 = k_2$ .

Noting the identity  $F_1^2 + F_2^2 \equiv (F_1 + iF_2)(F_1 - iF_2)$  it is seen that

$$\frac{F_1^2 + F_2^2}{2} = (\alpha_1 x + \alpha_2 y + \alpha_3 z)(\alpha'_1 x + \alpha'_2 y + \alpha'_3 z).$$

Again writing  $\alpha = \alpha_1x + \alpha_2y + \alpha_3z$ ,  $\alpha' = \alpha'_1x + \alpha'_2y + \alpha'_3z$ , we have as above

$$\alpha\alpha' = \frac{F_1^2 + F_2^2}{2} < k_1^2, \quad \alpha'' < k_2,$$

or

$$|N(\alpha)| < k_1^2 k_3,$$

while

$$k_1^2 k_3 = N(\alpha) |\sqrt{D}|.$$

We are now in a position to prove the theorem:

**THEOREM.** *Every ideal-class of the realm  $\mathfrak{R}(\theta)$  contains an ideal whose norm is smaller than the absolute value of the square root of the discriminant of the realm.*

*Proof.* Let  $\alpha$  be an ideal of the realm  $\mathfrak{R}(\theta)$  and let  $\bar{\alpha}$  be a second ideal such that  $\alpha\bar{\alpha}$  is a principal ideal, say  $(\alpha)$  (Art. 304). From the above lemma there is in the ideal  $\bar{\alpha}$  an integer  $\bar{\alpha}$  such that  $|N(\bar{\alpha})| \leq N(\bar{\alpha}) |\sqrt{D}|$ . Since  $\bar{\alpha}$  is divisible by  $\bar{\alpha}$ , we may write  $(\bar{\alpha}) = \bar{\alpha}\alpha_1$ , where  $\alpha_1$  is an ideal of  $\mathfrak{R}(\theta)$ .

Hence  $N(\alpha\alpha_1) = |N(\bar{\alpha})| \bar{\alpha} N(\alpha) |\sqrt{D}|$  or  $N(\alpha_1) \bar{\alpha} \leq |\sqrt{D}|$  (see also Art. 218).

Since  $(\alpha) = \alpha\bar{\alpha}$  and  $(\bar{\alpha}) = \bar{\alpha}\alpha_1$ , it is seen that  $\frac{\alpha}{\bar{\alpha}} = \frac{\alpha}{\alpha_1}$  or  $\alpha \sim \alpha_1$ ; and it has thus been proved that the ideal-class to which  $\alpha$  belongs, contains an ideal  $\alpha_1$  such that  $N(\alpha_1) \leq |\sqrt{D}|$ . The same is true of every ideal-class.

Hence to obtain directly the number of ideal-classes of a fixed realm  $\mathfrak{R}(\theta)$ , it is only necessary to consider the positive rational integers that are less than or at most equal to  $|\sqrt{D}|$ .

These rational integers are to be decomposed into their ideal-factors. Those ideal factors that are equivalent and whose norms are at the same time  $\leq |\sqrt{D}|$  constitute a class in question, and the number of such classes is thus determined.



ART. 310. **Derivation of the Prime Ideals in the Realm  $\mathfrak{R}(\theta)$ .** Suppose that the realm  $\mathfrak{R}(\theta)$  is fixed, the quantity  $\theta$  being a root of the irreducible equation

$$G(x) = x^3 + a_1x^2 + a_2x + a_3,$$

where  $a_1, a_2, a_3$  are rational integers.

It is required to construct the prime ideals  $\mathfrak{p}, \mathfrak{p}_1$ , etc., through which a rational prime integer  $p$  is divisible.

It is assumed at first that the prime integer  $p$  is not a divisor of the discriminant  $\Delta(\theta)$ ; and that is,  $\Delta(\theta) \not\equiv 0 \pmod{p}$ .

In Art. 305 it was proved that any ideal could be expressed as the greatest common divisor of two integers of the realm  $\mathfrak{R}(\theta)$ . It follows that  $\mathfrak{p}$  may be expressed in the form  $(p, \alpha)$  where  $\alpha$  is an integer of  $\mathfrak{R}(\theta)$ .

It was proved in Art. 102 that a basis of all integers of  $\mathfrak{R}(\theta)$  could be expressed in the form

$$\omega_1 = 1, \quad \omega_2 = \frac{-A + a_1 + \theta}{d}, \quad \omega_3 = \frac{A^2 - a_1A + a_2 + A\theta + \theta^2}{d^2\delta_1}$$

where  $d$  and  $\delta_1$  are definite divisors of  $\Delta(\theta)$ . Hence, every integer  $\alpha$  of  $\mathfrak{R}(\theta)$  may be written

$$\alpha = \frac{a + b\theta + c\theta^2}{d^2\delta_1},$$

where  $a, b$ , and  $c$  are rational integers.

If now  $\mathfrak{p}$  is the greatest common divisor of  $p$  and  $\alpha$ , it is also the greatest common divisor of  $p$  and  $d^2\delta_1\alpha$ , since  $d^2\delta_1$  is relatively prime to  $p$  and therefore also to  $\mathfrak{p}$ . And  $\mathfrak{p}$ , being the greatest common divisor of  $p$  and  $d^2\delta_1\alpha$ , is  $\mathfrak{p} = (p, d^2\delta_1\alpha)$ . Hence there remains the two possibilities either  $d^2\delta_1\alpha$  is of the first or of the second degree in  $\theta$ .

It follows that either

$$(1) \quad \mathfrak{p} = (p, a + b\theta),$$

or

$$(2) \quad \mathfrak{p} = (p, a + b\theta + c\theta^2),$$

and it remains to determine in either case the rational integers  $a, b, c$ .

Since the number  $x\theta \cdot p + y(a + b\theta)$  may be added as an element in the first case, and since  $p$  and  $b$  are relatively prime, the rational integers  $x$  and  $y$  may be so chosen that  $xp + yb = 1$ , and consequently an element of the form  $-A + \theta$  may be added to the ideal (1), which now becomes

$$\mathfrak{p} = (p, a + b\theta, -A + \theta).$$

Since  $a + b\theta - b(-A + \theta) = a + bA$ , it is seen that  $a + bA$  may be added as an element of  $\mathfrak{p}$ . It is clear, also, that  $a + bA$  must be divisible by  $p$ ; otherwise the ideal reduces to a unit ideal. Write  $a + bA = g \cdot p$ , where  $g$  is a rational integer. Further note that

$$gp + b(-A + \theta) = a + b\theta.$$

Hence  $a + b\theta$  may be omitted as an element, thus leaving

$$\mathfrak{p} = (p, -A + \theta).$$

It remains to determine  $A$ .

In this ideal it is evident that the element  $-A + \theta$  may be multiplied by  $(-A + \theta')(-A + \theta'')$ , which product is  $-A^3 - a_1A^2 - a_2A - a_3$  or  $-G(A)$ . And this number must be divisible by  $p$ , otherwise the ideal becomes a unit ideal. It follows that  $A$  must satisfy the congruence

$$G(x) \equiv 0 \pmod{p}.$$

If this congruence does not permit solution, then  $p$  has no ideal factor  $\mathfrak{p}$  of the form (1).

In the second case, namely when

$$\mathfrak{p} = (p, a + b\theta + c\theta^2),$$

we may, as in the first case, replace the second element by an element in which  $c = 1$ . The prime ideal then takes the form

$$\mathfrak{p} = (p, a + b\theta + \theta^2),$$

and if in this ideal such elements of the form  $a_1 + b_1\theta$  enter, the coefficients  $a_1$  and  $b_1$  must be divisible by  $p$ ; otherwise,  $\mathfrak{p}$  would reduce to the first case.

If the element  $a+b\theta+\theta^2$  is multiplied by the integer  $z+\theta$ , where  $z$  is a rational integer to be determined, and if we note that  $\theta^3+a_1\theta^2+a_2\theta+a_3=0$ , it is seen that the ideal may be written

$$\begin{aligned} \mathfrak{p} &= (p, a+b\theta+\theta^2, az+(a+bz)\theta \\ &\quad + (b+z)\theta^2+\theta^3, a_3+a_2\theta+a_1\theta^2+\theta^3, \dots) \\ &= (p, a+b\theta+\theta^2, az-a_3 \\ &\quad + (a+bz-a_2)\theta+(b+z-a_1)\theta^2, \dots). \end{aligned}$$

If  $z$  is determined so as to satisfy the congruence  $b+z-a_1 \equiv 0 \pmod{p}$ , then the ideal takes the form

$$\mathfrak{p} = (p, a+b\theta+\theta^2, az-a_3+(a+bz-a_2)\theta, \dots).$$

We therefore must have the congruences

$$\begin{aligned} a+bz-a_2 &\equiv 0 \pmod{p}, \\ az-a_3 &\equiv 0 \pmod{p}. \end{aligned}$$

If these two congruences are satisfied, it is seen that

$$(a+b\theta+\theta^2)(z+\theta) \equiv a_3+a_2\theta+a_1\theta^2+\theta^3 \pmod{p}.$$

Thus the quantities  $a$ ,  $b$ , and  $a+b\theta+\theta^2$  are determined, if  $a_3+a_2\theta+a_1\theta^2+\theta^3$  may be factored  $\pmod{p}$  into a linear and a quadratic factor.

Hence, to determine the prime-ideal factor of a rational prime integer  $p$  in a cubic realm  $\Re(\theta)$ , where  $\theta$  is a root of the equation

$$G(x) = x^3 + a_1x^2 + a_2x + a_3 = 0,$$

we have to determine the roots of the congruence

$$G(x) \equiv 0 \pmod{p}. \tag{i}$$

It has been shown that:

1. if  $A$  is a solution of (i), then is

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x-A)f_1(x) \pmod{p},$$

where  $f_1(x)$  is a rational integral function of the second degree in  $x$ ;

2. the congruence (i) has at most three distinct solutions.

I. If the congruence (i) has no solution, then in the realm  $\mathfrak{R}(\theta)$ ,  $p$  is not factorable into ideal-factors, and  $(p)$  is a prime ideal of the third degree, and that is  $N(p) = p^3$ .

II. If (i) admits the only solution  $x = A$ , so that:

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A)(x^2 + bx + a) \pmod{p},$$

then  $p$  admits the two prime-ideal factors

$$\mathfrak{p}_1 = (p, -A + \theta) \quad \text{and} \quad \mathfrak{p}_2 = (p, a + b\theta + \theta^2),$$

such that  $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ , where  $\mathfrak{p}_1$  is of the first degree and  $\mathfrak{p}_2$  of the second.

III. If the congruence (i) admits the three solutions  $A_1, A_2, A_3$ , so that

$$x^3 + a_1x^2 + a_2x + a_3 \equiv (x - A_1)(x - A_2)(x - A_3) \pmod{p},$$

then is  $p$  divisible by the three prime-ideal factors of the first degree

$$\mathfrak{p}_i = (p, -A_i + \theta) \quad (i = 1, 2, 3),$$

so that  $p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$ , where each ideal is of the first degree, and that is  $N(\mathfrak{p}_i) = p$  ( $i = 1, 2, 3$ ). (Sommer, *Vorlesungen*, p. 277; Reid, *Göttingen Dissertation* (1899), p. 25.)

ART. 311. If next we consider the case where  $p$  is a divisor of  $\Delta(\theta)$ , we encounter difficulties in deriving the prime-ideal factors of  $p$ .

If  $\Delta(\theta) \equiv 0 \pmod{p}$ , the congruence

$$G(x) = x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$$

has a multiple root, say  $x = A_1$ ; and either

$$G(x) \equiv (x - A_1)^2(x - A_2) \pmod{p},$$

or

$$G(x) \equiv (x - A_1)^3 \pmod{p}.$$

For if  $G'(x) = 3x^2 + 2a_1x + a_2$  is the derivative of the function  $G(x)$ , then a necessary and sufficient condition for a common solution of the two congruences  $G(x) \equiv 0 \pmod{p}$  and  $G'(x) \equiv 0 \pmod{p}$  is  $\Delta(\theta) \equiv 0 \pmod{p}$ , as is seen at once by eliminating  $x$  from the two congruences.

If, however,  $A$  is the common solution of the two

congruences  $G(x) \equiv 0 \pmod{p}$  and  $G'(x) \equiv 0 \pmod{p}$ ; and if we write

$$G(x) \equiv (x-A)f_1(x) \pmod{p},$$

then is

$$G'(x) \equiv f_1(x) + (x-A)f_1'(x) \pmod{p}.$$

From this latter formula it is seen that  $G'(x) \equiv 0 \pmod{p}$  can have the root  $x \equiv A \pmod{p}$ , when  $f_1(x) \equiv (x-A)f_2(x) \pmod{p}$ ; and that is, when  $G(x) \equiv (x-A)^2f_2(x) \pmod{p}$ .

If  $\Delta(\theta) \equiv 0 \pmod{p}$ , it might be surmised that the rational integer  $p$  was divisible by the square of a prime ideal. This is *not* always the case. The following theorem was proved by Dedekind<sup>1</sup> and later by Hensel.<sup>2</sup>

**THEOREM.** *All and only those rational prime integers which are divisors of the discriminant  $D$  of the realm are divisible by the square of a prime ideal.*

This theorem was proved for the quadratic realms in Art. 216. In this connection see the theorems for the general realms of rationality in Vol. II, Chapter VI.

### THE UNITS OF THE REALM $\mathfrak{R}(\theta)$

**ART. 312.** Among the integers of the realm  $\mathfrak{R}(\theta)$  those are of peculiar interest, whose norms are equal to  $\pm 1$ , and which are called *units* of the realm (Art. 90). If  $\epsilon$  is such an integer, then is  $\epsilon\epsilon'\epsilon'' = \pm 1$ , and that is,  $\epsilon$  satisfies an equation of the form

$$x^3 + a_1x^2 + a_2x \pm 1 = 0.$$

That  $\frac{1}{\epsilon}$  is also a unit, is seen by writing  $\frac{1}{y}$  for  $x$  in the equation just written.

<sup>1</sup> R. Dedekind, "Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen." *Abhandl. der math. Klasse der Kgl. Gesellschaft der Wissensch. zu Göttingen*, 23 Band, 1878.

<sup>2</sup> Hensel, *Crelle*, Vol. 113, 1894; Vols. 127, 128, 129; see also Hensel, *Jahresber. der deutschen math. Ver.*, Vol. 6 and *Gött. Nach.*, 1897; and Hilbert, *Zahlber.*, p. 195.



It is also evident that if  $\epsilon$  is a unit that is different from  $\pm 1$ , then every power  $\pm \epsilon^e$  with integral positive and negative exponents  $e$  are units; for clearly

$$\epsilon^e \cdot \epsilon'^e \epsilon''^e = (\epsilon \epsilon' \epsilon'')^e = \pm 1.$$

If the realms  $\Re(\theta)$ ,  $\Re(\theta')$ ,  $\Re(\theta'')$  are all real, the roots of the equations  $t^2 = \pm 1$ ,  $t^3 = \pm 1$ , when imaginary are *not* units of the three realms, since these realms do not contain complex integers.

If, further,  $\Re(\theta)$  is real and  $\Re(\theta')$  and  $\Re(\theta'')$  are conjugate imaginary realms, then in none of the three realms can there appear the roots of unity, other than  $\pm 1$ .

Suppose for example that

$$\eta' = \frac{a\theta'^2 + b\theta' + c}{k}$$

is a complex root of unity in the realm  $\Re(\theta')$ .

Then is  $\eta' \cdot \eta'' = \pm 1$ , so that  $\eta = \pm 1$ .

It follows that

$$\eta = \frac{a\theta^2 + b\theta + c}{k} = \pm 1,$$

or,  $\theta$  satisfies an equation  $a\theta^2 + b\theta + c \pm k = 0$ , of the 2nd degree which is *not* true since the cubic which  $\theta$  satisfies is irreducible (Art. 41).

In the same way it follows that every unit  $\epsilon$  of the realm  $\Re(\theta)$ , for which  $|\epsilon| = 1$ , is itself  $= \pm 1$ . For if  $\Re(\theta)$  is a *real* realm and if  $|\epsilon| = 1$ , then  $\epsilon$  being a real quantity is  $= \pm 1$ . If next  $\Re(\theta')$  is a complex realm in which  $|\epsilon'| = +1$ , then in the conjugate complex realm  $\Re(\theta'')$  it is evident that  $|\epsilon''| = 1$ , where  $\epsilon''$  is the conjugate complex of  $\epsilon'$ . It is further seen that  $|\epsilon| = +1$  in the real realm  $\Re(\theta)$ , and consequently  $\epsilon = \pm 1$ , as must be also  $\epsilon'$  and  $\epsilon''$ .

ART. 313. The following is a theorem<sup>1</sup> which in generalized form was proved by P. G. Lejeune Dirichlet, *Werke*, Vol. I, pp. 622, 632, 642.

LEMMA. *In every (real or imaginary) realm  $\Re(\theta)$  of the third degree there exists a unit which is different from  $\pm 1$ .*

The proof of this theorem is very similar to that given for the real quadratic realm of Arts. 230 et seq. See also Arts. 99 et seq.

I. First let the discriminant  $D$  of the realm be *positive* so that all the realms  $\Re(\theta)$ ,  $\Re(\theta')$ ,  $\Re(\theta'')$  are real. Let  $A_1$ ,  $A_2$ ,  $A_3$  be any three positive quantities, whose product is

$$A_1 A_2 A_3 = |\sqrt{D}|. \quad (i)$$

It is possible, due to the Minkowski Theorem of Art. 26, to determine rational integers  $u$ ,  $x$ ,  $y$ ,  $z$  which are not all zero, such that

$$\begin{aligned} |\alpha_1 u + \alpha \omega_1 x + \alpha \omega_2 y + \alpha \omega_3 z| &\leq A_1, \\ |\alpha'_1 u + \alpha' \omega'_1 x + \alpha' \omega'_2 y + \alpha' \omega'_3 z| &\leq A_2, \\ |\alpha''_1 u + \alpha'' \omega''_1 x + \alpha'' \omega''_2 y + \alpha'' \omega''_3 z| &\leq A_3, \\ \left| \frac{\alpha_1 u}{k} \right| + 0 + 0 + 0 &\leq A_4. \end{aligned}$$

The quantities  $A_1$ ,  $A_2$ ,  $A_3$ ,  $A_4$  satisfy the relation

$$A_1 A_2 A_3 A_4 = \left| \frac{\alpha_1 N(\alpha) \sqrt{D}}{k} \right|,$$

where  $\alpha_1$ ,  $\alpha$  are integers in  $\Re(\theta)$  and where  $\omega_1$ ,  $\omega_2$ ,  $\omega_3$  form the basis of all integers of  $\Re(\theta)$ .

Further put  $A_4 = \left| \frac{\alpha_1 N(\alpha)}{k} \right|$ , and write

$$\alpha = \alpha_1 u + \alpha \omega_1 x + \alpha \omega_2 y + \alpha \omega_3 z.$$

It follows that

$$A_1 A_2 A_3 = |\sqrt{D}|. \quad (i)$$

It is seen that  $\alpha$  is an integer of  $\Re(\theta)$  such that  $|\alpha| \leq A_1$ ,  $|\alpha'| \leq A_2$ ,  $|\alpha''| \leq A_3$ .

<sup>1</sup> See also H. Minkowski, *Geom. d. Zahlen*, pp. 137 et seq.; D. Hilbert, *Bericht*, Chapt. 6, pp. 214 et seq.

Since  $\alpha$  is an integer in  $\Re(\theta)$ , its norm, that is

$$|\alpha \cdot \alpha' \cdot \alpha''| \geq 1,$$

and consequently

$$|\alpha| \geq \frac{1}{|\alpha' \alpha''|}$$

and therefore also

$$\geq \frac{1}{A_2 A_3} \geq \frac{A_1}{A_1 A_2 A_3}.$$

Thus for  $\alpha$  and its conjugates  $\alpha'$  and  $\alpha''$ , there exist the inequalities

$$\left. \begin{aligned} A_1 &\geq |\alpha| \geq \frac{A_1}{|\sqrt{D}|} \\ A_2 &\geq |\alpha'| \geq \frac{A_2}{|\sqrt{D}|} \\ A_3 &\geq |\alpha''| \geq \frac{A_3}{|\sqrt{D}|} \end{aligned} \right\}. \quad (\text{ii})$$

Due to equation (i), the last inequality may be written

$$\frac{|\sqrt{D}|}{A_1 A_2} \geq |\alpha''| \geq \frac{1}{A_1 A_2}.$$

Consider next three new real positive quantities

$$B_1 = \frac{A_1}{|\sqrt{D}|}, \quad B_2 = \frac{A_2}{|\sqrt{D}|}, \quad B_3 = \frac{A_3 |\sqrt{D}|^3}{|\sqrt{D}|},$$

whose product, due to (i), is again  $= |\sqrt{D}|$ .

From similar considerations there exists an integer  $\beta$  of  $\Re(\theta)$  which satisfies the inequalities

$$\left. \begin{aligned} B_1 &\geq |\beta| \geq \frac{B_1}{|\sqrt{D}|} \\ B_2 &\geq |\beta'| \geq \frac{B_2}{|\sqrt{D}|} \\ B_3 &\geq |\beta''| \geq \frac{B_3}{|\sqrt{D}|} \end{aligned} \right\}. \quad (\text{iii})$$

Instead of the last inequality we may again write

$$\frac{|\sqrt{D}|}{B_1 B_2} \cong |\beta''| \cong \frac{1}{B_1 B_2}.$$

Further write

$$C_1 = \frac{B_1}{|\sqrt{D}|}, \quad C_2 = \frac{B_2}{|\sqrt{D}|}, \quad C_3 = \frac{B_3 |\sqrt{D}|^3}{|\sqrt{D}|},$$

and determine an algebraic integer  $\gamma$  in the same way as  $\alpha$  and  $\beta$  were determined above.

If this process is continued, there exists an unbroken series of algebraic integers which satisfy inequalities such as (ii) and (iii).

Since the discriminant  $|\sqrt{D}| > 1$ , it is evident from (ii) and (iii), that the numbers  $|\alpha|$ ,  $|\beta|$ ,  $|\gamma|$ ,  $\dots$ ; as well as the numbers  $|\alpha'|$ ,  $|\beta'|$ ,  $|\gamma'|$ ,  $\dots$  form a series of decreasing numbers, while the series  $|\alpha''|$ ,  $|\beta''|$ ,  $|\gamma''|$ ,  $\dots$  constitute a series of increasing numbers.

If we use the fact that the principal ideals  $(\alpha)$ ,  $(\beta)$ ,  $(\gamma)$ ,  $\dots$  constitute an endless series of ideals whose norms are  $\leq |\sqrt{D}|$ , and observe (Art. 309) that there can exist only a finite number of ideals, whose norms are less or at most equal to a finite rational number, it is seen that of the series  $(\alpha)$ ,  $(\beta)$ ,  $(\gamma)$ ,  $\dots$  two ideals must eventually become equal.

If, say,  $(\alpha) = (\gamma)$ , and if  $|\alpha| > |\gamma|$ , then the quotient  $\epsilon = \frac{\alpha}{\gamma}$  presents a unit of the realm  $\mathfrak{R}(\theta)$ , which is different from  $\pm 1$ . Due to the inequalities for  $\alpha$ ,  $\beta$ ,  $\gamma$ , etc., it is seen that  $|\epsilon| > 1$ ,  $|\epsilon'| > 1$  while  $|\epsilon''| < 1$ , where  $\epsilon' = \frac{\alpha'}{\gamma'}$  and  $\epsilon'' = \frac{\alpha''}{\gamma''}$ .

It is clear that  $|\epsilon|$  and  $|\epsilon'|$  cannot be equal. In an analogous manner one may construct a unit  $\eta$ , for which  $|\eta| > 1$ ,  $|\eta'| < 1$ , and  $|\eta''| > 1$ .

II. Suppose next that the discriminant  $D$  is *negative*. We may assume that  $\Re(\theta)$  is real, while  $\Re(\theta')$  and  $\Re(\theta'')$  are imaginary realms. Due to the Minkowski Theorem two positive real quantities  $A$  and  $A_1$  may be so chosen that  $AA_1^2 = |\sqrt{D}|$  and an integer  $\alpha$  of  $\Re(\theta)$  may be so determined that  $|\alpha| \leq A$  and  $|\alpha'| \leq A_1$ ; and since  $|\alpha'| = |\alpha''|$ , it follows also that  $|\alpha''| \leq A_1$ . In a similar manner as was shown above, it is seen that

$$\left. \begin{aligned} A &\geq |\alpha| \geq \frac{A}{|\sqrt{D}|} \\ A_1 &\geq |\alpha'| \geq \frac{A_1}{|\sqrt{D}|} \end{aligned} \right\}$$

Next write  $B = \frac{A}{|\sqrt{D}|}$  and  $B_1 = A_1 |\sqrt{D}|$ , so that  $BB_1^2 = |\sqrt{D}|$ , and construct the integer  $\beta$  of  $\Re(\theta)$  so that

$$|\beta| \leq B, \quad |\beta'| = |\beta''| \leq B_1.$$

Through a continuation of this process, an infinite series of ideals  $(\alpha), (\beta), \dots$  may be constructed, and as in the case where  $D > 0$  it is evident that there exists a unit different from  $\pm 1$  in each of the three realms  $\Re(\theta), \Re(\theta'), \Re(\theta'')$ .

In the derivation of such units and contrary to the preceding case, it is seen that either  $|\epsilon| > 1$  while  $|\epsilon'| = |\epsilon''| < 1$ , or  $|\eta| < 1$  while  $|\eta'| = |\eta''| > 1$ .

**ART. 314. The Dirichlet Theorem.**<sup>1</sup> *If among the three conjugate realms  $\Re(\theta), \Re(\theta'), \Re(\theta'')$ , there are  $r_1$  real realms and  $\frac{3-r_1}{2}$  pairs of imaginary realms, then in each of the three realms (for example in  $\Re(\theta)$ ) there are  $r = r_1 + r_2 - 1$  fundamental units, namely  $\epsilon_1$  and  $\epsilon_2$  when all three realms are real, and  $\epsilon_1$  when there are a pair of complex*

<sup>1</sup> See Smith's *Report*, where other references are found to Kummer's work and that of Kronecker.



realms. Further, every other unit of the realm in the first case may be expressed in the form  $\pm \epsilon_1^{\epsilon_1} \epsilon_2^{\epsilon_2}$  and in the second case in the form  $\pm \epsilon_1^{\epsilon_1}$ , where  $e_1$  and  $e_2$  are rational integers (see Art. 233).

Minkowski's proof (*loc. cit.*) is as follows (see also Hilbert, *Zahlbericht*, p. 214):

First let  $\mathfrak{R}(\theta)$ ,  $\mathfrak{R}(\theta')$ ,  $\mathfrak{R}(\theta'')$  be three real realms. There are two units  $\epsilon$  and  $\eta$ , see lemma above, such that  $|\epsilon| > 1$ ,  $|\epsilon'| > 1$ ,  $|\epsilon''| < 1$ , and  $|\eta| > 1$ ,  $|\eta'| < 1$ ,  $|\eta''| > 1$ .

If  $\xi$  is any arbitrary integer, the real quantities  $\log |\xi|$ ,  $\log |\xi'|$ ,  $\log |\xi''|$  are called the *logarithms* of the number  $\xi$ .

For brevity we may write

$$l(\xi) = \log |\xi|, \quad l_1(\xi) = \log |\xi'|, \quad l_2(\xi) = \log |\xi''|.$$

If  $\xi$  is a unit,  $\xi\xi'\xi'' = \pm 1$ , and consequently the logarithms of a unit  $\xi$  satisfy the equation

$$f_1(\xi) = l(\xi) + l_1(\xi) + l_2(\xi) = 0, \quad (i)$$

so that every unit must contribute a solution to this equation.

If one or all three logarithms  $l(\xi)$ ,  $l_1(\xi)$ , or  $l_2(\xi)$  is zero, it follows from the preceding article that necessarily  $\xi = \pm 1$ . Hence to derive the units of the realm that are other than  $\pm 1$ , it is necessary to find all the solutions of the equation (i), whose values are different from zero.

Write

$$f_2(\xi) = hl(\xi) + h_1l_1(\xi)$$

and determine  $h$  and  $h_1$  so that

$$f_2(\eta) = hl(\eta) + h_1l_1(\eta) > 0.$$

If we put  $h_1 = -l(\epsilon)$  and  $h = l_1(\epsilon)$ , it is evident that

$$f_2(\eta) = l_1(\epsilon)l(\eta) - l(\epsilon)l_1(\eta) > 0;$$

for  $l_1(\eta)$  is negative since  $|\eta'| < 1$ , while  $l(\eta)$ ,  $l(\epsilon)$ , and  $l_1(\epsilon)$  are positive.

Further note that the required solutions of equation (i)

may be presented in the form

$$\left. \begin{aligned} l(\xi) &= s_1 l(\epsilon) + s_2 l(\eta), \\ l_1(\xi) &= s_1 l_1(\epsilon) + s_2 l_1(\eta), \\ l_2(\xi) &= s_1 l_2(\epsilon) + s_2 l_2(\eta), \end{aligned} \right\} \quad (\text{ii})$$

where  $s_1$  and  $s_2$  are arbitrary real numbers. In fact the three values  $l(\xi)$ ,  $l_1(\xi)$ ,  $l_2(\xi)$  as given in (ii) satisfy identically (i); and corresponding to a given solution  $l(\xi)$ ,  $l_1(\xi)$ , and  $l_2(\xi)$  the quantities  $s_1$  and  $s_2$  may be uniquely determined as finite numbers from the first two of the equations in (ii) in the form

$$s_1 = \frac{l_1(\xi)l(\eta) - l(\xi)l_1(\eta)}{f_2(\eta)},$$

$$s_2 = \frac{-l_1(\xi)l(\epsilon) + l(\xi)l_1(\epsilon)}{f_2(\eta)}.$$

Observe that

$$\begin{aligned} l(\eta) > 0, & \quad l_1(\eta) < 0, & \quad l_2(\eta) > 0, \\ l(\epsilon) > 0, & \quad l_1(\epsilon) > 0, & \quad l_2(\epsilon) < 0, \end{aligned}$$

and that the signs of  $l(\xi)$ ,  $l_1(\xi)$ ,  $l_2(\xi)$  must be at least one positive and one negative. Since  $f_2(\eta) > 0$ , it is seen that when the values just written for  $s_1$  and  $s_2$  are substituted in the third formula under (ii), there is no contradiction as to sign.

For  $\xi = \epsilon$ , we have from (ii)  $s_1 = 1$  and  $s_2 = 0$ , and for  $\xi = \eta$ , it is seen that  $s_1 = 0$ , and  $s_2 = 1$ .

It may be shown next that the inequalities

$$0 \leq s_1 \leq 1, \quad 0 \leq s_2 \leq 1$$

can exist simultaneously for only a finite number of units. For, if these two inequalities exist for a unit  $\xi$ , we necessarily have for the absolute values

$$\begin{aligned} |l(\xi)| &\leq |l(\epsilon)| + |l(\eta)|, \\ |l_i(\xi)| &\leq |l_i(\epsilon)| + |l_i(\eta)| \quad (i=1, 2); \end{aligned}$$

and that is, the absolute values  $|\xi|$ ,  $|\xi'|$ ,  $|\xi''|$  are less than three definite numbers that depend only upon  $\epsilon$  and  $\eta$ .

If then

$$\xi = x + y\omega_2 + z\omega_3$$

(Arts. 93 and 103) represents an integer of the realm  $\mathfrak{R}(\theta)$ , and if  $x, y, z$  are computed from the equations

$$\begin{aligned} x + \omega_2 y + \omega_3 z &= \xi, \\ x + \omega_2' y + \omega_3' z &= \xi', \\ x + \omega_2'' y + \omega_3'' z &= \xi'', \end{aligned}$$

we have

$$x = \lambda_1 \xi + \lambda_2 \xi' + \lambda_3 \xi''$$

with similar values for  $y$  and  $z$ .

The quantities  $\lambda_1, \lambda_2, \lambda_3$  are constants whose absolute values are finite. If further the absolute values of the  $\xi$ 's lie within finite limits, then  $|x|$  must be less than a finite number as must also  $|y|$  and  $|z|$ . Thus it is seen that only a finite number of combinations of rational integral values can be given to  $x, y, z$ , so that  $|\xi|, |\xi'|$ , and  $|\xi''|$  lie within definite limits.

All the units whose expression in the form (ii) is such that

$$0 \leq s_1 \leq 1, \quad 0 \leq s_2 \leq 1$$

may be arranged in two classes.

The first class contains the units, for which  $s_2 = 0$ , while the second class contains those for which  $s_2 > 0$ .

In the first class determine that unit  $\epsilon_1$  for which  $s_1$  takes its *smallest value*, say  $S_1$ , which is different from zero; and in the second class determine that unit  $\epsilon_2$  for which  $s_2$  takes its *smallest value*, say  $S_2$ .

There is then *no* unit other than  $\pm 1$  for whose expression in the form (ii) exist simultaneously the inequalities

$$0 \leq s_1 < S_1 \quad \text{and} \quad 0 \leq s_2 < S_2. \quad (\text{iii})$$

If  $\xi$  denotes an arbitrary unit of the realm, and if  $e_1$  and  $e_2$  are rational integers, to be determined later, then

also  $\frac{\xi}{\epsilon_1^{e_1} \cdot \epsilon_2^{e_2}}$  is a unit of the realm.

Write

$$\begin{aligned} L &= l(\xi) - e_1 l(\epsilon_1) - e_2 l(\epsilon_2), \\ L_1 &= l_1(\xi) - e_1 l_1(\epsilon_1) - e_2 l_1(\epsilon_2), \\ L_2 &= l_2(\xi) - e_1 l_2(\epsilon_1) - e_2 l_2(\epsilon_2). \end{aligned}$$

If we put  $l(\epsilon_1) = S_1 l(\epsilon)$  and  $l(\epsilon_2) = S l(\epsilon) + S_2 l(\eta)$  in the above expressions, we have

$$\left. \begin{aligned} L &= l(\xi) - (e_1 S_1 + e_2 S) l(\epsilon) - e_2 S_2 l(\eta) \\ L_1 &= l_1(\xi) - (e_1 S_1 + e_2 S) l_1(\epsilon) - e_2 S_2 l_1(\eta) \end{aligned} \right\} \quad (\text{iv})$$

Next from (ii) it is seen that we may put  $L$  and  $L_1$  in the form

$$\begin{aligned} L &= s_1 l(\epsilon) + s_2 l(\eta), \\ L_1 &= s_1 l_1(\epsilon) + s_2 l_1(\eta). \end{aligned}$$

Writing these values for  $L$  and  $L_1$  in (iv), it is seen that

$$\begin{aligned} l(\xi) &= (s_1 + e_1 S_1 + e_2 S) l(\epsilon) + (s_2 + e_2 S_2) l(\eta), \\ l_1(\xi) &= (s_1 + e_1 S_1 + e_2 S) l_1(\epsilon) + (s_2 + e_2 S_2) l_1(\eta). \end{aligned}$$

Solving for  $s_1 + e_1 S_1 + e_2 S$  and  $s_2 + e_2 S_2$ , it is seen that

$$\left. \begin{aligned} s_2 &= \frac{-l_1(\xi) l(\epsilon) + l(\xi) l_1(\epsilon)}{f_2(\eta)} - e_2 S_2 \\ s_1 &= \frac{l_1(\xi) l(\eta) - l(\xi) l_1(\eta)}{f_2(\eta)} - e_1 S_1 - e_2 S \end{aligned} \right\} \quad (\text{v})$$

Since  $f_2(\eta) > 0$ , we may determine  $e_2$  from the first of these equations and then  $e_1$  from the second as positive or negative integers such that  $s_1$  and  $s_2$  satisfy the inequalities (iii). But this is contrary to the statement that the two inequalities *can not* be simultaneously satisfied. It follows then that  $L = 0$  and  $L_1 = 0$ . Hence, also  $L_2 = 0$ . And from these equations  $e_1$  and  $e_2$  are determined.

It follows that

$$\frac{\xi}{\epsilon_1^2 \epsilon_2^2} = \pm 1, \quad \text{or} \quad \xi = \pm \epsilon_1^2 \epsilon_2^2$$

and with this the Dirichlet Theorem is proved when the three conjugate realms are real.

For the second case where  $D < 0$ ,  $\Re(\theta)$  being a real realm while  $\Re(\theta')$  and  $\Re(\theta'')$  are a pair of conjugate imaginary realms, let  $\epsilon_1$  be that unit in  $\Re(\theta)$  which has the *smallest absolute* value among all those units whose absolute values are  $> 1$ . It may be then proved in a similar manner as was done above for the units in the real realms that any arbitrary unit  $\xi$  of the realm may be expressed in the form

$$\xi = \pm \epsilon_1^{e_1},$$

where  $e_1$  is a positive or negative rational integer.

For, write  $E = \frac{\xi}{\epsilon_1^{e_1}}$  and suppose that  $E \neq 1$  so that either  $|E| > 1$ , or  $\frac{1}{|E|} > 1$ . In the latter case put  $E = \frac{\epsilon_1^{e_1}}{\xi}$ . It is seen for the first case that  $l(E) = l(\xi) - e_1 l(\epsilon_1)$  and it is clear that  $e_1$  may be so chosen that

$$l(E) < l(\epsilon_1)$$

which is contrary to the assumption made relative to  $\epsilon_1$ . A similar result is had for the second case.

Observe here that from  $l(E) = 0$ , the integer  $e_1$  is uniquely determined and that  $l_1(E)$  is also zero.

#### EXAMPLES

In solving the following examples one may consult the Göttingen dissertation of L. W. Reid, entitled *Tafel der Klassenanzahl für kubische Zahlkörper*. It may be proved that in every class there exists an ideal  $(\alpha)$  such that  $|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^r \frac{3!}{3^3} |\sqrt{D}|$ , where  $r$ , denoting the number of pairs of imaginary roots, is here either 0 or 1. (See Vol. II, Chapt. VIII, of the present work.)

1. If  $\theta$  is a root of the equation

$$x^3 + x + 1 = 0,$$

then is

$$\Delta(\theta) = -31 \quad \text{and} \quad D = -31.$$

Show that the basis of  $\Re(\theta)$  is  $1, \theta, \theta^2$ , and that  $h = 1$ . Show that in



this realm 2 and 5 are irreducible and that

$$3 = (1 - \theta)(\theta^2 + \theta + 2) = \bar{\omega}_1 \cdot \bar{\omega}_2,$$

where  $\bar{\omega}_1$  and  $\bar{\omega}_2$  are principal ideals. The units are  $\theta$  and  $1 + \theta$ .

2. Let  $\theta$  be a root of the equation

$$x^3 + 6x + 8 = 0.$$

Show that

$$\Delta(\theta) = -2592 = -2^5 \cdot 3^4,$$

that  $1, \theta, \frac{\theta}{2}$  may be taken as basis of all integers, and that

$D = -2^3 \cdot 3^4$ . Observe that  $A$  and  $D_1$ , where  $D_1$  is a divisor of  $\Delta(\theta)$  must satisfy the congruences (see Art. 102):

$$3(A - a_1)^2 + 2a_1(A - a_1) + a_2 \equiv 0 \pmod{D_1^2},$$

$$(A - a_1)^3 + a_1(A - a_1)^2 + a_2(A - a_1) + a_3 \equiv 0 \pmod{D_1^3},$$

where here  $a_1 = 0, a_2 = 6, a_3 = -8$ , giving  $A = 0, D_1 = 2$ . Show that

$$(2) = \left(2, 1 + \theta + \frac{\theta^2}{2}\right)^2 \left(2, \frac{\theta^2}{2}\right),$$

$$(3) = (3, \theta - 1)^3,$$

$$(5) = (5, \theta - 1)(5, 2 + \theta + \theta^2),$$

$$(7) = (7, \theta - 2)(7, 3 + 2\theta + \theta^2);$$

that  $h = 3$  and that a unit is  $\theta + 1$ .

3. If  $x^3 + 3x + 5 = 0$  has a root  $\theta$ , show that the basis of all integers of the realm  $\Re(\theta)$  is  $1, \theta, \frac{1 + 2\theta + \theta^2}{3}$ ; that units are  $\theta + 1, \frac{\theta^2 + \theta + 1}{3}$ ; and  $h = 1$ .

4. If  $\theta$  is a root of

$$x^3 + 8x^2 + 2 = 0,$$

show that a basis is  $1, \theta, \frac{3 + 3\theta + \theta^2}{7}$ ; that  $h = 1$ .

5.  $\theta$  being a root of

$$x^3 + 8x + 1 = 0,$$

show that a basis is  $1, \theta, \frac{\theta^2 + 2\theta + 2}{5}$  and that

$$2 = \left(\frac{\theta^2 + 2\theta + 7}{5}\right) \left(\frac{\theta^2 - 3\theta + 7}{5}\right).$$

6. If  $\theta$  is a root of

$$x^3 + 100 = 0,$$

show that a basis is  $1, \theta, \frac{10-10\theta+\theta^2}{3 \cdot 10}$  in the realm  $\Re(\theta)$ ; while  $1, \theta, \frac{-2+2\theta+\theta^2}{3 \cdot 2}$  form a basis in  $\Re(\theta)$ , if  $\theta$  is a root of

$$x^3+28=0.$$

7. In general (see Sommer, p. 261), let  $\theta$  be defined by an irreducible cubic

$$x^3+a_3=0.$$

Suppose further that  $a_3$  is *not* divisible by the third power of a prime integer, and write

$$a_3=n \cdot N^2,$$

where  $n$  and  $N$  are integers. In  $\Re(\theta)$  prove that:

- (1) If  $a_3 \equiv 0 \pmod{3}$ , then  $1, \theta, \frac{\theta^2}{2}$  form a basis.
- (2) If  $a_3 \not\equiv 0 \pmod{3}$ , but  $a_3 \equiv \pm 2$ , or  $a_3 \equiv \pm 4 \pmod{9}$ , then again a basis is  $1, \theta, \frac{\theta^2}{2}$ .
- (3) If  $a_3 \equiv 1 \pmod{9}$ , then  $1, \theta, \frac{N-N\theta+\theta^2}{3N}$  is a basis when  $N \equiv 1 \pmod{3}$ , and  $1, \theta, \frac{-N+N\theta+\theta^2}{3N}$  is a basis when  $N \equiv -1 \pmod{3}$ .
- (4) If  $a_3 \equiv -1 \pmod{9}$ , then  $1, \theta, \frac{N+N\theta+\theta^2}{3N}$  is a basis when  $N \equiv 1 \pmod{3}$  and  $1, \theta, \frac{-N-N\theta+\theta^2}{3N}$  is a basis if  $N \equiv -1 \pmod{3}$ .

**GABINET MATEMATYCZNY**  
Towarzystwa Naukowego Warszawskiego

# INDEX

(The numerals refer to pages)

- Adjoin  
quantities to a realm, 56 ff., 66,  
76, 104, 341, 553.
- Algebra, 110 ff.
- Algebraic integers. (*See* Integer.)  
integers, 110, 133, 554.  
integers, which belong to an ex-  
ponent, 380.  
of a fixed realm, 121 ff., 249 ff.,  
261, 553.  
quantity, 89.
- Algorithm of the Greatest Common  
Divisor, 10, 20, 161.  
ceases to be applicable, 166.
- Ambiguous classes, 460.  
independent, 461.  
number of, 468.  
without ambiguous ideals, 465.
- Ambiguous forms, 509.
- Ambiguous ideals, 408, 461, 509 ff.  
number of, 465.
- Associated integers, 119, 162.
- Basal invariant (*Grundzahl*), 127,  
134, 135, 160, 267.
- Basis of all integers.  
and lattice-points, 532.  
complementary, 270 ff.  
cubic realm, 142 ff., 559, 562, 575.  
minimal, 127, 266.  
of a fixed realm, 125 ff., 130, 140  
ff., 145, 150, 221, 261 ff., 559.  
of a modul, 220, 262.  
of an ideal (quadratic), 342, 348.  
quadratic realm, 133.  
ring, 410.
- Basis of an algebraic realm, 79 ff.,  
122 ff., 155, 269.
- Body (*Körper, Zahlkörper*). (*See*  
Realm.)
- Chain of normal divisors, 101, 107.
- Character-system of an ideal-class,  
451.  
of an ideal, 449.  
of an integer, 449.
- Class.  
of equivalent forms, 498, 527.  
of ideals, 364, 565.  
of ideals and lattices, 540.  
of quadratic forms, 339.  
number of, 366, 480, 527, 568.  
principal, 365.  
product of, 366.  
reciprocal, 366.
- Composition. (*See* Multiplication.)
- Composition of quadratic forms,  
521 ff.
- Congruences, definition, 280.  
and equivalent systems, 286, 301.  
linear with respect to ideals, 384.  
modular systems, 282 ff., 286 ff.,  
321 ff.  
of  $n$ th degree, 321, 378.  
of two functions, 280.  
quadratic, 388, 419.  
simultaneous with respect to  
moduls, 219.  
with respect to algebraic numbers,  
120.  
with respect to ideals, 347 ff., 376,  
387.  
with respect to moduls, 205 ff.,  
234, 321.
- Conjugate.  
ideals, 349.  
numbers, 56, 553.  
realms, 57, 553.  
roots, 56, 142.
- Coordinates of an algebraic number,  
79, 270.

- Dedekind's moduls, 161 ff.  
 Degree of a realm, 57, 102.  
   of a prime ideal, 354, 577.  
   of congruences, 378.  
 Determinants, equal unity, 139.  
 Dirichlet's Theorem regarding units,  
   404, 589.  
 Different.  
   of a cubic number, 556.  
   of a number, 129.  
 Discriminant, 18, 19, 123 ff., 130,  
   157, 261.  
   criterion for a basis, 80.  
   equal unity, 496.  
   divisor of, 364, 395, 461, 583.  
   not equal unity, 558.  
   of algebraic number, 128.  
   of a modul, 262.  
   of an equation, 128.  
   of a quadratic realm.  
   of a ring, 410.  
 Divisibility, 171.  
 Divisibility of one algebraic number  
   by another, 116.  
   of an integer by an ideal, 335, 341,  
   579.  
   of a number by a modul, 174.  
   of ideal classes, 366.  
   of one algebraic integer by an-  
   other, 115, 170.  
   of one ideal by another, 355.  
   of one modul by another, 176, 316.  
   of one modular system by another,  
   286 ff., 328.  
 Division of ideals, 341.  
 Divisor realm, 88.  
 Divisors, 4, 5, 49.  
   modular systems, 312.  
 Divisor of integers, 364, 395.  
   of discriminant. (*See* Discrimi-  
   nant.)  
   of ideals, 355, 565.  
   of modular systems, 283 ff., 325.  
   of moduls, 177, 217.  
   of number of ideal classes, 371.  
   of realms of rationality, 83, 98.  
   (*See* Greatest Common Divisor.)  
 Elements of a modul, 114.  
   basis, 80, 131, 512.  
   ideal, 343, 355.  
   modular system, 283, 294.  
    $n$  independent, 223 ff.  
 Equivalence of ideals, 364 ff., 526,  
   564.  
 Equivalence of linear forms, 280 ff.  
   proper and improper, 498, 513.  
 Equivalent forms (quadratic), 339,  
   498 ff.  
 Equivalent modular systems, 286,  
   301.  
 Euclid's scheme, 10; for Greatest  
   Common Divisor. (*See* Algo-  
   rithm.)  
 Existence of roots, 51.  
   of genuses, 469, 475.  
 Exponent of algebraic integer, 380.  
 Extreme element, 170.  
 Factors, 1, 2, 49.  
   irreducible, 49, 172.  
   of algebraic integers, 162, 169 ff.,  
   559.  
   of ideals, 353, 356, 573. (*See*  
   Kummer.)  
   of integral functions, 1, 2, 6, 326.  
 Fermat's Greater Theorem, 481.  
   in algebraic realms, 489, 492.  
   Kummer, 485.  
   Legendre, 483.  
 Fermat's Theorem.  
   for ideals, 376.  
   for modular systems, 299.  
   generalization for moduls, 215 ff.,  
   328.  
 Forms, conjugate.  
   correlated with ideals of quadratic  
   realms, 497 ff., 504 ff.  
   equivalent, 498.  
   linear homogeneous, 22. (*See*  
   Minkowski.)  
   primitive, 497, 518, 520.  
   principal, 502.  
   proper and improper equivalent,  
   498.  
   quadratic, 338, 497 ff.  
   reduced, 528.

- with prime ideals, 507.
- Function, reducible, 1, 2, 40, 53.  
 algebraic, 55.  
 hyperbolic, 543.  
 integral, 284 ff., 366.
- Fundamental set of lattice-points, 531.  
 in cubic realms, 589.  
 units in quadratic realms, 398.
- Galois' Realms, 66, 93. (*See Normal.*)
- Gattung (Kronecker), 77.
- Gaussian Lemma, 3.  
 generalization of, 42.
- Generation of realms, 38, 56, 64.
- Genus.  
 application, 475.  
 existence of 469.  
 number of, 474.  
 of quadratic realms, 452.  
 principal, 452.
- Geometric meaning of ideals (quadratic), 530 ff.
- Geometry of numbers. (*See Minkowski.*)
- Greatest Common Divisor, 22, 162.  
 ceases to be applicable, 166.  
 Euclid's scheme for finding, 21.  
 of algebraic integers, 172.  
 of ideals, 355.  
 of modular systems, 288.  
 of moduls, 179 ff., 257 ff.  
 of realms, 58.  
 ring-ideals, 411.
- Greatest Common Divisor of numbers, 10, 20.  
 of functions, 12, 49.  
 of modular systems, 288.  
 of moduls, 179.  
 of realms, 92, 99.
- Hensel's Theorem, 331.
- Hilbert, Law of Reciprocity, 433 ff.  
 number-ring, 409.  
 proof of Minkowski's Theorem, 22.  
 symbol for norm-residues, 433 ff.
- Hurwitz, proof of Minkowski's Theorem, 22.
- Ideal numbers, 501, 552; of Plato, 530. (*See Kummer.*)
- Ideals, 169, 335.  
 ambiguous, 408, 461, 509 ff.  
 basis of, 340  
 canonical basis, 343.  
 classes, finite number of, 366, 480, 577.  
 correlation of and quadratic forms 339, 497 ff.  
 divisibility, 341, 563, 565.  
 equality of, 341.  
 equivalent. (*See Equivalent.*)  
 factors of prime integers, 358.  
 forms, 339.  
 geometrical presentation of, 530 ff.  
 multiplication of, 341, 563.  
 (name), 338, 561.  
 norm of, 347, 574.  
 of cubic realms, 560.  
 of quadratic realms, 340 ff.  
 Poincaré's method of presenting, 551.  
 prime, 354, 356, 364, 572.  
 principal, 341, 346, 502, 533, 545, 569.  
 reciprocal, 577.  
 ring, 410.  
 simple examples of, 334.
- Imprimitive numbers. (*See Primitive.*)
- Incongruent units, complete system.  
 system of residues. (*See Residues.*)  
 with respect to a modular system, 298.
- Index of algebraic number, 128, 134.
- Integer, algebraic, 110.  
 belongs to an exponent, 380.
- Integer, expressed through sum of squares, 417, 429 ff.
- Integers, sum, product, 112 ff., 553 ff.
- Integral function, 6.
- Integrity, realms of, 37 ff.
- Irreducible equation, 52, 78, 91.  
 function, 84.
- Irreducibility of certain functions, 9, 40, 53.



- Jacobi, Law of Reciprocity, 529.
- Kummer factors, 337.
- Kummer (*see* Ideal) numbers, 500, 501, 552.
- Lagrange, interpolation formula, 15.
- Lattice-points, 531 ff.  
and ideal classes, 540.  
bases of quadratic realms, 532.  
fundamental set of, 531, their number 538.  
of an imaginary realm, 530 ff.  
of a real realm, 541 ff.
- Lattices, 531.  
reverting into themselves, 549.  
similar and principal ideals, 535.  
unit, 549.
- Leader, of a ring, 411.
- Linear form, 22, 123, 173, 281 ff.
- Linear independent quantities, 68, 123, 133, 221 ff., 258.  
Criterion for, 69.
- Least common multiple.  
of modular systems, 288.  
of moduls, 177 ff.  
of realms, 58, 99.
- Legendre's symbol for quadratic residues. (*See* Symbol.)
- Measure of lengths, Euclid, 541.  
Descartes, 541.  
pseudometric, 541.
- Mesh, 531.
- Minkowski's Theorem for linear forms, 23 ff., 399.  
Geometrie der Zahlen, 529, 552.  
Theorem as to number of ideal classes, 366, 566, 577.
- Modular systems (Kronecker), 268 ff., 280 ff. (*See* Order-modul.)  
as divisors, 325 ff.  
canonical forms of, 305 ff.  
decomposition of, 300, ff., 317.  
mixed, 292.  
multiplication of, 287.  
of first kind, 291.  
of second kind, 291, 317.  
prime, 315, 319.  
pure, 292, 317 ff.  
reduction of, 303 ff.
- Moduls (Dedekind), 161 ff.  
algebraic, 248 ff.  
complementary, 268 ff.  
defined, 173.  
equal, 177.  
finite, 220 ff., 247.  
integral, 267.  
multiplication of, 185, 248.  
multiplication of by algebraic integers, 183.  
of finite order, 176, 181, 186, 257 ff.  
product of, 185.  
quotient of, 193, 248.
- Multiple of a modul, 177, 217, 221.  
modular system, 283.
- Multiplication of ideals, 341, 521, 563.  
of modular systems, 287.  
of moduls, 185, 248.  
(*See* Composition.)
- Norm.  
of a quadratic realm, 347.  
less than  $|\sqrt{D}|$ , 366, 579.  
of a cubic realm, 574.  
of a divisor of a realm, 98, 101.  
of an algebraic number, 74, 110, 116.  
of an ideal, 347, 574.  
of a product, 351, 576.  
of a realm, 66.  
of fundamental unit, 407.  
of several realms, 96.
- Normal realms. (*See* Galois.)
- Norm-residues, 433 ff.  
symbol of, 433, 351, 576.
- Order of a modul, 176, 221, 228, 258.
- Order-modul ("Art", "Species"), 201, 204, 247, 249, 260, 261.
- Pell's equation, 137.
- $\Phi$ -function of Euler.  
defined for ideals, 372.  
product theorem, 375.  
summation theorem, 376.

- Prime number, 162.  
   and correlated forms, 507.  
   ideal, 354.  
   factor of prime integer, 356, 364.  
   ideal in cubic realms, 580.  
   ideal in quadratic realms, 354.  
   factor of prime integer, 356, 364.  
   factors, resolution of ideals into,  
     354, 573.  
   function, 41.  
   modular system, 315 ff.  
   relatively, 45, 48, 343.  
   relative to an ideal, 358 ff.  
   relative to modular system, 297.
- Primitive function, 4, 43, 47.  
   forms, 497, 418, 520.  
   number with respect to a prime  
     ideal, 379.  
   quantities, 77, 85, 86, 108.
- Product of ideal and its conjugate,  
   349.  
   forms or functions, 40.  
   of ideal classes, 366.  
   of ideals, 356, 413.  
   of modular systems, 287, 317.  
   of moduls, 185, 248.  
   of norms, 351.  
   of primitive functions, 5, 44.
- Pseudometric geometry, 541.
- Quotient of moduls, 193.
- Realm (*Körper*, *Zahlkörper*), 1, 37.  
   absolute, 38.
- Realm of rationality, 33 ff.  
   algebraic, 55 ff., 57, 71, 89.  
   algebraic realm determined by  
     algebraic quantity, 76.  
   biquadratic, 107.  
   conjugate, 57.  
   cubic, 105, 139, 150, 553.  
   cyclotomic, 155 ff., 496.  
   defined, 284.  
   degree of, 57.  
   derivation of, 38, 56, 64.  
   divisor, 88, 100.  
   finite, 76 ff., 257, 261.  
   identical, 39, 61, 85.  
   quadratic, 133.  
   stock, 39, 92.
- Realm, normal, 56, 92, 106, 108.  
 Realm, simple, 100.
- Reciprocity, quadratic law for prime  
   integers, 417 ff.  
   in a quadratic realm, 390.
- Reducible function 1, 2, 40.  
   equation, 110.
- Relative equality of two realms, 95.
- Representatives, complete system of  
   with respect.  
   to a modul, 209.  
   to an ideal, 347.
- Residues, norm—, 433 ff.
- Residues, quadratic, 388 ff.  
   complete system of incongruent,  
     with respect to a modul, 209.  
   complete system, with respect to  
     prime integer, 435.  
   number of, 232, 236 ff.  
   with respect to a modular system,  
     297.  
   with respect to a modul, 205.  
   with respect to an ideal, 347, 352,  
     380, 574.
- Resultant defined, 16.
- Ring ideal, 410.
- Ring-leader, 411.
- Ring-number, 409 ff.
- Root-expression, 104.
- Root of polynomials, 8, 53.  
   of congruences, 321, 379.  
   of equations, 56, 111, 257.  
   multiple, 10.
- Schönemann Theorem, 10, 11.
- Spur of an algebraic number, 74,  
   110, 116, 152.
- Standard curve in pseudometric ge-  
   ometry, 542.
- Symbol  $\left(\frac{p}{q}\right)$  of Legendre, 360 ff.
- Symbol  $\left(\frac{d}{p}\right)$ , 388.
- Symbol  $\left(\frac{n, m}{p}\right)$ , 434 ff.

- Symbol,  $(a, b)$ , 209.  
 value of this integer, 235 ff., 277.
- Transcendental quantity, 55.
- Unique factorization of ideals, 354 ff.
- Unique factorization of rational integers, 20.  
 failure of, 167 ff., 334 ff.  
 of algebraic integers, 162, 165, 339.  
 of polynomials, 49.
- Unit, geometric meaning of, 540, 548.  
 complementary, 300, 321.
- Unit ideal, 341.
- Unit modul, 248, 251, 253 ff.
- Unit modular system, 298 ff., 316.
- Units, algebraic, 117.  
 of a character-system, 449 ff.  
 their product, 459 ff.
- Units, number of incongruent, 298, 320.  
 and lattice-points, 540, 548. (*See* Dirichlet.)
- Units of a cubic realm, 584 ff.  
 cyclotomic realm, 156.  
 quadratic realm, 136, 345, 396, 403.
- Units of a ring, 411, 415.  
 fundamental in cubic realms, 589.  
 fundamental in quadratic realm, 403, 479.
- Units, system of independent, 298.
- Wilson's Theorem.  
 for ideals, 382.  
 for modular systems, 323.

~~GABINET MATEMATYCZNY  
 Towarzystwa Naukowego Warszawskiego~~







