XVI.

Sur la théorie des nombres complexes idéaux. (Extrait d'une lettre adressée à M. Hermite.)

[Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Paris, Bd. 90, S. 1205—1207 (1880).]

Je prends la liberté de vous communiquer la remarque suivante sur les théorèmes signalés par M. Sylvester dans les *Comptes rendus* des 16 et 23 février, lesquels se rapportent à quelques congruences ressortant de la théorie de la division du cercle. Comme toute la théorie des congruences est entièrement contenue dans celle des *idéaux*, les théorèmes de M. Sylvester ne sont que des conséquences très spéciales d'un seul théorème, par lequel sont définis tous les idéaux qui se rencontrent dans la théorie des nombres, composés rationnellement de racines de l'unité. Ce théorème, comme je l'ai déjà fait remarquer dans le § 27 de mon Mémoire *Sur la théorie des nombres entiers algébriques* (Paris, 1877, p. 109), se déduit facilement des résultats obtenus par M. Kummer, à l'aide de certains principes généraux dont l'exposition complète dépasserait les bornes de cette Communication; pour le moment, il suffira d'énoncer le théorème en question.

Soit θ une racine primitive de l'équation $\theta^m = 1$; l'ensemble K_m de tous les nombres $\eta = F(\theta)$ qui se déduisent de θ par les opérations rationnelles de l'Arithmétique constitue ce que j'appelle un *corps* de nombres; la théorie des idéaux de ce corps cyclotomique K_m, dont le *degré* est égal à $\varphi(m)$, a été établie par M. Kummer (*Mémoires de l'Académie de Berlin*, 1856). Prenons maintenant un nombre déterminé $\eta = F(\theta)$, et cherchons le degré n de l'équation irréductible $\psi(\eta) = 0$, dont η est la racine; pour cela, il faut considérer le système de tous les nombres entiers rationnels qui sont premiers avec m et incongrus suivant m; parmi ces nombres, dont le nombre est égal à $\varphi(m)$, il y a un système (h), comprenant tous

les exposants h, qui satisfont à la condition $F(\theta^h) = F(\theta)$ et qui forment un *groupe*, c'est-à-dire que le produit de deux quelconques d'entre eux se trouve dans le même système (h); le nombre de ces exposants h est $\frac{\varphi(m)}{n}$.

L'ensemble de tous les nombres $\omega = f(\eta)$, composés rationnellement de η, constitue un corps cyclotomique Ω de degré n, lequel est un *diviseur* du corps K_m. Réciproquement, si Ω est un corps dont tous les nombres sont contenus dans le corps K_m, il existe toujours des nombres η qui engendrent le corps Ω de la manière indiquée ci-dessus. Le corps Ω est complètement déterminé par le groupe (h), et à chaque groupe (h) correspond un corps Ω.

Après avoir rappelé ces principes bien connus de la théorie de la division du cercle, je vais maintenant proposer le théorème général sur les idéaux d'un tel corps cyclotomique Ω. En me servant des notations dont j'ai fait usage dans le Mémoire cité plus haut, je désigne par v l'idéal principal consistant en tous les nombres *entiers* contenus dans le corps Ω. Soit p un nombre premier quelconque (rationnel, positif); on peut poser $m = m'p'$, où p' désigne la plus haute puissance de p, laquelle divise le nombre m; soit en outre $\frac{\varphi(p')}{g}$ le nombre de tous ceux, parmi les nombres h contenus dans le groupe (h), qui sont égaux à $1 \pmod{m'}$, et soit f le plus petit exposant positif qui satisfasse à la condition que p^f soit congru, suivant le module m', à l'un des nombres h du groupe (h); alors le degré n du corps Ω sera divisible par le produit fg, et, si l'on pose $n = efg$, on aura la décomposition

$$vp = (\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e)^g,$$

où les e idéaux premiers $\mathfrak{p}$ sont différents entre eux; le *degré* de ces idéaux est égal à f, c'est-à-dire que leur *norme* est donnée par l'équation

$$N(y) = p^f.$$

Ce théorème général revient à celui de M. Kummer pour le cas $n = \varphi(m)$.

Dans un Mémoire sur la dépendance entre la théorie des congruences et celle des idéaux (Göttingue, 1878), j'ai démontré que les équations irréductibles de degré n auxquelles satisfont les nombres entiers d'un corps quelconque Ω de degré n, prises par rapport à

un module premier p, se résolvent en facteurs irréductibles, dont les degrés coïncident, en général, avec les degrés des idéaux premiers $\mathfrak{p}$ qui divisent le nombre p. Par suite, la condition pour que ces congruences aient des racines *commensurables* [*)] consiste dans l'existence d'un tel idéal $\mathfrak{p}$ dont le degré soit égal à 1. En faisant l'application de ce fait à notre exemple, où il s'agit des équations $\psi(\eta) = 0$ de la division du cercle, on voit bien que les racines x de la congruence cyclotomique $\psi(x) \equiv 0 \pmod{p}$ ne seront commensurables que dans le cas $f = 1$, c'est-à-dire dans le cas que p soit congru, suivant le module m', à l'un des nombres h du groupe (h). Pour descendre finalement de la théorie générale aux théorèmes de M. Sylvester, il suffit d'observer que le corps Ω du degré $\frac{1}{2}\varphi(m)$, qui provient du nombre $\eta = \theta + \theta^{-1}$, correspond au groupe (h) des deux nombres $h \equiv \pm 1 \pmod{m}$[**)].

[*) D. h. im rationalen Bereiche lösbar sind.]

[**) Sylvester hat in zwei Noten [Compt. rend., Bd. 90, S. 287—289, 345—347 (1880)] gezeigt, daß dieses spezielle Polynom $\psi(x)$, abgesehen von Teilern von m, nur Primzahlteiler von der Form $p = tm \pm 1$ haben kann.]