XXXVIII.

Charakteristische Eigenschaft einklassiger Körper Ω.

Die erforderliche und hinreichende Bedingung dafür, daß ein endlicher Körper Ω einklassig ist, besteht darin, daß für je zwei ganze Zahlen α, β in Ω, deren letztere β von Null verschieden ist, immer zwei ganze Zahlen μ, ν in Ω gewählt werden können, deren erstere μ relative Primzahl zu β ist, und für welche die Norm $N(\alpha\mu + \beta\nu)$ absolut $< N(\beta)$ ist.

Beweis. I. Ist Ω einklassig, und $\mathfrak{o}$ die Hauptordnung, d. h. das System aller ganzen Zahlen in Ω, so ist

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}\delta \text{ (Hauptideal).}$$

Ist α teilbar durch β, so kann man $\delta = \beta$, $\alpha = \beta\gamma$, $\mu = -1$, $\nu = \gamma$ setzen, wodurch den Forderungen genügt wird, weil μ relative Primzahl zu β, wo $N(\alpha\mu + \beta\nu) = 0$ abs. $< N(\beta)$ ist. Wenn aber α nicht teilbar durch β ist, so setze man

$$\alpha = \delta\alpha_1, \quad \beta = \delta\beta_1, \quad \text{also} \quad \mathfrak{o}\alpha_1 + \mathfrak{o}\beta_1 = \mathfrak{o};$$

mithin sind α_1, β_1 relative Primzahlen, und es gibt ganze Zahlen α_2, die der Kongruenz

$$\alpha_1\alpha_2 \equiv 1 \pmod{\beta_1}$$

genügen (§ 174, S. 533, § 178, XIII, S. 559 und S. 556).

Ist nun π das Produkt aller derjenigen in δ aufgehenden Primzahlen des Körpers Ω, die nicht in β_1 aufgehen (evtl. $\pi = 1$, wenn es keine solche Primzahl gibt), so sind β_1, π relative Primzahlen, und folglich (§ 180, II, S. 568) gibt es in $\mathfrak{o}$ Zahlen μ, die den simultanen Kongruenzen

$$\mu \equiv \alpha_2 \pmod{\beta_1}, \quad \mu \equiv 1 \pmod{\pi}$$

genügen; hieraus folgt, daß μ relative Primzahl zu π und (wie α_2) zu β_1, also auch zu β ist, weil jede in $\beta = \delta\beta_1$ aufgehende Primzahl entweder in β_1 oder in δ, also in π aufgeht. Aus der ersteren dieser Folgerungen folgt ferner

$$\alpha_1\mu \equiv \alpha_1\alpha_2 \equiv 1 \pmod{\beta_1},$$

also gibt es in $\mathfrak{o}$ eine Zahl ν, die der Bedingung

$$\alpha_1\mu + \beta_1\nu = 1, \quad \alpha\mu + \beta\nu = \delta$$

genügt, woraus der Beweis von I, nämlich

$$N(\alpha\mu + \beta\nu) = N(\delta) = \frac{N(\beta)}{N(\beta_1)} \text{ abs.} < N(\beta)$$

folgt, weil β_1 keine Einheit, also $N(\beta_1) > 1$ ist (α nicht teilbar durch β).

II. Umkehrung: Der endliche Körper Ω, dessen Hauptordnung $\mathfrak{o}$, ist gewiß einklassig, wenn es für je zwei Zahlen α, β in $\mathfrak{o}$, deren letztere von Null verschieden ist, immer zwei Zahlen μ, ν in $\mathfrak{o}$ gibt, deren erstere relative Primzahl zu β ist, und die der Bedingung

$$N(\alpha\mu + \beta\nu) \text{ abs.} < N(\beta)$$

genügen.

Bei dem Beweise wollen wir, wenn α, β, α', β' Zahlen in $\mathfrak{o}$ sind, durch das Zeichen

$$(\alpha, \beta) \sim (\alpha', \beta')$$

andeuten, daß der Komplex aller gemeinsamen Teiler von α, β identisch mit dem aller gemeinsamen Teiler von α', β' ist. Sind nun α, β gegeben, und μ, ν so gewählt, daß sie den beiden Bedingungen genügen, und setzen wir

$$\gamma = \alpha\mu + \beta\nu,$$

so folgt daraus

$$(\alpha, \beta) \sim (\beta, \gamma);$$

denn offenbar ist jeder gemeinsame Teiler von α, β auch ein Teiler von γ, also gemeinsamer Teiler von β, γ; und aus $\alpha\mu = \gamma - \beta\nu$ folgt, daß jeder gemeinsame Teiler von β, γ auch ein Teiler von $\alpha\mu$ und, weil er als Teiler von β relative Primzahl zu μ ist, auch Teiler von α, also gemeinsamer Teiler von α, β ist, wie behauptet war. Aus jedem Paare α, β, wo β von Null verschieden, kann man daher eine Zahl γ in $\mathfrak{o}$ bilden, die den Bedingungen

$$(\alpha, \beta) \sim (\beta, \gamma) \quad \text{und} \quad N(\gamma) \text{ abs.} < N(\beta)$$

genügt.

Der Fall $\gamma = 0$ tritt offenbar nur dann ein, wenn jeder Teiler von β, also auch β selbst in α aufgeht (und umgekehrt, wenn α durch β teilbar ist, so kann man μ, ν wie in I so wählen, daß $\gamma = 0$ wird); in diesem Fall besitzen also α, β einen größten gemeinsamen Teiler β.

Ist aber γ von Null verschieden, so kann man wieder eine Zahl δ in $\mathfrak{o}$ bilden, die den Bedingungen

$$(\gamma, \delta) \sim (\beta, \gamma) \sim (\alpha, \beta) \quad \text{und} \quad N(\delta) < N(\gamma) < N(\beta)$$

genügt, woraus offenbar auch $(\gamma, \delta) \sim (\alpha, \beta)$ folgt. Fährt man, wenn δ nicht Null ist, so fort, so erhält man eine Reihe von Zahlen $\beta, \gamma, \delta, \varepsilon, \cdots$ in $\mathfrak{o}$, deren Normen absolut immer kleiner werden; es muß daher in dieser Reihe nach einer endlichen Anzahl von Schritten auch die Zahl Null auftauchen, und wenn τ in ihr die letzte von Null verschiedene Zahl ist, so ergibt sich:

$$(\alpha, \beta) \sim (\tau, 0),$$

woraus wie oben folgt, daß je zwei Zahlen α, β in $\mathfrak{o}$, deren letzte nicht verschwindet, einen größten gemeinsamen Teiler τ in $\mathfrak{o}$ besitzen, was auch durch

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}\tau$$

ausgedrückt werden kann; mithin ist (§ 178, XII, S. 559) jedes Ideal des Körpers Ω ein Hauptideal, d. h. Ω ist einklassig, w. z. b. w.

Erläuterungen zur vorstehenden Abhandlung.

Das hier gegebene Kriterium ist erst in neuester Zeit — im Rahmen allgemeinerer Untersuchungen — wiedergefunden worden: H. Hasse, Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen. J. f. M. **159** (1928), S. 3—12. Die Zitate beziehen sich auf die 4. Auflage von Dirichlet-Dedekind; der Satz selbst liegt aber viel weiter zurück, wie eine nicht druckfertige, sehr alte Ausarbeitung zeigt.

Noether.