Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0187
LOG Titel: §. 168. Primideale in quadratischen Körpern
LOG Typ: chapter

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

§. 168.

Wir wollen nun zum Schlusse die vorhergehenden allgemeinen Untersuchungen auf die quadratischen Körper anwenden, um von dem gewonnenen Standpunct aus den Hauptgegenstand dieses Werkes noch einmal zu überblicken.

Ist die ganze rationale Zahl D keine Quadratzahl und auch durch kein Quadrat (ausser 1) theilbar, so bilden die Zahlen $t + u\sqrt{D}$, wenn t, u alle rationalen Zahlen durchlaufen, einen quadratischen Körper, welcher durch die beiden Substitutionen $\varphi(t + u\sqrt{D}) = t \pm u\sqrt{D}$ in sich selbst übergeht. Setzt man $\theta = \frac{1}{2}(1 + \sqrt{D})$ oder $= \sqrt{D}$, je nachdem $D \equiv 1 \pmod 4$ ist oder nicht, so bilden die Zahlen $1, \theta$ eine Grundreihe des Körpers, und seine Grundzahl Δ ist entsprechend $= D$ oder $= 4D$. Die quadratische Gleichung, welcher θ genügt, sei

$$f(\theta) = \theta^2 - b\theta + c = 0,$$

so ist $x + y\theta$ mit $x + y(b - \theta)$ conjugirt, und

$$\Delta = (2\theta - b)^2 = b^2 - 4c.$$

Ist nun $\mathfrak{p}$ irgend ein Primideal des Körpers, und p die durch $\mathfrak{p}$ theilbare positive rationale Primzahl, so ist $N(\mathfrak{p}) = p^2$ oder $= p$, je nachdem $\mathfrak{i}(p) = \mathfrak{p}$ oder ein Product aus zwei Primidealen $\mathfrak{p}, \mathfrak{p}'$ ist. Im letzteren Falle bilden die Zahlen $0, 1, 2 \ldots (p - 1)$, weil sie incongruent sind, ein vollständiges Restsystem (mod. $\mathfrak{p}$), d. h. jede ganze Zahl des Körpers ist einer rationalen ganzen Zahl congruent; mithin giebt es auch eine rationale ganze Zahl t, welcher θ congruent ist, und folglich ist $f(t) = t^2 - bt + c$ eine ganze rationale durch $\mathfrak{p}$, also auch durch p theilbare Zahl, d. h.

$$t^2 - bt + c \equiv 0 \pmod p,$$

oder in der Sprache der Theorie der höheren Congruenzen: die quadratische Function $f(x) = x^2 - bx + c$ ist nach dem Modul p congruent einem Producte aus zwei Functionen ersten Grades $(x - t)$ und $(x - b + t)$ mit rationalen Coefficienten. Umgekehrt: hat die Congruenz $f(x) \equiv 0 \pmod p$ eine rationale Wurzel $x \equiv t$, so ist

$$f(t) = (t - \theta)(t - b + \theta) \equiv 0 \pmod p;$$

wäre nun $\mathfrak{i}(p)$ ein Primideal, so müsste wenigstens einer der Factoren $(t-\theta)$, $(t-b+\theta)$ durch p theilbar sein, was aber nicht der Fall ist, weil die Zahlen $1, \theta$ eine *Grundreihe* des Körpers bilden; mithin ist $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ ein Product aus zwei Primidealen $\mathfrak{p}$ und $\mathfrak{p}'$, deren Normen $= p$ sind; ist nun $t-\theta$ durch $\mathfrak{p}$ theilbar, also $\mathfrak{i}(t-\theta) = \mathfrak{p}\mathfrak{q}$, so ist $\mathfrak{q}$ nicht theilbar durch $\mathfrak{p}'$, weil sonst $(t-\theta)$ durch p theilbar wäre, und da $\mathfrak{i}(t-\theta)\,\mathfrak{i}(t-b+\theta) = \mathfrak{p}\mathfrak{q}\mathfrak{i}(t-b+\theta)$ durch $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ theilbar ist, so muss $(t-b+\theta)$ durch $\mathfrak{p}'$ theilbar sein; man kann daher

$$\theta \equiv t \pmod{\mathfrak{p}}, \quad \theta \equiv b - t \pmod{\mathfrak{p}'}$$

setzen, und $\mathfrak{p}$, $\mathfrak{p}'$ *conjugirte* Primideale nennen, weil aus $x + y\theta \equiv 0 \pmod{\mathfrak{p}}$ stets $x + y(b-\theta) \equiv 0 \pmod{\mathfrak{p}'}$ folgt.

Es fragt sich nun, ob diese beiden Primideale $\mathfrak{p}$, $\mathfrak{p}'$ identisch sein können. Dann muss $\theta \equiv t \equiv b - t \pmod{\mathfrak{p}}$, also $2t - b$ durch $\mathfrak{p}$ und folglich auch durch p theilbar sein, und da $4f(t) = (2t-b)^2 - \Delta \equiv 0 \pmod{p}$ ist, so muss

$$\Delta \equiv 0 \pmod{p}$$

sein. Umgekehrt: ist p eine in der Grundzahl $\Delta = b^2 - 4c$ aufgehende rationale Primzahl, so giebt es immer eine ganze rationale t, welche den beiden Congruenzen

$$f(t) \equiv 0, \quad 2t \equiv b \pmod{p}$$

genügt; ist nämlich p ungerade, so ist t durch die zweite Congruenz bestimmt, und aus $4f(t) = (2t-b)^2 - \Delta$ folgt $f(t) \equiv 0$; ist aber $p = 2$, also b gerade, so ist t durch die erste Congruenz $f(t) \equiv t^2 + c \equiv 0 \pmod{2}$ bestimmt, nämlich $t \equiv c \pmod{2}$, und die zweite Congruenz ist ebenfalls erfüllt. Aus der Existenz einer rationalen Wurzel t der Congruenz $f(t) \equiv 0$ folgt aber, wie oben gezeigt ist, $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$, wo $\mathfrak{p}$ und $\mathfrak{p}'$ zwei Primideale bedeuten, für welche $\theta \equiv t \pmod{\mathfrak{p}}$, $\theta \equiv b - t \pmod{\mathfrak{p}'}$ ist; da nun ausserdem $t \equiv b - t \pmod{p}$ ist, so folgt, dass $(\theta - t)$ sowohl durch $\mathfrak{p}$ als auch durch $\mathfrak{p}'$ theilbar ist; wären nun $\mathfrak{p}$ und $\mathfrak{p}'$ verschieden, also relative Primideale, so müsste $(\theta - t)$ auch durch $\mathfrak{p}\mathfrak{p}'$, d. h. durch p theilbar sein; da dies nicht der Fall ist, so sind $\mathfrak{p}$ und $\mathfrak{p}'$ identisch, also ist $\mathfrak{i}(p) = \mathfrak{p}^2$. Wir sind mithin zu folgendem Resultat gelangt:

Geht die rationale Primzahl p in der Grundzahl Δ auf, so ist $\mathfrak{i}(\mathfrak{p}) = \mathfrak{p}^2$ das Quadrat eines Primideals $\mathfrak{p}$; ist p eine in Δ nicht aufgehende Primzahl, so ist $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ ein Product aus zwei

verschiedenen Primidealen $\mathfrak{p}, \mathfrak{p}'$, *oder* $\mathfrak{i}(p)$ *ein Primideal, je nachdem die Congruenz* $f(t) \equiv 0 \pmod{p}$ *eine rationale Wurzel* t *besitzt oder nicht.*

Die Zahl $p = 2$ bietet den ersten Fall dar, wenn $\Delta \equiv 0 \pmod 4$, also $D \equiv 2, 3 \pmod 4$ ist; ist dagegen $\Delta = D \equiv 1 \pmod 4$, so tritt der zweite oder dritte Fall ein, je nachdem c gerade oder ungerade, d. h. je nachdem $D \equiv 1$ oder $\equiv 5 \pmod 8$ ist. Hieraus erklärt sich das eigenthümliche Verhalten der Zahl 2 in der Theorie der quadratischen Reste (§. 36).

Ist p eine ungerade, in Δ nicht aufgehende rationale Primzahl, so folgt aus $4f(t) = (2t - b)^2 - \Delta$, dass der zweite oder dritte Fall eintritt, je nachdem

$$\left(\frac{\Delta}{p}\right) = \left(\frac{D}{p}\right) = +1 \quad \text{oder} = -1$$

ist. Um alle Fälle am bequemsten zusammenzufassen, führen wir für jede positive ganze rationale Zahl m eine Charakteristik (Δ, m) der Art ein, dass

$$(\Delta, mm') = (\Delta, m)\,(\Delta, m')$$

und, wenn p eine rationale Primzahl bedeutet,

$$(\Delta, p) = 0, \quad = +1, \quad = -1$$

ist, je nachdem $\mathfrak{i}(p)$ Quadrat eines Primideals, oder ein Product aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist. Bedeutet nun $\tau(m)$ die Anzahl aller verschiedenen Ideale $\mathfrak{a}$, deren Normen $= m$ sind, so ist

$$\tau(p^r) = (\Delta, 1) + (\Delta, p) + (\Delta, p^2) + \cdots + (\Delta, p^r),$$

und allgemein

$$\tau(m) = \Sigma\,(\Delta, n),$$

wo n alle Divisoren von m durchläuft. Hieraus folgt (vergl. §§. 89, 91, 124)

$$\Sigma \frac{\tau(m)}{m^s} = \Sigma \frac{1}{m^s} \Sigma \frac{(\Delta, m)}{m^s},$$

also, wenn $(s - 1)$ positiv unendlich klein wird,

$$\lim \Sigma \frac{s-1}{N(\mathfrak{a})^s} = \lim \Sigma \frac{(\Delta, m)}{m^s},$$

wo m nur alle diejenigen positiven ganzen rationalen Zahlen zu durchlaufen braucht, welche relative Primzahlen zu Δ sind, oder auch