REIN ARITHMETISCHER BEWEIS ÜBER DIE UNENDLICHKEIT DER PRIMIDEALE 1. GRADES AUS EINEM ENDLICHEN ALGEBRAISCHEN ZAHLKÖRPER

von

Mikao MORIYA

Es sei P der rationale Zahlkörper und K ein algebraischer Zahlkörper vom Grade n über P. Dann gilt bekanntlich folgender Satz:

In K gibt es unendlich viele Primideale 1. *Grades.* Zum Beweis dieses Satzes nimmt man bisher, soweit ich weiß, ein transzendentes Hilfsmittel—die DEDEKINDsche ζ-Funktion—zu Hilfe. In der vorliegenden Note will ich aber zu zeigen versuchen, wie man diesen Satz ohne Benutzung der ζ-Funktionen beweisen kann.

Wir greifen zunächst aus K ein primitives Element θ von K/P heraus, welches eine ganze algebraische Zahl ist. Bezeichnet nun ω_1, ω_2, $\cdots$, ω_n eine Minimalbasis der Hauptordnung von K, so gilt:

$$\theta^i = c_{i1}\,\omega_1 + \cdots + c_{in}\,\omega_n \qquad i = 0,1, \cdots, n-1,$$

wo die c_{ij} ganz rational sind. Setzt man hierbei

$$C = \begin{vmatrix} c_{01} & \cdots & c_{0n} \\ \vdots & & \\ c_{n-1\,1} & \cdots & c_{n-1\,n} \end{vmatrix},$$

so gilt offenbar für eine beliebige ganze algebraische Zahl γ aus K:

$$\gamma\, C = \sum_{i=0}^{n-1} a_i\, \theta^i \qquad ,$$

wo die Zahlen a_0, a_1, $\cdots$, a_{n-1} ganz rational sind.

Nun sei p eine zu C prime Primzahl. Dann existiert eine ganze rationale Zahl u, für welche die Kongruenz

$$Cu \equiv 1 \mod p$$

erfüllt ist. Wenn dabei für einen Primidealteiler $\mathfrak{p}$ von p aus K die Kongruenz

$$\theta \equiv a \mod \mathfrak{p} \quad (a \text{ ist ganz rational})$$

gilt, dann ist

$$\gamma \equiv \gamma\, Cu \equiv \sum_{i=0}^{n-1} a_i\, u\, \theta^i \equiv \sum_{i=0}^{n-1} a_i\, u a^i \mod \mathfrak{p};$$

d.h. jede ganze algebraische Zahl aus K ist mod $\mathfrak{p}$ stets einer ganzen rationalen Zahl kongruent. Also ist $\mathfrak{p}$ vom Grade 1.

Um also den Satz zu beweisen, genügt zu zeigen, daß es unendlich viele Primideale aus K gibt, nach denen θ stets ganzen rationalen Zahlen kongruent ist, weil C in K nur endlich viele Primidealteiler besitzt.

Nun kann man sich leicht davon überzeugen, daß irgendein Primidealteiler einer Primzahl p aus K dann und nur dann in $\theta - a$ aufgeht, wenn $N_{K/P}(\theta - a)$ durch p teilbar ist, wobei a eine ganze rationale Zahl bezeichnet. Bezeichnet man jetzt die definierende Gleichung von θ mit $f(x) = x^n + \cdots + c_n$, so ist bekanntlich

$$f(a) = (-1)^n\, N_{K/P}(\theta - a);$$

d.h. für irgendeinen Primteiler $\mathfrak{p}$ von p gilt dann und nur dann die Kongruenz

$$\theta \equiv a \mod \mathfrak{p},$$

wenn $f(a)$ durch p teilbar ist. Somit ist der Beweis des Satzes auf den Beweis der folgenden Tatsache reduziert:

Es existieren unendlich viele ganze rationale Zahlen $a_1, a_2, \cdots, a_n, \cdots$ *und die voneinander verschiedenen Primzahlen* $p_1, p_2, \cdots, p_n, \cdots$ *derart, daß die Zahlen* $f(a_1), f(a_2), \cdots, f(a_n), \cdots$ *bzw. durch* $p_1, p_2, \cdots, p_n, \cdots$ *teilbar sind.*

Der Beweis der letzten Tatsache wird aber auf den des folgenden Satzes zurückgeführt:

Es sei $g(x) = a_0 x^n + \cdots + a_n$ $(a_0 \neq 0, n > 0)$ *ein Polynom von* x *mit ganzen rationalen Koeffizienten, und* $q_1, q_2, \cdots, q_s$ *seien beliebig vorgegebene Primzahlen. Dann existiert stets eine solche ganze rationale Zahl* a, *daß* $g(a)$ *mindestens einen von* $q_1, q_2, \cdots, q_s$ *verschiedenen Primteiler besitzt.*

Beweis. Wenn $a_n = 0$ ist, so ist $g(x) = xg_0(x)$, wo $g_0(x)$ ein ganzzahliges Polynom bezeichnet. Da es sicher eine von den $q_1, q_2, \cdots, q_s$ verschiedene Primzahl q gibt, so ist $g(q) = qg_0(q)$ durch q teilbar. Wir wollen also den Fall betrachten, wo $a_n \neq 0$ ist. Zunächst kann man

$$a_n = \varepsilon q_1^{\nu_1} q_2^{\nu_2} \cdots q_s^{\nu_s} b \qquad (b, q_i) = 1, \quad \nu_i \geqq 0 \ (i = 1, 2, \cdots, s)$$

setzen, wo b eine natürliche Zahl ist und $\varepsilon = 1$ oder -1 bezeichnet, je nachdem a_n positiv oder negativ ist. Da

$$\lim_{x \to \infty} \left| a_0 x^{n-1} + \cdots + a_{n-1} \right| \longrightarrow \infty$$

ist, so kann man eine natürliche Zahl M so bestimmen, daß für jede natürliche Zahl $N > M$ stets $|a_0 N^{n-1} + \cdots + a_{n-1}| > 1$ ist. Offenbar kann man die natürlichen Zahlen $\mu_1, \cdots, \mu_s$ so bestimmen, daß μ_i größer ist als $\nu_i \, (i = 1, \cdots, s)$ und $a = q_1^{\mu_1} q_2^{\mu_2} \cdots q_s^{\mu_s} b > M$ ist. Für dieses a gilt:

$$g(a) = q_1^{\nu_1} q_2^{\nu_2} \cdots q_s^{\nu_s} b \, [q_1^{\mu_1 - \nu_1} q_2^{\mu_2 - \nu_2} \cdots q_s^{\mu_s - \nu_s} (a_0 a^{n-1} + \cdots + a_{n-1}) + \varepsilon] \, ;$$

und die in der eckigen Klammer stehende Zahl besitzt offenbar einen von den $q_1, q_2, \cdots, q_s$ verschiedenen Primteiler, w.z.b.w.

Folgerung 1. Ist $\overline{K}$ der kleinste, K enthaltende galoissche Körper über P, so zerfällt in $\overline{K}$ eine Primzahl voll, wenn sie kein Diskriminantenteiler von K/P ist und ein Primideal 1. Grades als einen Primteiler besitzt. Es gibt also unendlich viele Primzahlen, welche in $\overline{K}$, um so mehr in K, *vollzerfallen*.

Folgerung 2. Ist $K = P(e^{\frac{2\pi i}{m}})$ ein Kreisteilungskörper, so zerfällt eine Primzahl p mit $p \nmid m$ dann und nur dann in K voll, wenn die Kongruenz

$$p \equiv 1 \mod m$$

erfüllt ist. Da es unendlich viele Primzahlen gibt, welche in K vollzerfallen, so ist folgender Satz bewiesen:

Es gibt unendlich viele Primzahlen, welche der Kongruenz

$$x \equiv 1 \mod m$$

genügen; d.h. es gibt unendlich viele Primzahlen von der Form

$$mt + 1 \quad (t = 1, 2, \cdots, n, \cdots) \, .$$