Zur Theorie der Kreiskörper.

Von MICHAEL BAUER in Budapest.

Es sei ω eine primitive m-te Einheitswurzel, welche der primitiven Kreisteilungsgleichung $F_m(x)=0$ genügt. Bekanntlich bilden die Zahlen

$$1,\ \omega,\ \omega^2, \ldots, \omega^{\varphi(m)},$$

wo $\varphi(m)$ die bekannte Eulersche Funktion ist, ein Fundamentalsystem der ganzen Zahlen des Körpers $R(\omega)$, welche durch ω bestimmt wird. Ich möchte für diese bekannte Tatsache einen Beweis angeben, den ich schon vor längerer Zeit gefunden habe und der sich wesentlich auf Dedekinds Untersuchungen über außerwesentliche Diskriminantenteiler stützt.

1. Die Wurzel Ω der ganzzahligen irreduziblen Gleichung $F(x)=0$ mit dem höchsten Koeffizienten 1 bestimme den Körper $R(\Omega)$. Ist D die Diskriminante von $F(x)$, so fällt

$$(1) \qquad D=dk^2, \qquad k \text{ rational ganz}$$

aus, wo d die Diskriminante des Körpers $R(\Omega)$ bedeutet. Die Primzahlen $p|k$ werden außerwesentliche Diskriminantenteiler genannt. DEDEKIND[1]) hat die notwendige und hinreichende Bedingung aufgestellt, welche darüber entscheidet, ob p ein außerwesentlicher Teiler ist. Wir brauchen nur den folgenden Teil des Satzes, den DEDEKIND ohne Anwendung der Idealtheorie beweist:

[1]) R. DEDEKIND, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Abhandlungen der Königl. Gesellschaft der Wissenschaften zu Göttingen,* **23** (1878), S. 1—23 = *Gesammelte math. Werke,* Bd. I. (Braunschweig, 1930), S. 202—230.

Ist p ein außerwesentlicher Teiler und gilt die Relation

(2) $$F(x) = P_1(x)^{g_1} \dots P_i(x)^{g_i} \dots P_r(x)^{g_r} + pM(x),$$

wo die $P_i(x)$ (mod p) verschiedene irreduzible Polynome bedeuten, deren höchste Koeffizienten gleich 1 sind, dann ist $M(x)$ (mod p) zumindest durch ein Polynom $P_k(x)$ teilbar, wo $g_k > 1$ ausfällt.

2. Wir müssen beweisen, daß die Diskriminante der Gleichung $F_m(x) = 0$ keinen außerwesentlichen Teiler besitzt. Da im Falle $(m, p) = 1$, $x^m - 1$ (mod p^α) keinen mehrfachen Faktor enthält, so sind die Primzahlen $(p, m) = 1$ keine außerwesentliche Teiler. Es sei nun

(3) $$m = np^\beta, \quad \beta \geqq 1, \quad (n, p) = 1.$$

Da nach SCHÖNEMANN ein (mod p^α) irreduzibles Polynom, dessen höchster Koeffizient gleich 1 ist, (mod p) eine Potenz eines (mod p) irreduziblen Polynoms ist und die Zerlegungen in Primfaktoren (mod p) eindeutig sind, so besitzt $F_n(x)$ eine Zerlegung

(4) $$F_n(x) = S_1(x) \dots S_i(x) \dots S_t(x) \qquad (\text{mod } p^2),$$

wo die $S_i(x)$ *bereits* (mod p) *irreduzibel* und verschieden ausfallen. Aus

$$F_m(x) \equiv F_n(x)^{\varphi(p^\beta)} \qquad (\text{mod } p)$$

folgt

(4*) $$F_m(x) \equiv S_1(x)^{\varphi(p^\beta)} \dots S_i(x)^{\varphi(p^\beta)} \dots S_t(x)^{\varphi(p^\beta)} \qquad (\text{mod } p),$$

also ist

(4**) $$F_m(x) = S_1(x)^{\varphi(p^\beta)} \dots S_i(x)^{\varphi(p^\beta)} \dots S_t(x)^{\varphi(p^\beta)} + pM(x).$$

Nun können wir zeigen, daß die Zahl p kein außerwesentlicher Teiler ist. Im Falle $p = 2$, $\beta = 1$ sind die Exponenten gleich 1. In den übrigen Fällen müßte $M(x)$ (mod p) durch ein gewisses Polynom $S_k(x)$ teilbar sein, $S_k(x)$ wäre also ein gemeinsamer Teiler von $F_m(x)$ und $F_n(x)$ (mod p^2). Das ist aber infolge der bekannten Relation

(5) $$\frac{x^{np^\beta} - 1}{x^{np^{\beta-1}} - 1} = (x^{np^{\beta-1}} - 1)(x^{np^{\beta-1}(p-2)} + 2x^{np^{\beta-1}(p-3)} + \\ + \dots + p - 1) + p$$

ausgeschlossen, womit der Satz bewiesen ist.

3. Ich möchte darauf hinweisen, daß die Zerlegung von $F_m(x)$ (mod p^α) sehr wenig ausgenützt wurde. Bekanntlich läßt sich auf elementare Weise beweisen[2]), daß die Zerlegung von $F_m(x)$ (mod p^α) in irreduzible Faktoren, deren höchste Koeffizienten gleich 1 sind, eindeutig ist. Die Grade und die Exponenten sind aus der Zerlegung von $F_m(x)$ (mod p) ableitbar.

(Eingegangen am 3. November 1937.)

[2]) M. Bauer, Zur Theorie der Fundamentalgleichung, *Journal für Math.*, **149** (1919), S. 89—96, § 2. Der Beweis benutzt nicht die Irreduzibilität von $F_m(x)$.