p-adischer Beweis des zweiten Hauptsatzes von Herrn Ore.

Von Michael Bauer (Budapest) und Nikolaj Tschebotaröw (Kasan).
(Aus einem Briefwechsel zusammengestellt).

Der „zweite Hauptsatz" von Herrn Ö. Ore[1]), der erlaubt, ohne Kenntnis der Minimalbasis die Zerlegung *jeder* Primzahl auf Primidealfaktoren in einem beliebigen algebraischen Zahlkörper zu erledigen, lässt sich sehr elementar mit Hilfe der Theorie p-adischer Zahlen von Herrn K. Hensel[2]) beweisen. Der Beweisgang erfolgt folgendermassen.

1. Es sei

$$(1) \qquad \begin{gathered} f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0, \\ a_i \text{ rat.-ganz } (i = 1, 2, \ldots n),\ f(\omega) = 0 \end{gathered}$$

eine irreduzible Gleichung. Wir wollen eine rationale Primzahl p im Körper $K(\omega)$ in Primidealfaktoren zerlegen.

2. Zunächst wird $f(x)$ in p-adische irreduzible Faktoren zerlegt und so bekommt man die höchsten Primidealpotenzen. Ist $\Phi(x)$ ein p-adischer irreduzibler Faktor und

$$(2) \qquad \Phi(x) = x^m + c_1 x^{m-1} + \ldots + c_m \ (p),$$

dann ist

$$(3) \qquad p = \mathfrak{p}^g . \mathfrak{Q},\ (\mathfrak{p}, \mathfrak{Q}) = 1,$$

$$(4) \qquad f \text{ Grad von } \mathfrak{p},\ m = fg.$$

Der Faktor $\Phi(x)$ kann auch durch ein gewöhnliches Polynom ersetzt werden, das $\equiv \Phi \pmod{p^\alpha}$ ist, α genügend gross. Wir können demnach m durch eine endliche Anzahl von Operationen ermitteln.

[1]) Ö. Ore, Über den Zusammenhang zwischen u. s. w. II, *Math. Ann.* **97**, S. 585, Satz 9.

[2]) K. Hensel, Die Theorie der algebraischen Zahlen, Leipzig, 1908.

3. Es ist bekannt, dass das Polynom $\Phi(x)$ im Körper (p^f-1)-ter Einheitswurzeln in irreduzible Faktoren g-ten Grades zerfällt. Es kann andererseits bei keiner Adjunktion weiter zerfallen, wenn im erweiterten Rationalitätsbereich p nicht kritisch ist. Denn p enthält den Primidealfaktor in der g-ten Potenz (oder in Hensel-schen Bezeichnungen: $\pi^g \sim p$). Wenn wir daher zu $K(p)$ einen Oberkörper von $K(p, \alpha)$, $(\alpha^{p^f-1}-1=0)$ adjungieren, dessen Diskriminante relativ prim zu p ist, so zerfällt $\Phi(x)$ in irreduzible Polynome vom genau g-ten Grade. Der Körper $K(p, \beta)$, $(\beta^{p^m-1}-1=0)$ genügt aber diesen Bedingungen. Um also g zu finden, genügt es den Grad von Teilern des Polynoms $\Phi(x)$ zu bestimmen, die im Körper $K(p, \beta)$ irreduzibel sind, wobei β eine primitive (p^m-1)-te Einheitswurzel ist. Dies kann man auch durch eine endliche Anzahl von Operationen ermitteln.

(Eingegangen am 21. Juni 1928)