Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern.

(Erste Mitteilung.)

Von

Öystein Ore in Oslo.

In den Untersuchungen über den Zusammenhang zwischen der Theorie der Ideale und den höheren Kongruenzen hat Dedekind versucht, die Verbindung zwischen den Idealeigenschaften und den Eigenschaften der definierenden Gleichung eines Körpers zu bestimmen. Seine Untersuchungen sind aber auf Gleichungen von spezieller Form beschränkt und auch für diese erhalten seine Resultate nicht die notwendige Allgemeinheit, indem die sogenannten gemeinsamen außerwesentlichen Diskriminantenteiler auftreten. Bei seinen Untersuchungen über die Verzweigungstheorie der algebraischen Körper wird der Diskriminantensatz unter gleichzeitiger Heranziehung von mehreren erzeugenden Gleichungen erreicht.

Die Kroneckersche Theorie der Ideale mit der Einführung von unabhängigen Variablen als Hilfsgrößen leistet für die Verzweigungstheorie nicht mehr als die Dedekindsche, und man kann daraus auch keine Schlüsse auf die Eigenschaften der definierenden Gleichungen ziehen.

Bei der Henselschen Theorie der Ideale wird der Körper durch p-adische und π-adische Zahlen erweitert, und man erhält in diesem erweiterten Körper durch den Henselschen Hauptsatz direkt einen Zusammenhang zwischen der Primidealzerlegung einer Primzahl und der Zerlegung der definierenden Gleichung im p-adischen Bereiche.

In dieser Arbeit werde ich zeigen, wie man in voller Allgemeinheit den Dedekindschen Gedankengang durchführen kann und wie man sehr natürlich unter Anwendung der Theorie der Primzahlpotenzmoduln für eine feste endliche Potenz p^a und ohne Adjunktion von Hilfsgrößen diese Probleme behandeln und lösen kann. Speziell gebe ich eine neue und aus-

nahmslose Behandlung der Verzweigungstheorie bei den algebraischen Körpern.

Diese Untersuchungen beruhen auf dem folgenden Hauptsatz, der dem Henselschen analog ist:

Wird der Körper durch die irreduzible Gleichung $f(x) = 0$ definiert, und besteht für $f(x)$ die Zerlegung in irreduzible Faktoren $(\mathrm{mod}\, p^\alpha)$, $\alpha > \delta + 1$,

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x) (\mathrm{mod}\, p^\alpha),$$

wobei der Grad von $f_i(x)$ gleich n_i ist, so hat die Primzahl p die Primidealzerlegung

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}, \qquad N\mathfrak{p}_i^{e_i} = p^{n_i}.$$

Die Diskriminante von $f(x)$ ist genau durch p^δ teilbar.

Von diesem Satz ausgehend, behandle ich zunächst die Eigenschaften des Führers; und durch Einführung von neuen Führerbegriffen (Partialführern in bezug auf Primzahlen und Primideale) wird gezeigt, wie sich der Führer zerlegt; es wird auch gezeigt, wie man für die definierende Gleichung eine Normalform angeben kann, wobei alle Partialführer der Primideale gleich Eins werden. Weiter führe ich die Abbildungskörper für die Primideale ein und studiere damit u. a. die Eigenschaften des Index; es ergibt sich daraus eine neue Formel für die Zusammensetzung des Index.

Dann werden die Eigenschaften der Körperdifferente und Körperdiskriminante behandelt und gezeigt, wie man durch Einführung der Supplementzahlen diese Größen ohne Ausnahme bestimmen kann. Die Dedekind-Henselsche Ungleichung für die Differentenexponenten wird unter Anwendung eines einfachen Hilfssatzes in ein paar Zeilen bewiesen; durch diesen Hilfssatz erhält man auch den Lückensatz für die Supplementzahlen, wodurch der sonst übliche Ausnahmefall vollständig erledigt wird. Zuletzt gebe ich einige Existenzsätze für algebraische Körper mit vorgeschriebenen Idealzerlegungen und Differentenexponenten, insofern sie nach den obigen Sätzen mit der Primidealzerlegung verträglich sind; diese Sätze sind auch für mehrere andere Untersuchungen von Bedeutung. Es wird auch hier die genaue obere Grenze der Multiplizität angegeben, womit eine Primzahl in der Diskriminante eines Körpers n-ten Grades aufgehen kann. Ich mache speziell darauf aufmerksam, daß es unterhalb dieser Grenze Lückenzahlen gibt, welche nicht als Diskriminantenexponenten vorkommen können.

Kapitel I.

Einige Sätze über höhere Kongruenzen für Primzahlpotenzmoduln.

§ 1.

Ein Hilfssatz.

Die hier gegebene Behandlung der Theorie der algebraischen Zahlen beruht auf der Theorie der höheren Kongruenzen für Primzahlpotenzmoduln, und ich werde daher in diesem Kapitel die notwendigen Theoreme aus diesem Gebiet aufstellen.

Bekanntlich hat die Theorie der höheren Kongruenzen für Primzahlpotenzmoduln nicht denselben einfachen Charakter wie für Primzahlmoduln, und namentlich gilt nicht mehr der Satz von der eindeutigen Zerlegung der Polynome in irreduzible Faktoren. Wie ich aber in Kapitel 2 zeige, wird dieser Satz durch einen anderen Hauptsatz ersetzt.

Es soll zunächst ein wichtiger Hilfssatz entwickelt werden.

Es seien

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n,$$
$$g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$$

zwei Polynome, wobei hier, wie sonst immer unter Polynom eine ganze rationale Funktion mit ganzen rationalen Koeffizienten verstanden wird.

Weiter sei

$$R = R(f(x), g(x))$$

die Resultante von $f(x)$ und $g(x)$, wobei R eine ganze rationale Zahl ist. Es wird $R \neq 0$ angenommen, so daß die Polynome $f(x)$ und $g(x)$ keinen gemeinsamen Faktor haben.

Mit p soll immer eine rationale Primzahl bezeichnet werden. Es sei p^ϱ die genaue Potenz, worin p in der Resultante R aufgeht.

Wenn dann $F(x)$ ein beliebiges Polynom vom Grade kleiner als $n + m$ ist, also

$$F(x) = c_0 x^{n+m-1} + c_1 x^{n+m-2} + \ldots + c_{n+m-1},$$

so soll bewiesen werden, daß man immer solche Polynome $f_1(x)$ und $g_1(x)$ bestimmen kann, daß

$$(1) \qquad f(x) g_1(x) + g(x) f_1(x) \equiv p^\varrho F(x) \pmod{p^\alpha}$$

ist, wo $\alpha > \varrho$ eine beliebige ganze rationale Zahl ist und wo weiter die Grade von $f_1(x)$ und $g_1(x)$ kleiner als n bzw. m sind, also

$$f_1(x) = A_0 x^{n-1} + A_1 x^{n-2} + \ldots + A_{n-1}$$
$$g_1(x) = B_0 x^{m-1} + B_1 x^{m-2} + \ldots + B_{m-1}.$$

Die Richtigkeit dieser Behauptung beweist man leicht, indem man in (1) die Produkte ausmultipliziert und die Koeffizienten der entsprechenden Potenzen von x vergleicht. Man erhält so das System von linearen Kongruenzen

$$(2) \qquad \left.\begin{array}{l} a_0 B_0 + \qquad\qquad b_0 A_0 \qquad\qquad \equiv p^\varrho c_0 \\ a_1 B_0 + a_0 B_1 + b_1 A_0 + b_0 A_1 \equiv p^\varrho c_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \end{array}\right\} (\mathrm{mod}\ p^\alpha),$$

und man sieht leicht, daß die Determinante dieses Systems gleich R ist. Durch passende Multiplikation mit Unterdeterminanten erhält man aus (2) Kongruenzen von der Form

$$R A_i \equiv p^\varrho K_i (\mathrm{mod}\ p^\alpha) \qquad (i = 0, 1, \ldots n-1),$$
$$R B_i \equiv p^\varrho H_i (\mathrm{mod}\ p^\alpha) \qquad (i = 0, 1, \ldots m-1),$$

wo K_i und H_i ganze rationale Zahlen sind, welche als lineare Ausdrücke in den Koeffizienten c_i dargestellt werden können. Setzt man nun $R = p^\varrho R'$, wobei R' also nicht durch p teilbar ist, kommt

$$A_i \equiv R'' K_i (\mathrm{mod}\ p^{\alpha-\varrho}),$$
$$B_i \equiv R'' H_i (\mathrm{mod}\ p^{\alpha-\varrho}),$$

wobei

$$R' R'' \equiv 1 (\mathrm{mod}\ p^{\alpha-\varrho})$$

ist. Umgekehrt folgt leicht, daß diese Werte von A_i und B_i eine Relation von der Form (1) geben.

Wie man auch bemerkt, sind die Koeffizienten A_i und $B_i (\mathrm{mod}\ p^{\alpha-\varrho})$ eindeutig bestimmt und wenn daher $f_2(x)$ und $g_2(x)$ zwei andere Polynome sind, wofür die Gradzahlen kleiner als n, bzw. m sind, und weiter die Kongruenz

$$f(x) g_2(x) + g(x) f_2(x) \equiv p^\varrho F(x) (\mathrm{mod}\ p^\alpha)$$

besteht, so hat man notwendigerweise

$$f_1(x) \equiv f_2(x), \quad g_1(x) \equiv g_2(x) (\mathrm{mod}\ p^{\alpha-\varrho}).$$

Diese Resultate können folgendermaßen ausgesprochen werden:

Satz 1. *Wenn die Resultante der Polynome $f(x)$ und $g(x)$ genau durch p^ϱ teilbar ist und weiter $F(x)$ ein gegebenes Polynom vom Grade kleiner als $n+m$ bezeichnet, kann man immer Polynome $f_1(x)$ und $g_1(x)$ mit Gradzahlen kleiner als n und m so bestimmen, daß*

$$f(x) g_1(x) + g(x) f_1(x) \equiv p^\varrho F(x) (\mathrm{mod}\ p^\alpha),$$

und die Polynome $f_1(x)$ und $g_1(x)$ sind dann $(\mathrm{mod}\ p^{\alpha-\varrho})$ eindeutig bestimmt.

§ 2.

Faktoren der Polynome (mod p^α).

Ein Polynom $\varphi(x)$ heißt *Teiler* von einem Polynome $f(x)$ (mod p^α), wenn eine Kongruenz

$$f(x) \equiv \varphi(x)\,\varphi_1(x) \pmod{p^\alpha}$$

besteht.

Ein Polynom soll *reduziert* heißen, wenn der Koeffizient der höchsten Potenz von x nicht durch p teilbar ist. Im allgemeinen kann man dann annehmen, daß dieser Koeffizient gleich eins ist.

Im folgenden werden auch nicht-reduzierte Polynome vorkommen, wie ich aber zeige, kann man für solche Polynome einfach eine Normalform (mod p^α) angeben. Es gilt nämlich der Satz:

Satz 2. *Es seien in*

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-r-1} x^{r+1} + a_{n-r} x^r + \ldots + a_n$$

alle Koeffizienten $a_0, a_1, \ldots, a_{n-r-1}$ *durch* p *teilbar, während* a_{n-r} *nicht durch* p *teilbar ist. Es besteht dann eine Zerlegung*

$$f(x) \equiv g(x)\,(A + p\,h(x)) \pmod{p^\alpha},$$

wobei $g(x)$ *ein reduziertes Polynom vom Grade* r *ist,* $h(x)$ *ist ein Polynom und* A *bezeichnet eine durch* p *nicht teilbare Konstante, und weiter ist diese Zerlegung* (mod p^α) *nur in einer Weise ausführbar.*

Dieser Satz ist schon von Schönemann[1]) bewiesen, ich gebe aber hier einen anderen Beweis.

Es besteht die Kongruenz

$$f(x) \equiv a_{n-r}(x^r + b_1 x^{r-1} + \ldots + b_r) = a_{n-r}\,g^{(1)}(x), \pmod{p},$$

wenn nur die Zahlen b_i so gewählt sind, daß

$$b_i a_{n-r} \equiv a_{n-r+i} \pmod{p}$$

ist, was offenbar immer möglich ist. Daraus folgt, daß man $A = a_{n-r}$ setzen kann.

Der Satz wird jetzt durch vollständige Induktion bewiesen. Es bestehe die Kongruenz

$$f(x) \equiv g^{(\alpha-1)}(x)\,(A + p\,h^{(\alpha-1)}(x)) \pmod{p^{\alpha-1}}$$

und nach der Voraussetzung über die Eindeutigkeit kann man dann

$$g^{(\alpha)}(x) = g^{(\alpha-1)}(x) + p^{\alpha-1} G(x),$$

$$A + p\,h^{(\alpha)}(x) = A + p\,h^{(\alpha-1)}(x) + p^{\alpha-1} H(x)$$

[1]) Th. Schönemann, Von denjenigen Moduln, welche Potenzen von Primzahlen sind, Journ. für Math. **32** (1846), S. 93—105, § 54.

annehmen. Die Zusatzpolynome $G(x)$ und $H(x)$ werden dadurch bestimmt, daß die Relation

$$f(x) \equiv (g^{(\alpha-1)}(x) + p^{\alpha-1} G(x))(A + p h^{(\alpha-1)}(x) + p^{\alpha-1} H(x)) \pmod{p^\alpha}$$

bestehen muß. Daraus folgt

$$f(x) - g^{(\alpha-1)}(x)(A + p h^{(\alpha-1)}(x)) \equiv p^{\alpha-1}(H(x) g^{(\alpha-1)}(x) + A G(x)) \pmod{p^\alpha}$$

oder wenn man

$$f(x) - g^{(\alpha-1)}(x)(A + p h^{(\alpha-1)}(x)) = p^{\alpha-1} F(x)$$

setzt, erhält man zur Bestimmung von $G(x)$ und $H(x)$

$$F(x) \equiv H(x) g^{(\alpha-1)}(x) + A G(x) \pmod{p}.$$

Diese Kongruenz kann aber nur $(\mathrm{mod}\ p)$ in einer eindeutigen Weise befriedigt werden, und zwar indem man $F(x)$ durch $g^{(\alpha-1)}(x)$ dividiert,

$$F(x) = q(x) g^{(\alpha-1)}(x) + r(x),$$

wobei also

$$H(x) \equiv q(x), \qquad A G(x) \equiv r(x) \pmod{p}$$

wird. Der Satz 2 ist dadurch bewiesen.

Es sei jetzt $f(x)$ ein reduziertes Polynom und weiter

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x) \pmod{p^\alpha}$$

eine beliebige Zerlegung von $f(x)$ in Faktoren $(\mathrm{mod}\ p^\alpha)$. Man kann dann nach Satz 2 immer annehmen, daß ein Faktor $f_i(x)$ die Form

$$f_i(x) \equiv g_i(x)(A_i + p h_i(x)) \pmod{p^\alpha}$$

hat, wobei $g_i(x)$ reduziert ist und die Konstante A_i soll nicht durch p teilbar sein. Das Produkt

$$G(x) = g_1(x) g_2(x) \dots g_r(x)$$

ist dann wieder reduziert, und weiter kann man auch

$$A + p H(x) = (A_1 + p h_1(x)) \dots (A_r + p h_r(x)) \tag{3}$$

setzen, wobei A nicht durch p teilbar ist. Aus der Kongruenz

$$f(x) \equiv G(x)(A + p H(x)) \pmod{p^\alpha}$$

schließt man aber

$$A + p H(x) \equiv 1 \pmod{p^\alpha}. \tag{4}$$

Denn der Grad von $G(x)$ ist, wie man leicht sieht, gleich dem Grade von $f(x)$, und wenn es in $p H(x)$ Glieder gäbe, welche nicht $(\mathrm{mod}\ p^\alpha)$ verschwinden, würden daraus durch Multiplikation mit $G(x)$ Glieder entstehen, welche nicht in $f(x)$ enthalten wären. Die Richtigkeit von (4) ist also nachgewiesen.

Aus (3) folgt dann

$$(A_1 + p\,h_1(x)) \ldots (A_r + p\,h_r(x)) \equiv 1 \pmod{p^\alpha},$$

und daraus leitet man sofort den Satz ab:

Satz 3. *Wenn ein reduziertes Polynom* $(\mathrm{mod}\ p^\alpha)$ *durch ein Polynom von der Form* $A + p\,F(x)$ *teilbar ist, gibt es immer ein anderes Polynom* $B + p\,G(x)$, *so daß*

$$(A + p\,F(x))\,(B + p\,G(x)) \equiv 1 \pmod{p^\alpha}.$$

Solche Polynome $A + p\,F(x)$ kann man passend *Einheitsteiler* $(\mathrm{mod}\ p^\alpha)$ nennen. Man erkennt leicht an Beispielen, daß solche Einheitsteiler für alle α existieren. So ist z. B.

$$1 + x^m\,p^\beta, \qquad \beta \geqq \frac{\alpha}{2}$$

ein Einheitsteiler $(\mathrm{mod}\ p^\alpha)$, indem

$$(1 + x^m\,p^\beta)\,(1 - x^m\,p^\beta) \equiv 1 \pmod{p^\alpha}.$$

Ein Polynom $\varphi(x)$ soll *irreduzibel* $(\mathrm{mod}\ p^\alpha)$ heißen, wenn $\varphi(x)$ reduziert ist und außer sich selbst keine reduzierte Teiler $(\mathrm{mod}\ p^\alpha)$ enthält. Aus dem Vorausgehenden folgt einfach, daß jedes reduzierte Polynom in irreduzible Faktoren zerlegt werden kann, ich bemerke aber sofort, daß diese Zerlegung im allgemeinen nicht eindeutig bestimmt ist.

Von den unwesentlichen Einheitsteilern wird im folgenden bei der Zerlegung eines reduzierten Polynoms immer abgesehen.

§ 3.

Über den Zusammenhang zwischen den Faktoren $(\mathrm{mod}\ p^\alpha)$ für verschiedene α.

Für die weitere Untersuchung der Zerlegungen der Polynome ist ein Satz, der in anderer Gestalt bereits von Herrn Hensel[2]) aufgestellt ist, von Wichtigkeit.

Es sei $f(x)$ ein gegebenes, reduziertes Polynom, und weiter $D = D(f(x))$ die Diskriminante von $f(x)$. Es wird $D \neq 0$ vorausgesetzt, d. h. $f(x)$ soll keine mehrfachen Faktoren enthalten; man setzt voraus, daß D genau durch p^δ teilbar ist.

Weiter wird angenommen, daß eine Zerlegung

$$f(x) \equiv f_1(x)\,f_2(x) \pmod{p^{\delta+1}} \tag{5}$$

besteht, wobei also $f_1(x)$ und $f_2(x)$ reduziert angenommen werden. Wenn

[2]) K. Hensel, Theorie der algebraischen Zahlen, Kap. IV, § 3. Leipzig 1908.

dann die Resultante $R(f_1(x), f_2(x))$ genau durch p^ϱ teilbar ist, so folgt aus der Relation

$$D \equiv D(f_1(x))\, D(f_2(x))\, R^2(f_1(x), f_2(x)) \pmod{p^{\delta+1}}$$

sofort, daß $\delta \geqq 2\varrho$ sein muß[3]).

Man kann nun beweisen, daß man aus der Zerlegung (5) für alle $\alpha > \delta + 1$ eine Zerlegung

$$f(x) \equiv f_1^{(\alpha)}(x)\, f_2^{(\alpha)}(x) \pmod{p^\alpha} \tag{6}$$

ableiten kann, wobei

$$f_1^{(\alpha)}(x) \equiv f_1(x), \qquad f_2^{(\alpha)}(x) \equiv f_2(x) \pmod{p^{\delta-\varrho+1}} \tag{7}$$

ist.

Man beweist auch diesen Satz durch Induktion, indem man

$$f(x) \equiv f_1^{(\alpha-1)}(x)\, f_2^{(\alpha-1)}(x) \pmod{p^{\alpha-1}} \tag{8}$$

als bewiesen voraussetzt, wobei also auch

$$f_1^{(\alpha-1)}(x) \equiv f_1(x), \qquad f_2^{(\alpha-1)}(x) \equiv f_2(x) \pmod{p^{\delta-\varrho+1}} \tag{9}$$

sein soll. Da, wie schon bemerkt, $\delta - \varrho \geqq \varrho$ ist, so wird auch die Resultante von $f_1^{(\alpha-1)}(x)$ und $f_2^{(\alpha-1)}(x)$ genau durch p^ϱ teilbar.

Setzt man jetzt

$$f_1^{(\alpha)}(x) = f_1^{(\alpha-1)}(x) + p^{\alpha-1-\varrho} g_1(x),$$
$$f_2^{(\alpha)}(x) = f_2^{(\alpha-1)}(x) + p^{\alpha-1-\varrho} g_2(x),$$

so sind wegen (9) sicher die Kongruenzen (7) erfüllt. Weiter kann man aber die Zusatzfunktionen $g_1(x)$ und $g_2(x)$ so bestimmen, daß auch die Zerlegung (6) besteht. Dazu ist nur erforderlich, daß die Kongruenz

$$f(x) \equiv f_1^{(\alpha-1)}(x)\, f_2^{(\alpha-1)}(x) + p^{\alpha-1-\varrho}(g_1(x)\, f_2^{(\alpha-1)}(x) + g_2(x)\, f_1^{(\alpha-1)}(x)) \pmod{p^\alpha}$$

besteht, indem man bemerkt, daß das Glied

$$p^{2\alpha-2-2\varrho}\, g_1(x)\, g_2(x)$$

$(\mathrm{mod}\, p^\alpha)$ verschwindet. Nach (8) kann man aber

$$p^{\alpha-1} F(x) = f(x) - f_1^{(\alpha-1)}(x)\, f_2^{(\alpha-1)}(x)$$

setzen, so daß man zur Bestimmung von $g_1(x)$ und $g_2(x)$ die Kongruenz

$$g_1(x)\, f_2^{(\alpha-1)}(x) + g_2(x)\, f_1^{(\alpha-1)}(x) \equiv p^\varrho F(x) \pmod{p^{\varrho+1}}$$

erhält. Diese Kongruenz ist aber nach Satz 1 immer lösbar, wodurch unsere Behauptung bewiesen ist.

---

[3]) Es ist von Interesse zu bemerken, daß diese Relation nicht zu bestehen braucht, wenn man *nicht-reduzierte* Faktoren $(\mathrm{mod}\, p^\alpha)$ zuläßt.

Es sei nun

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x) \pmod{p^{\delta+1}} \tag{10}$$

eine beliebige Zerlegung von $f(x)$ in reduzierte Faktoren. Es wird vorausgesetzt, daß die Diskriminante $D(f_i(x))$ eines Faktors genau durch p^{δ_i} teilbar ist, während die Resultante $R_{ij} = R(f_i(x), f_j(x))$ genau durch $p^{\varrho_{ij}}$ teilbar sein soll. Nach einem bekannten Satze über Diskriminanten folgt dann aus (10)

$$\delta = \sum_{i=1}^{r} \delta_i + 2 \sum_{i>j} \varrho_{ij}. \tag{11}$$

Setzt man hier der Kürze wegen

$$\varrho' = \sum_{i>j} \varrho_{ij}, \tag{12}$$

so geht die Gleichung (11) in

$$\delta = \sum_{i=1}^{r} \delta_i + 2\varrho' \tag{13}$$

über.

Unter Anwendung der vorstehenden Untersuchungen folgt dann die Richtigkeit des Satzes:

Besteht für $f(x)$ die Zerlegung (10), so besteht auch für alle $\alpha > \delta + 1$ eine entsprechende Zerlegung

$$f(x) \equiv f_1^{(\alpha)}(x) f_2^{(\alpha)}(x) \dots f_2^{(\alpha)}(x) \pmod{p^\alpha}, \tag{14}$$

wobei allgemein

$$f_i^{(\alpha)}(x) \equiv f_i(x) \pmod{p^{\delta-\varrho'+1}} \qquad (i = 1, 2, \dots, r).$$

Man leitet auch mittels dieser Untersuchungen einfach als Spezialfall den Satz von Schönemann[4]) ab:

Besteht die Zerlegung

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x) \pmod{p},$$

wobei die Faktoren $f_i(x) \pmod{p}$ alle zueinander relativ prim sind, so besteht für alle α eine Zerlegung

$$f(x) \equiv f_1^{(\alpha)}(x) f_2^{(\alpha)}(x) \dots f_r^{(\alpha)}(x) \pmod{p^\alpha},$$

wobei

$$f_i^{(\alpha)}(x) \equiv f_i(x) \pmod{p} \qquad (i = 1, 2, \dots, r).$$

Unter Anwendung dieser Sätze werde ich nun die Zerlegung eines Polynoms in irreduzible Faktoren $(\mathrm{mod}\, p^\alpha)$ untersuchen. §12.

Aus dem Schönemannschen Satze schließt man sofort, daß eine irreduzible Funktion $(\mathrm{mod}\, p^\alpha)$ entweder kongruent einer Primfunktion $(\mathrm{mod}\, p)$

[4]) Th. Schönemann, a. a. O. § 59.

oder kongruent einer Potenz einer Primfunktion $(\mathrm{mod}\, p)$ ist. Wenn die irreduzible Funktion $(\mathrm{mod}\, p^\alpha)$ nämlich verschiedene Primfunktionen $(\mathrm{mod}\, p)$ enthielte, so würde sie auch $(\mathrm{mod}\, p^\alpha)$ reduzibel.

Es sei jetzt (10) eine Zerlegung von $f(x)$ in irreduzible Funktionen, d. h. die Faktoren $f_i(x)$ sollen alle $(\mathrm{mod}\, p^{\delta+1})$ irreduzibel sein. Die irreduziblen Funktionen $f_i(x)$ müssen dann alle voneinander verschieden sein, da sonst die Diskriminante von $f(x)$ nicht genau durch p^δ teilbar sein kann.

Aus einer irreduziblen Funktion $f_i(x)\,(\mathrm{mod}\, p^{\delta+1})$ erhält man einen entsprechenden Faktor $f_i^{(\alpha)}(x)$ in der Zerlegung (14) von $f(x)\,(\mathrm{mod}\, p^\alpha)$. Man kann dann zeigen, daß auch $f_i^{(\alpha)}(x)$ eine irreduzible Funktion $(\mathrm{mod}\, p^\alpha)$ ist, d. h. die Zerlegung (14) ist eine Zerlegung von $f(x)$ in irreduzible Faktoren $(\mathrm{mod}\, p^\alpha)$.

Man hat nämlich bewiesen, daß

$$f_i^{(\alpha)}(x) \equiv f_i(x)\,(\mathrm{mod}\, p^{\delta-\varrho'+1})$$

ist. Nach (11) und (12) ist aber

$$\delta_i \leqq \delta - \varrho',$$

so daß auch die Kongruenz

$$f_i^{(\alpha)}(x) \equiv f_i(x)\,(\mathrm{mod}\, p^{\delta_i+1})$$

besteht. Daraus folgt aber, daß $f_i^{(\alpha)}(x)\,(\mathrm{mod}\, p^{\delta_i+1})$ irreduzibel sein muß, und also ist $f_i^{(\alpha)}(x)$ um so mehr $(\mathrm{mod}\, p^\alpha)$ eine irreduzible Funktion. Das Polynom $f_i(x)$ muß nämlich $(\mathrm{mod}\, p^{\delta_i+1})$ irreduzibel sein, da sonst $f_i(x)$ nach dem früher Bewiesenen für alle höheren Potenzen von p, also auch $(\mathrm{mod}\, p^{\delta+1})$ reduzibel wäre, gegen die Voraussetzung.

Man kann diese Resultate in einem Satze zusammenfassen:

Satz 4. *Zerlegt man das Polynom $f(x)$ in irreduzible Faktoren* $(\mathrm{mod}\, p^{\delta+1})$

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x)\,(\mathrm{mod}\, p^{\delta+1}),$$

so besteht für alle $\alpha > \delta + 1$ eine entsprechende Zerlegung in irreduzible Faktoren $(\mathrm{mod}\, p^\alpha)$

$$f(x) \equiv f_1^{(\alpha)}(x) f_2^{(\alpha)}(x) \dots f_r^{(\alpha)}(x)\,(\mathrm{mod}\, p^\alpha),$$

wobei

$$f_i^{(\alpha)}(x) \equiv f_i(x)\,(\mathrm{mod}\, p^{\delta-\varrho'+1}) \qquad (i = 1, 2, \dots, r).$$

Aus diesem Satze folgt, daß die Zahlen δ_i und ϱ_{ij} für die entsprechenden Faktoren $f_i^{(\alpha)}(x)$ dieselben wie für $f_i(x)$ sein werden, sie sind also von α unabhängig.

In dem nächsten Kapitel werde ich als Anwendung der Untersuchungen

über algebraische Zahlen auch einen Hauptsatz über die Mehrdeutigkeitsverhältnisse bei den Zerlegungen $(\mathrm{mod}\, p^a)$ geben.

Kapitel II.

Allgemeine Untersuchungen über algebraische Zahlkörper.

§ 1.

Zwei Hilfssätze.

Es sollen jetzt die Eigenschaften eines algebraischen Zahlkörpers K vom Grade n untersucht werden. Der Körper K wird durch eine ganze algebraische Zahl ϑ definiert, wobei ϑ der irreduziblen Gleichung

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0, \quad f(\vartheta) = 0 \tag{1}$$

genügt, worin die Koeffizienten a_i ganze rationale Zahlen sind.

Alle Zahlen in K werden durch die Zahlen

$$F(\vartheta) = c_0 + c_1 \vartheta + \ldots + c_{n-1} \vartheta^{n-1} \tag{2}$$

erzeugt, wenn die c_i alle rationalen Werte durchlaufen. Für K kann man bekanntlich auch eine *Minimalbasis*

$$\omega_1, \omega_2, \ldots, \omega_n \tag{3}$$

finden, so daß jede Zahl ω in K in der Form

$$\omega = b_1 \omega_1 + b_2 \omega_2 + \ldots + b_n \omega_n$$

dargestellt werden kann, und wenn ω eine ganze Zahl des Körpers ist, so sind alle b_i ganze rationale Zahlen. Die Diskriminante einer Minimalbasis heißt die *Körperdiskriminante* und soll mit d bezeichnet werden.

Alle Zahlen von der Form (2), wobei die Koeffizienten c_i ganz rational sind, bilden einen *Ring* R, d. h. die Summe und Differenz $F_1(\vartheta) \pm F_2(\vartheta)$ und Produkt $F_1(\vartheta) F_2(\vartheta)$ von zwei Zahlen in R ist wieder in R enthalten.

Es soll zunächst ein einfacher Hilfssatz bewiesen werden. Aus den Eigenschaften der Minimalbasis (3) folgt, daß Gleichungen von der Form

$$\left\{\begin{aligned} 1 &= c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1n}\omega_n, \\ \vartheta &= c_{21}\omega_1 + c_{22}\omega_2 + \ldots + c_{2n}\omega_n, \\ &\cdots\cdots\cdots\cdots\cdots \\ \vartheta^{n-1} &= c_{n1}\omega_1 + c_{n2}\omega_2 + \ldots + c_{nn}\omega_n \end{aligned}\right. \tag{4}$$

bestehen müssen, wobei alle c_{ij} ganz rational sind. Die Determinante

$$k = |c_{ij}| \qquad (i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, n)$$

heißt der *Index* der Zahl ϑ. Wenn D die Diskriminante der Gleichung (1) ist, so beweist man leicht aus (4), daß die Relation

$$D = k^2 d \tag{5}$$

besteht; es folgt daraus, daß die ganze rationale Zahl k nicht verschwinden kann.

Aus den Gleichungen (4) folgen Relationen von der Form

$$k\omega_i = A_{i0} + A_{i1}\vartheta + \ldots + A_{i,n-1}\vartheta^{n-1} \quad (i = 1, 2, \ldots n), \tag{6}$$

wobei auch alle A_{ij} ganz rational sind.

Es sei jetzt der Index k genau durch $p^\varkappa$ teilbar, so daß man $k = p^\varkappa k'$ setzen kann, wo k' nicht durch p teilbar ist; der Buchstabe $\varkappa$ soll im folgenden immer diese feste Bedeutung haben. Wenn daher $\alpha > \varkappa$ eine ganze rationale Zahl ist, so folgt aus (6) leicht, daß die Zahlen $p^\varkappa \omega_i \pmod{p^\alpha}$ alle kongruent einer Zahl des Ringes R sind. Daraus sieht man sofort die Richtigkeit des folgenden Satzes ein.

Satz 1. *Wenn ω eine beliebige ganze Körperzahl ist, so ist immer $p^\varkappa \omega \pmod{p^\alpha}$ $\alpha > \varkappa$, kongruent einer Zahl des Ringes R. Dabei kann α beliebig groß gewählt werden, und $p^\varkappa$ bezeichnet die genaue Potenz, worin p in k aufgeht.*

Ich beweise auch an dieser Stelle einen anderen wichtigen Hilfssatz. Es soll untersucht werden, wann eine Ringzahl in R durch p^α teilbar ist, also die Bedingung dafür, daß eine Kongruenz von der Form

$$F(\vartheta) = b_0 + b_1\vartheta + \ldots + b_{n-1}\vartheta^{n-1} \equiv 0 \pmod{p^\alpha}$$

besteht. Man ersetzt die Potenzen ϑ^r durch ihre Werte (4) und erhält dadurch die Kongruenzen

$$\left.\begin{aligned} b_0 c_{11} + b_1 c_{21} + \ldots + b_{n-1} c_{n1} &\equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ b_0 c_{1n} + b_1 c_{2n} + \ldots + b_{n-1} c_{nn} &\equiv 0 \end{aligned}\right\} \pmod{p^\alpha}.$$

Die Determinante dieses Systems ist gleich k und man leitet daher daraus die Kongruenzen

$$k b_i \equiv 0 \pmod{p^\alpha} \qquad (i = 0, 1, \ldots, n-1)$$

ab. Dann wird aber

$$b_i \equiv 0 \pmod{p^{\alpha-\varkappa}} \qquad (i = 0, 1, \ldots, n-1),$$

und es ist also bewiesen:

Satz 2. *Wenn eine Ringzahl $F(\vartheta)$ durch p^α teilbar sein soll, müssen alle Koeffizienten b_i durch $p^{\alpha-\varkappa}$ teilbar sein, d. h. es besteht die identische Kongruenz*

$$F(x) \equiv 0 \pmod{p^{\alpha-\varkappa}}.$$

Aus diesem Satze folgt sofort, daß für zwei Ringzahlen $F_1(\vartheta)$ und $F_2(\vartheta)$ die Kongruenz

$$F_1(\vartheta) \equiv F_2(\vartheta) \pmod{p^\alpha}$$

nur dann bestehen kann, wenn

$$F_1(x) \equiv F_2(x) \pmod{p^{\alpha-\varkappa}}.$$

§ 2.

Beweis des Hauptsatzes.

Es soll nun die erste Hauptaufgabe behandelt werden: Man soll den Zusammenhang zwischen der Form des Polynoms $f(x)$ und der Primidealzerlegung einer Primzahl p untersuchen.

Es sei

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x) \pmod{p^\alpha} \tag{7}$$

eine Zerlegung von $f(x)$ in irreduzible Faktoren $(\mathrm{mod}\, p^\alpha)$, wobei $\alpha \geqq \delta + 1$ vorausgesetzt wird, wenn wie früher die Gleichungsdiskriminante D von $f(x)$ genau durch p^δ teilbar ist. Nach Kap. 1 kann man annehmen, daß die Faktoren $f_i(x)$ reduziert sind; die Grade der Faktoren sollen mit

$$n_1, n_2, \dots, n_r \tag{8}$$

bezeichnet werden, wobei natürlich

$$n_1 + n_2 + \dots + n_r = n \tag{9}$$

ist.

Aus (1) und (7) folgt für $x = \vartheta$ die Kongruenz

$$f_1(\vartheta) f_2(\vartheta) \dots f_r(\vartheta) \equiv 0 \pmod{p^\alpha}, \tag{10}$$

und daraus schließt man, daß die Zahlen $f_i(\vartheta)$ mit p gewisse gemeinsame Idealteiler besitzen müssen.

Es sei wie in Kap. 1 die Resultante von zwei irreduziblen Funktionen $f_i(x)$ und $f_j(x)$ genau durch $p^{\varrho_{ij}}$ teilbar, während die Diskriminante D_i von $f_i(x)$ genau durch p^{δ_i} teilbar sein soll; zwischen den Zahlen ϱ_{ij} und δ_i besteht dann die Relation (11) Kap. 1. Nach Satz 1, Kap. 1, kann man nun solche Polynome $A_{ij}(x)$ und $B_{ij}(x)$ bestimmen, daß

$$A_{ij}(x) f_i(x) + B_{ij}(x) f_j(x) \equiv p^{\varrho_{ij}} \pmod{p^\alpha}. \tag{11}$$

Wenn dann $\mathfrak{p}$ ein beliebiges Primideal ist, das in p aufgeht, so wird vorausgesetzt, daß die Zahl $f_i(\vartheta)$ genau durch $\mathfrak{p}^{\gamma_i}$ teilbar ist; die Zahl γ_i soll die *charakteristische Zahl des Primideals* $\mathfrak{p}$ *in bezug auf* $f_i(x)$ heißen.

Geht das Primideal $\mathfrak{p}$ in p genau in der Potenz $\mathfrak{p}^e$ auf, so folgt

aus (11), wenn man $x = \vartheta$ setzt, daß nicht zugleich γ_i und γ_j größer als $e\varrho_{ij}$ sein kann. Wenn daher γ_i die größte unter den Zahlen

$$\gamma_1, \gamma_2, \ldots, \gamma_r \tag{12}$$

ist, so hat man für die anderen charakteristischen Zahlen, wie man aus (11) für $x = \vartheta$ sieht, die Ungleichungen

$$\gamma_j \leqq e\varrho_{ij}, \qquad (i \neq j) \tag{13}$$

welche auch bestehen, wenn es unter den Zahlen (12) mehrere größte gibt.

Aus (10) folgt aber leicht die Ungleichung

$$\gamma_1 + \gamma_2 + \ldots + \gamma_r \geqq e\alpha,$$

und daher nach (13)

$$\gamma_i + e(\varrho_{i1} + \ldots + \varrho_{i,i-1} + \varrho_{i,i+1} + \ldots + \varrho_{ir}) \geqq e\alpha,$$

oder

$$\gamma_i \geqq e(\alpha - \varrho_{i1} - \ldots - \varrho_{i,i-1} - \varrho_{i,i+1} - \ldots - \varrho_{ir}).$$

Setzt man wie in Kap. 1

$$\varrho' = \sum_{i>j} \varrho_{ij}, \tag{14}$$

so ist

$$\varrho' \geqq \varrho_{i1} + \ldots + \varrho_{i,i-1} + \varrho_{i,i+1} + \ldots + \varrho_{ir},$$

und daher

$$\gamma_i \geqq e(\alpha - \varrho'). \tag{15}$$

Nach der Relation (13) Kap. 1 schließt man daher, daß es für jedes Primideal $\mathfrak{p}$, das in p aufgeht, eine einzige größte charakteristische Zahl γ_i gibt, während für alle anderen die Ungleichungen (13) bestehen.

Dies soll im folgenden kurz so ausgedrückt werden, daß *das Primideal* $\mathfrak{p}$ *zur irreduziblen Funktion* $f_i(x)$ *gehört.*

Es ist also bewiesen, daß jedes Primideal $\mathfrak{p}$ zu einer einzigen irreduziblen Funktion $f_i(x) \pmod{p^\alpha}$ gehört. Es soll nun bewiesen werden, daß es auch zu jeder irreduziblen Funktion $f_i(x)$ mindestens ein zugehöriges Primideal gibt.

Wenn nämlich dies nicht der Fall wäre, so würde also für ein i die Zahl $f_i(\vartheta)$ für jeden Primidealteiler $\mathfrak{p}$ von p nur durch $\mathfrak{p}^{\gamma_i}$ teilbar sein, wobei

$$\gamma_i \leqq e\varrho_{ij} \qquad (j \neq i)$$

wäre, wenn $\mathfrak{p}$ zur irreduziblen Funktion $f_j(x)$ gehöre. Daraus folgt aber nach (10), daß die Zahl

$$f_1(\vartheta) \ldots f_{i-1}(\vartheta) f_{i+1}(\vartheta) \ldots f_r(\vartheta)$$

für alle Primideale $\mathfrak{p}$ durch $\mathfrak{p}^{e(\alpha-\varrho_{ij})}$, also auch durch $\mathfrak{p}^{e(\alpha-\varrho')}$ teilbar würde. Es muß daher die Kongruenz

$$f_1(\vartheta)\dots f_{i-1}(\vartheta)f_{i+1}(\vartheta)\dots f_r(\vartheta) \equiv 0 \,(\mathrm{mod}\, p^{\alpha-\varrho'})$$

bestehen. Wird aber darauf der Satz 2, Kap. 2, angewandt, so folgt die identische Kongruenz

$$f_1(x)\dots f_{i-1}(x)f_{i+1}(x)\dots f_r(x) \equiv 0 \,(\mathrm{mod}\, p^{\alpha-\varrho'-\varkappa}),$$

welche aber nicht bestehen kann, indem die linke Seite nicht durch p teilbar ist. Man muß also

$$\alpha \leqq \varrho' + \varkappa$$

haben, was auch nicht möglich ist, indem $\alpha \geqq \delta + 1$ und nach (13) Kap. 1 folgt $\varrho' \leqq \frac{\delta}{2}$ und ebenso nach (5) $\varkappa \leqq \frac{\delta}{2}$.

Unsere Behauptung ist also bewiesen.

Es sollen nun genauer die Eigenschaften eines Primideals $\mathfrak{p}$ studiert werden, das zur irreduziblen Funktion $f_i(x)$ gehört.

Nach dem Satze 4, Kap. 1, kann man aus (7) eine entsprechende Zerlegung von $f(x)$ in irreduzible Faktoren für alle Moduln $(\mathrm{mod}\, p^\beta)$ $\beta > \alpha$ bestimmen,

$$f(x) \equiv f_1^{(\beta)}(x)\, f_2^{(\beta)}(x)\dots f_r^{(\beta)}(x) \,(\mathrm{mod}\, p^\beta),$$

wobei allgemein

$$f_i^{(\beta)}(x) \equiv f_i(x) \,(\mathrm{mod}\, p^{\alpha-\varrho'}).$$

Für die Faktoren $f_i^{(\beta)}(x)$ erhält man daher dieselben Zahlen ϱ_{ij} und δ_i wie für die entsprechenden $f_i(x)$. Weiter werden auch die charakteristischen Zahlen für ein Primideal $\mathfrak{p}$ nicht geändert; nur wenn $\mathfrak{p}$ zur irreduziblen Funktion $f_i(x)$ gehört, so wird die entsprechende charakteristische Zahl γ_i für $f_i^{(\beta)}(x)$ mit β beliebig groß, indem man nach (15)

$$\gamma_i \geqq e(\beta - \varrho')$$

hat, d. h. es besteht die Kongruenz

$$f_i^{(\beta)}(\vartheta) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}^{e(\beta-\varrho')}). \tag{16}$$

Es soll jetzt untersucht werden, wann eine Ringzahl $F(\vartheta)$ durch eine Potenz von $\mathfrak{p}$ teilbar sein kann, der Einfachheit wegen wird vorausgesetzt, daß der Exponent ein Multiplum von e ist, d. h. man soll untersuchen, wann $F(\vartheta)$ durch $\mathfrak{p}^{e\gamma}$ teilbar sein kann.

Für jedes γ gibt es sicher Polynome $G_\gamma(x) \not\equiv 0 \,(\mathrm{mod}\, p)$, wofür die Kongruenz

$$G_\gamma(\vartheta) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}^{e\gamma}) \tag{17}$$

erfüllt ist. Denn nach (16) hat sicher $f_i^{(\beta)}(x)$ diese Eigenschaft, wenn nur $\beta \geqq \gamma + \varrho'$ gewählt wird. Unter den Polynomen $G_\gamma(x)$, wofür die Kongruenz (17) erfüllt ist, gibt es sicher solche, wofür der Grad möglichst klein wird und der Grad von einem solchen Polynome ist gewiß $\leqq n_i$. Man kann auch annehmen, daß ein solches Polynom reduziert ist. Denn im entgegengesetzten Falle kann man nach Satz 2, Kap. 1, $G_\gamma(x)$ in die Form

$$G_\gamma(x) \equiv F_\gamma(x)(A + p H_\gamma(x)) \pmod{p^\gamma}$$

schreiben, wobei $F_\gamma(x)$ reduziert und die Zahl A nicht durch p teilbar ist. Da die Zahl $A + p H_\gamma(\vartheta)$ nicht durch $\mathfrak{p}$ teilbar ist, enthält $F_\gamma(\vartheta)$ auch die Potenz $\mathfrak{p}^{e\gamma}$ und man kann daher $G_\gamma(x)$ durch das reduzierte $F_\gamma(x)$ ersetzen.

Der Grad m_γ eines solchen Polynoms $F_\gamma(x)$ wird natürlich von γ abhängen und mit γ wachsen oder jedenfalls nicht abnehmen. Da aber $m_\gamma \leqq n_i$ ist, so folgt, daß es ein γ_0 gibt, so daß, wenn $\gamma > \gamma_0$ ist, der Grad von $F_\gamma(x)$ von γ unabhängig und also gleich m_{γ_0} wird. Man kann aber dann zeigen, daß $m_{\gamma_0} = n_i$ ist. Denn dividiert man $f_i^{(\beta)}(x)$ durch $F_\gamma(x)$, so erhält man

$$f_i^{(\beta)}(x) = Q(x) F_\gamma(x) + R(x) \qquad (\gamma > \gamma_0, \quad \beta > \gamma + \varrho'), \tag{18}$$

woraus für $x = \vartheta$ folgt, daß die Zahl $R(\vartheta)$ auch durch $\mathfrak{p}^{e\gamma}$ teilbar ist. Da aber der Grad von $R(x)$ kleiner als m_{γ_0} ist, müssen in $R(x)$ alle Koeffizienten durch p teilbar sein, so daß man

$$R(x) = p^\lambda R_1(x), \qquad R_1(x) \not\equiv 0 \pmod{p}, \tag{19}$$

setzen kann. Die Zahl $R_1(\vartheta)$ wird also durch $\mathfrak{p}^{e(\gamma-\lambda)}$ teilbar, und dies ist nur möglich, wenn

$$e(\gamma - \lambda) < e\gamma_0$$

ist, also

$$\lambda > \gamma - \gamma_0.$$

Wählt man nun γ so groß, daß $\gamma - \gamma_0 \geqq \delta + 1$ und also $\lambda > \delta + 1$ ist, so folgt aus (19) und (18)

$$f_i^{(\beta)}(x) \equiv Q(x) F_\gamma(x) \pmod{p^{\delta+1}}.$$

Diese Kongruenz ist aber nicht möglich, außer wenn $Q(x) \equiv 1 \pmod{p^{\delta+1}}$ ist, indem $f_i^{(\beta)}(x) \pmod{p^{\delta+1}}$ eine irreduzible Funktion ist; man hat also $m_\gamma = m_{\gamma_0} = n_i$, wenn $\gamma > \gamma_0$ ist. Allgemeiner sieht man ein, daß immer die Kongruenz

$$F_\gamma(x) \equiv f_i^{(\beta)}(x) \pmod{p^{\gamma-\gamma_0}} \qquad (\beta \geqq \gamma + \varrho')$$

besteht.

Wenn nun eine beliebige Ringzahl $F(\vartheta)$ durch $\mathfrak{p}^{e\gamma}$, $\gamma > \gamma_0$ teilbar sein soll, kann man $F(x)$ durch $f_i^{(\beta)}(x)$ dividieren,

$$F(x) = Q(x) f_i^{(\beta)}(x) + R(x) \qquad (\beta \geqq \gamma + \varrho'), \tag{20}$$

und für $x = \vartheta$ folgt daraus, daß $R(\vartheta)$ durch $\mathfrak{p}^{e\gamma}$ teilbar ist, woraus man wie früher $R(x) \equiv 0 \pmod{p^{\gamma-\gamma_0}}$ schließt, so daß nach (20) die Kongruenz

$$F(x) \equiv Q(x) f_i^{(\beta)}(x) \pmod{p^{\gamma-\gamma_0}}$$

besteht. Man kann daher sagen:

Wenn eine Ringzahl $F(\vartheta)$ durch $\mathfrak{p}^{e\gamma}$ teilbar sein soll, so besteht die identische Kongruenz

$$F(x) \equiv 0 \,(\mathrm{modd}\, p^{\gamma-\gamma_0}, f_i^{(\beta)}(x)).$$

Daraus folgt weiter einfach, daß, wenn für zwei Ringzahlen $F_1(\vartheta)$ und $F_2(\vartheta)$ die Kongruenz

$$F_1(\vartheta) \equiv F_2(\vartheta) \pmod{\mathfrak{p}^{e\gamma}}$$

bestehen soll, so hat man identisch

$$F_1(x) \equiv F_2(x) \,(\mathrm{modd}\, p^{\gamma-\gamma_0}, f_i^{(\beta)}(x)).$$

Aus der letzten Bemerkung kann man eine sehr wichtige Eigenschaft des Primideals $\mathfrak{p}$ herleiten. Da es nämlich unter den Polynomen $F(x)$ $(\mathrm{modd}\, p^{\gamma-\gamma_0}, f_i^{(\beta)}(x))$ genau $p^{n_i(\gamma-\gamma_0)}$ verschiedene Reste gibt, so gibt es auch mindestens $p^{n_i(\gamma-\gamma_0)}$ verschiedene Ringzahlen für den Modul $\mathfrak{p}^{e\gamma}$.

Andererseits kann man eine beliebige Körperzahl ω nach § 1 immer in der Form

$$\omega = \frac{F(\vartheta)}{k}$$

schreiben, wobei $F(\vartheta)$ eine Ringzahl und k der Index ist. Wenn dann ω durch $\mathfrak{p}^{e\gamma}$ teilbar sein soll, muß also $F(\vartheta)$ durch $\mathfrak{p}^{e(\gamma+\varkappa)}$ teilbar sein. Dies ist aber, wie man leicht bemerkt, sicher der Fall, wenn

$$F(x) \equiv 0 \,(\mathrm{modd}\, p^{\gamma+\varkappa}, f_i^{(\beta)}(x)) \qquad (\beta > \gamma + \varkappa + \varrho')$$

ist. Da es für den Doppelmodul $(\mathrm{modd}\, p^{\gamma+\varkappa}, f_i^{(\beta)}(x))$ genau $p^{n_i(\gamma+\varkappa)}$ verschiedene Reste gibt, so wird es im Körper höchstens $p^{n_i(\gamma+\varkappa)}$ verschiedene Zahlen $(\mathrm{mod}\, \mathfrak{p}^{e\gamma})$ geben.

Wenn nun der Grad von $\mathfrak{p}$ gleich f ist, so wird

$$N(\mathfrak{p}^{e\gamma}) = p^{ef\gamma}$$

und man hat daher die Ungleichungen

$$p^{n_i(\gamma-\gamma_0)} \leqq p^{ef\gamma} \leqq p^{n_i(\gamma+\varkappa)}$$

oder auch

$$n_i(\gamma - \gamma_0) \leqq ef\gamma \leqq n_i(\gamma + \varkappa),$$

woraus folgt, wenn man durch γ dividiert

$$n_i\left(1-\frac{\gamma_0}{\gamma}\right) \leqq ef \leqq n_i\left(1+\frac{\varkappa}{\gamma}\right).$$

Da man hier γ beliebig groß machen kann, so wird daraus folgen, daß n_i beliebig nahe an ef kommt, und da es sich um ganze rationale Zahlen handelt, erhält man folglich die wichtige Gleichung

$$ef = n_i. \tag{21}$$

Unter Anwendung der Gleichung (21) kann man nun die wichtige Tatsache beweisen, daß es für jede irreduzible Funktion $f_i(x)$ nur ein einziges zugehöriges Primideal gibt. Denn wie schon bewiesen, gibt es jedenfalls zu jedem $f_i(x)$ *ein* entsprechendes $\mathfrak{p}_i$, und wenn Ordnung und Grad von $\mathfrak{p}_i$ mit e_i und f_i bezeichnet werden, so ist nach (21) $e_i f_i = n_i$. Wenn man dann das Ideal

$$p' = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r}$$

bildet, so ist sicher p' ein Teiler von p. Da aber

$$Np' = p^{\sum_{i=1}^{r} e_i f_i} = p^{\sum_{i=1}^{r} n_i} = p^n$$

ist, so muß man auch $p' = p$ haben, d. h. es kann für jedes $f_i(x)$ nur das einzige $\mathfrak{p}_i$ geben. Es ist daher der folgende Hauptsatz bewiesen:

Satz 3. *Besteht für $f(x)$ die Zerlegung in irreduzible Faktoren* $(\mathrm{mod}\, p^\alpha)$, $\alpha \geqq \delta + 1$,

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x) \,(\mathrm{mod}\, p^\alpha),$$

wobei der Grad von $f_i(x)$ gleich n_i ist, so hat die Primzahl p in R die Primidealzerlegung

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r},$$

wobei

$$N(\mathfrak{p}_i^{e_i}) = p^{n_i}.$$

§ 3.

Anwendungen des Hauptsatzes.

Es werden im folgenden die Bezeichnungen angewandt: Die Primzahl p soll die Primidealzerlegung

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r}, \qquad N\mathfrak{p}_i = p^{f_i} \tag{22}$$

haben. Wenn dann

$$f(x) \equiv f_1(x) f_2(x) \dots f_r(x) \,(\mathrm{mod}\, p^\alpha) \qquad (\alpha \geqq \delta + 1)$$

eine Zerlegung von $f(x)$ in irreduzible Faktoren $(\mathrm{mod}\, p^\alpha)$ ist, so hat man also

$$e_i f_i = n_i, \tag{23}$$

wenn n_i der Grad von $f_i(x)$ ist. Wenn weiter die Zahl $f_j(\vartheta)$ genau durch $\mathfrak{p}_i^{\gamma_{ij}}$ teilbar ist, so heißt γ_{ij} die charakteristische Zahl von $f_j(x)$ in bezug auf $\mathfrak{p}_i$. Es bestehen dann nach § 2 die Ungleichungen

$$\gamma_{ij} \leqq \varrho_{ij} e_i \qquad (i \neq j),$$

während die Zahl $f_i(\vartheta)$ nach (15) sicher durch $\mathfrak{p}_i^{e_i(\alpha-\varrho')}$ teilbar ist.

Man kann nun genauer angeben, wann eine Ringzahl $F(\vartheta)$, $F(x) \not\equiv 0 \,(\mathrm{mod}\, p)$ durch eine Potenz $\mathfrak{p}_i^{e_i\gamma}$ teilbar ist. Nimmt man nämlich zuerst an, daß der Grad von $F(x)$ kleiner als n_i ist, so bildet man die Zahl

$$f_1^{(\beta)}(\vartheta) \ldots f_{i-1}^{(\beta)}(\vartheta)\, F(\vartheta)\, f_{i+1}^{(\beta)}(\vartheta) \ldots f_r^{(\beta)}(\vartheta) \qquad (\beta \geqq \gamma + \varrho').$$

Diese Zahl ist sicher durch $\mathfrak{p}_i^{e_i\gamma}$ teilbar, während jedes von $\mathfrak{p}_i$ verschiedene Primideal $\mathfrak{p}_j$ sicher in der Potenz $\mathfrak{p}_i^{e_j\gamma}$ vorkommt. Man hat daher

$$f_1^{(\beta)}(\vartheta) \ldots f_{i-1}^{(\beta)}(\vartheta)\, F(\vartheta)\, f_{i+1}^{(\beta)}(\vartheta) \ldots f_r^{(\beta)}(\vartheta) \equiv 0 \,(\mathrm{mod}\, p^\gamma)$$

woraus nach Satz 2

$$f_1^{(\beta)}(x) \ldots f_{i-1}^{(\beta)}(x)\, F(x)\, f_{i+1}^{(\beta)}(x) \ldots f_r^{(\beta)}(x) \equiv 0 \,(\mathrm{mod}\, p^{\gamma-\varkappa})$$

folgt. Diese letzte Kongruenz ist aber nur möglich, wenn man

$$F(x) \equiv 0 \,(\mathrm{mod}\, p^{\gamma-\varkappa})$$

hat. Im allgemeinen Falle, wo der Grad von $F(x)$ größer als n_i ist, folgt dann leicht wie früher aus der Kongruenz

$$F(\vartheta) \doteq 0 \,(\mathrm{mod}\, \mathfrak{p}_i^{e_i\gamma})$$

die identische Kongruenz

$$F(x) \equiv 0 \,(\mathrm{modd}\, p^{\gamma-\varkappa}, f_i^{(\beta)}(x)) \qquad (\beta \geqq \gamma + \varrho').$$

Satz 4. *Wenn eine Ringzahl $F(\vartheta)$ durch $\mathfrak{p}_i^{e_i\gamma}$ teilbar sein soll, muß das Polynom $F(x) \,(\mathrm{mod}\, p^{\gamma-\varkappa})$ durch $f_i^{(\beta)}(x)$, $\beta \geqq \gamma + \varrho'$, teilbar sein.*

Man kann auch eine wichtige Anwendung von diesem Satze auf die Theorie der höheren Kongruenzen für Primzahlpotenzmoduln geben.

Es seien

$$\begin{aligned} f(x) &\equiv f_1^{(\alpha)}(x)\, f_2^{(\alpha)}(x) \ldots f_r^{(\alpha)}(x) \,(\mathrm{mod}\, p^\alpha) \qquad (\alpha \geqq \delta + 1), \\ &\equiv \varphi_1^{(\alpha)}(x)\, \varphi_2^{(\alpha)}(x) \ldots \varphi_s^{(\alpha)}(x), \end{aligned} \tag{24}$$

zwei Zerlegungen von dem Polynome $f(x)$ in irreduzible Faktoren $(\mathrm{mod}\, p^\alpha)$. Wegen der Eindeutigkeit der Zerlegung von p in Primideale folgt dann

zunächst, daß $r = s$ sein muß. Weiter wird ein Primideal $\mathfrak{p}_i$ zu den beiden irreduziblen Faktoren $\varphi_i^{(\alpha)}(x)$ und $f_i^{(\alpha)}(x)$ derart gehören, daß

$$f_i^{(\alpha)}(\vartheta) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}_i^{e_i(\alpha-\varrho')}),$$
$$\varphi_i^{(\alpha)}(\vartheta) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}_i^{e_i(\alpha-\varrho'')})$$

ist, wobei ϱ'' für die zweite Zerlegung (24) dieselbe Bedeutung wie ϱ' für die erste hat. Nach (23) folgt, daß sowohl $f_i^{(\alpha)}(x)$ als $\varphi_i^{(\alpha)}(x)$ vom Grade n_i ist. Man kann nun, was unwesentlich ist, $\varrho'' \geqq \varrho'$ voraussetzen. Dann folgt nach Satz 4, daß $\varphi_i^{(\alpha)}(x) \,(\mathrm{mod}\, p^{\alpha-\varrho''-\varkappa})$ durch $f_i^{(\alpha)}(x)$ teilbar sein muß. Da aber $\varkappa \leqq \frac{\delta}{2}$, $\varrho'' \leqq \frac{\delta}{2}$ ist, so folgt daraus einfach

$$f_i^{(\alpha)}(x) \equiv \varphi_i^{(\alpha)}(x) \,(\mathrm{mod}\, p^{\alpha-\delta}).$$

Es ist daher bewiesen:

Satz 5. *Zerlegt man ein irreduzibles Polynom $f(x)$ in irreduzible Faktoren* $(\mathrm{mod}\, p^{\alpha})$, *so ist diese Zerlegung* $(\mathrm{mod}\, p^{\alpha-\delta})$ *eindeutig, d. h. wenn zwei Zerlegungen*

$$\begin{aligned} f(x) &\equiv f_1^{(\alpha)}(x)\, f_2^{(\alpha)}(x) \ldots f_r^{(\alpha)}(x) \\ &\equiv \varphi_1^{(\alpha)}(x)\, \varphi_2^{(\alpha)}(x) \ldots \varphi_s^{(\alpha)}(x) \end{aligned} (\mathrm{mod}\, p^{\alpha})$$

bestehen, so ist $r = s$ und für alle $i = 1, 2, \ldots, r$

$$\varphi_i^{(\alpha)}(x) \equiv f_i^{(\alpha)}(x) \,(\mathrm{mod}\, p^{\alpha-\delta}).$$

Dieser Satz kann natürlich auch direkt, ohne Anwendung der Theorie der algebraischen Zahlen bewiesen werden.

Kapitel III.

Über die Eigenschaften von Diskriminanten und Differenten.

§ 1.

Über Führer.

Wie schon in Kap. II § 1 bemerkt, bilden die Zahlen

$$(1) \qquad R(\vartheta) = a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1},$$

wobei die a_i ganz rational sind, einen Ring, d. h. die Summe, Differenz und Produkt von zwei solchen Zahlen hat wieder dieselbe Form. Im allgemeinen werden nicht alle ganze Körperzahlen zum Ringe gehören; wenn aber k den Index der Zahl ϑ bezeichnet, so folgt aus Kap. II § 1 leicht, daß wenn ω eine ganze Körperzahl ist, so wird

$$(2) \qquad k\omega = A(\vartheta)$$

eine Ringzahl.

Alle Zahlen φ des Körpers, welche die Eigenschaft haben, daß für jedes ω das Produkt

$$\omega\,\varphi = A(\vartheta) \tag{3}$$

eine Ringzahl wird, bilden, wie man leicht sieht, ein Ideal $\mathfrak{f}$, das nach Dedekind der *Führer* des Ringes heißt. Aus (2) folgt sofort, daß $\mathfrak{f}$ ein Teiler von k sein muß. Setzt man in (3) $\omega = 1$, so folgt, daß alle Zahlen in $\mathfrak{f}$ auch dem Ringe angehören.

Die Zahl $f'(\vartheta)$ heißt die *Differente der Zahl* ϑ, und es ist dann

$$D = \pm N(f'(\vartheta)), \tag{4}$$

wobei D die *Gleichungsdiskriminante* von der Gleichung $f(x) = 0$ ist. Man beweist dann weiter leicht, daß eine Relation

$$f'(\vartheta) = \mathfrak{f}\cdot\mathfrak{d} \tag{5}$$

besteht, wo das Ideal $\mathfrak{d}$ von der speziellen Wahl der Zahl ϑ unabhängig ist. Das Ideal $\mathfrak{d}$ heißt die *Differente des Körpers* und hat die wichtige Eigenschaft, daß

$$N(\mathfrak{d}) = |d|, \tag{6}$$

wobei d die *Körperdiskriminante* ist.

Man kann nun weitere Führerbegriffe einführen, indem man die Bedingung (3) durch entsprechende Kongruenzen ersetzt. So bilden alle ganzen Zahlen $\varphi_p^{(\alpha)}$ mit der Eigenschaft, daß für alle ω die Kongruenz

$$\omega\,\varphi_\gamma^{(\alpha)} \equiv A(\vartheta)\,(\mathrm{mod}\,p^\alpha)$$

besteht, ein Ideal $\mathfrak{f}_p^{(\alpha)}$, das sicher ein Teiler von $\mathfrak{f}$ wird.

Das Ideal $\mathfrak{f}_p^{(\alpha)}$ wird natürlich von α abhängig, aber man kann zeigen, daß wenn nur α oberhalb einer bestimmten Grenze liegt, so wird $\mathfrak{f}_p^{(\alpha)}$ von α unabhängig, und zwar hat man

$$\mathfrak{f}_p = \mathfrak{f}_p^{(\varkappa)} = \mathfrak{f}_p^{(\alpha)} \qquad (\alpha > \varkappa), \tag{7}$$

wenn wie früher der Index k genau durch $p^\varkappa$ teilbar ist. Dies folgt einfach aus der Tatsache, daß wenn eine Kongruenz

$$\omega \equiv P_\varkappa(\vartheta)\,(\mathrm{mod}\,p^\varkappa) \tag{8}$$

gilt, so kann man auch ein Polynom $P_\alpha(x)$ so bestimmen, daß

$$\omega \equiv P_\alpha(\vartheta)\,(\mathrm{mod}\,p^\alpha) \qquad (\alpha > \varkappa)$$

wird. Aus (8) folgt nämlich sofort

$$\omega = P_\varkappa(\vartheta) + p^\varkappa\,\omega_1,$$

wobei ω_1 wieder eine ganze Zahl ist, und daher ist nach Satz 1 Kap. II auch $p^\varkappa\,\omega_1\,(\mathrm{mod}\,p^\alpha)$ kongruent einer Ringzahl.

Das von α unabhängige Ideal $\mathfrak{f}_p$ in (7) soll der *Führer des Ringes in bezug auf* p heißen, und wenn ω eine Körperzahl ist, und φ eine Zahl in $\mathfrak{f}_p$, so besteht immer eine Kongruenz

$$\omega\varphi \equiv P(\vartheta) \pmod{p^\alpha},$$

wobei α beliebig groß gewählt werden kann.

Da nach Satz 1 Kap. II immer $p^\varkappa\omega \pmod{p^\alpha}$ kongruent einer Ringzahl ist, so wird $\mathfrak{f}_p$ immer ein Teiler von $p^\varkappa$ und kann daher nur solche Primideale enthalten, welche in p aufgehen. Wenn p nicht in k aufgeht, ist $p^\varkappa = 1$ und man erhält daher auch $f_p = 1$. Die Ideale $\mathfrak{f}_p$ werden also nur dann vom Einheitsideale verschieden, wenn p ein Teiler von k ist.

Man beweist nun:

Satz 1. *Der Führer* $\mathfrak{f}$ *ist gleich dem Produkte aller Führer* $\mathfrak{f}_p$, *wobei* p *die Primzahlteiler von* k *durchläuft, also*

$$\mathfrak{f} = \prod_{k/p} \mathfrak{f}_p.$$

Zunächst folgt aus einer Gleichung (3), daß auch die entsprechenden Kongruenzen für alle Moduln bestehen, so daß eine Zahl φ in $\mathfrak{f}$ auch zu allen Idealen $\mathfrak{f}_p$ gehört, und also, da die $\mathfrak{f}_p$ zueinander teilerfremd sind, auch zu ihrem Produkt. $\mathfrak{f}$ muß daher durch das Produkt $\prod \mathfrak{f}_p$ teilbar sein.

Wenn aber umgekehrt φ eine Zahl des Ideals $\prod \mathfrak{f}_p$ ist, so besteht auch immer eine Kongruenz

$$\omega\varphi \equiv P_p(\vartheta) \pmod{p^\alpha},$$

oder

$$\omega\varphi = P_p(\vartheta) + p^\alpha\omega_p. \tag{9}$$

Für eine andere Primzahl q folgt entsprechend, daß $\omega\varphi$ und daher auch nach (9) $p^\alpha\omega_p \pmod{q^\beta}$ eine Zahl des Ringes wird. Dann wird also auch $\omega_p \pmod{q^\beta}$ eine Zahl des Ringes und man erhält aus (9) eine Gleichung von der Form

$$\omega\varphi = P_{p,q}(\vartheta) + p^\alpha q^\beta \omega_{pq}.$$

Ebenso zeigt man allgemein, daß wenn $p, q, \ldots, r$ die verschiedenen Primzahlteiler von k sind, so besteht eine Gleichung

$$\omega\varphi = P_{p,q,\ldots,r}(\vartheta) + p^\alpha q^\beta \ldots r^\gamma \omega_{p,q,\ldots,r}.$$

Da hier das letzte Glied durch k teilbar wird, so muß $\omega\varphi$ auch selbst eine Zahl des Ringes sein und daher zu $\mathfrak{f}$ gehören.

Zuletzt erwähne ich noch einen weiteren Führerbegriff. Wenn $\mathfrak{p}$ ein Primideal ist, das in p genau in der Potenz $\mathfrak{p}^e$ aufgeht, so kann man $p = \mathfrak{p}^e\mathfrak{q}$ setzen, wo $\mathfrak{q}$ nicht durch $\mathfrak{p}$ teilbar ist. Die Zahlen φ, wofür immer eine Kongruenz

$$\omega\varphi \equiv P(\vartheta) \pmod{\mathfrak{p}^\alpha}$$

besteht, bilden ein Ideal $\mathfrak{f}_\mathfrak{p}^{(\alpha)}$. Man zeigt auch hier leicht, daß wenn $\alpha > e\varkappa$ ist, $\mathfrak{f}_\mathfrak{p} = \mathfrak{f}_\mathfrak{p}^{(\alpha)}$ von α unabhängig wird. Dies folgt, indem man beweist, daß man aus einer Kongruenz

$$\omega \equiv P_{e\varkappa}(\vartheta) \pmod{\mathfrak{p}^{e\varkappa}} \tag{10}$$

eine Kongruenz

$$\omega \equiv P_\alpha(\vartheta) \pmod{\mathfrak{p}^\alpha}$$

ableiten kann. Man kann nämlich immer eine solche Zahl ψ bestimmen, daß die Kongruenzen

$$\psi \equiv 1 \pmod{\mathfrak{p}^\alpha}, \qquad \psi \equiv 0 \pmod{\mathfrak{q}^\varkappa}$$

erfüllt sind, und wenn man dann (10) mit ψ multipliziert, erhält man eine Kongruenz von der Form

$$\omega \equiv P_{e\varkappa}(\vartheta) + p^\varkappa \omega \pmod{\mathfrak{p}^\alpha},$$

woraus nach Satz 1, Kap. II folgt, daß $\omega \pmod{\mathfrak{p}^\alpha}$ kongruent einer Ringzahl ist.

Das Ideal $\mathfrak{f}_\mathfrak{p}$ heißt der *Führer des Ringes in bezug auf* p, und wenn φ eine Zahl in $\mathfrak{f}_\mathfrak{p}$ ist, so besteht für alle ganze Körperzahlen ω eine Kongruenz

$$\omega\varphi \equiv P(\vartheta) \pmod{\mathfrak{p}^\alpha},$$

wo α beliebig groß gewählt werden kann. Wie oben zeigt man leicht, daß jede durch $\mathfrak{p}^{e\varkappa}$ teilbare Zahl $(\mathrm{mod}\,\mathfrak{p}^\alpha)$ zum Ringe gehört, so daß $\mathfrak{f}_\mathfrak{p}$ ein Teiler von $\mathfrak{p}^{e\varkappa}$ und folglich auch eine Potenz von $\mathfrak{p}$ sein muß.

Ich werde jetzt den Zusammenhang zwischen den Führern $\mathfrak{f}_\mathfrak{p}$ und dem entsprechenden Primzahlführer $\mathfrak{f}_p$ ermitteln. Es sei die Primidealzerlegung von p durch (22), Kap. II gegeben, und da $\mathfrak{f}_{\mathfrak{p}_i}$ eine Potenz von $\mathfrak{p}_i$ ist, kann man

$$\mathfrak{f}_{\mathfrak{p}_i} = \mathfrak{p}_i^{\gamma_i} \tag{11}$$

setzen.

Es werden nun die allgemeinen Bezeichnungen des Kapitels II angewandt, und die charakteristischen Zahlen des Primideals $\mathfrak{p}_i$ sind daher $\gamma_{i1}, \gamma_{i2}, \ldots, \gamma_{ir}$. Man setzt

$$\gamma_i = \gamma_{i1} + \ldots + \gamma_{i,i-1} + \gamma_{i,i+1} + \ldots + \gamma_{i,r}, \tag{12}$$

und nach der Definition der Zahlen $\gamma_{i,j}$ ist dann die Zahl

$$\Pi_i(\vartheta) = f_1(\vartheta) \ldots f_{i-1}(\vartheta) f_{i+1}(\vartheta) \ldots f_r(\vartheta)$$

genau durch $\mathfrak{p}_i^{\gamma_i}$ teilbar.

Da alle durch $\mathfrak{p}_i^{\gamma_i}$ teilbaren Körperzahlen kongruent einer Ringzahl

$(\mathrm{mod}\,\mathfrak{p}_i^{\alpha})$ sind, so wird es auch im Ringe $e_i f_i = n_i$ durch $\mathfrak{p}_i^{r_i}$ teilbare Zahlen

$$R_1^{(i)}(\vartheta),\ R_2^{(i)}(\vartheta),\ \ldots,\ R_{n_i}^{(i)}(\vartheta)$$

so geben, daß sie ein Fundamentalsystem für $\mathfrak{p}_i^{r_i}\ (\mathrm{mod}\,\mathfrak{p}_i^{\alpha})$ bilden [5]), d. h. jede durch $\mathfrak{p}_i^{r_i}$ teilbare Zahl ω läßt sich $(\mathrm{mod}\,\mathfrak{p}_i^{\alpha})$ kongruent einer Summe

$$\omega \equiv a_1^{(i)} R_1^{(i)}(\vartheta) + a_2^{(i)} R_2^{(i)}(\vartheta) + \ldots + a_{n_i}^{(i)} R_{n_i}^{(i)}(\vartheta)\ (\mathrm{mod}\,\mathfrak{p}_i^{\alpha})$$

schreiben, wobei die Zahlen $a_j^{(i)}$ alle ganz rational sind.

Bildet man dann weiter das System von n Zahlen

$$K_{i,j}(\vartheta) = \Pi_i(\vartheta)\, R_j^{(i)}(\vartheta) \qquad (j = 1, 2, \ldots, n_i;\ i = 1, 2, \ldots, r),$$

so sind diese Zahlen, wie man leicht sieht, ein Fundamentalsystem in bezug auf p für ein Ideal

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\gamma_i + r_i},$$

d. h. jede durch $\mathfrak{a}$ teilbare Zahl kann in der Form

$$\omega \equiv \sum_{i,j} a_j^{(i)} K_{i,j}(\vartheta)\ (\mathrm{mod}\,p^{\alpha})$$

dargestellt werden, wobei alle $a_j^{(i)}$ ganz rational sind. Da alle Zahlen $K_{i,j}(\vartheta)$ zum Ringe gehören, so folgt, daß $\mathfrak{f}_p$ ein Teiler von $\mathfrak{a}$ sein muß.

Man kann aber zeigen, daß $\mathfrak{a} = \mathfrak{f}_p$ ist, indem man beweist, daß kein Primideal in $\mathfrak{f}_p$ in einer kleineren Potenz als $\mathfrak{p}_i^{\gamma_i + r_i}$ vorkommt. Es soll nun bewiesen werden, daß nicht alle Zahlen im Ideale $\frac{\mathfrak{a}}{\mathfrak{p}_i}\ (\mathrm{mod}\,p^{\alpha})$ zum Ringe gehören. Man kann nämlich eine solche Ringzahl $F(\vartheta)$ finden, daß sie genau durch $\mathfrak{p}_i^{e_i + r_i - 1}$ teilbar ist, und weiter kann man auch voraussetzen, daß der Grad von $F(x)$ kleiner als n_i ist. Weiter kann man auch $F(x)$ so wählen, daß $F(x) \not\equiv 0\ (\mathrm{mod}\,p)$ wird, indem sonst, wie man leicht sieht, jede durch $\mathfrak{p}_i^{r_i - 1}$ teilbare Zahl kongruent einer Ringzahl $(\mathrm{mod}\,\mathfrak{p}_i^{\alpha})$ wurde. Wenn man dann die Zahl

$$\omega = \Pi_i(\vartheta)\frac{F(\vartheta)}{p}$$

bildet, so ist, wie man leicht sieht, ω eine ganze Zahl, welche zum Ideale $\frac{\mathfrak{a}}{\mathfrak{p}_i}$ gehört. Es kann aber keine Kongruenz

$$\omega = \Pi_i(\vartheta)\frac{F(\vartheta)}{p} \equiv F_1(\vartheta)\ (\mathrm{mod}\,p^{\alpha})$$

bestehen, indem sonst nach Kap. II, Satz 2 die identische Kongruenz

$$\Pi_i(x)\, F(x) \equiv p\, F_1(x)\ (\mathrm{mod}\,p^{\alpha - \varkappa})$$

[5]) Man sehe meine Arbeit: Ö. Ore, Bestimmung der Differente eines algebraischen Zahlkörpers, § 1, Acta Math. **46** (1925), S. 365–392.

bestehen würde, was nach den Voraussetzungen über $F(x)$ nicht möglich ist. Es folgt daher

Satz 2. *Der Führer* $\mathfrak{f}_p$ *des Ringes ist durch die Formel*

$$\mathfrak{f}_p = \prod_{i=1}^{r} \mathfrak{p}_i^{\gamma_i + \tau_i}$$

bestimmt.

Es sei wie früher e_i und f_i die Ordnung bzw. Gradzahl eines Primideals $\mathfrak{p}_i$. Wenn dann $\varphi(x) \pmod p$ eine beliebige Primfunktion f_i-ten Grades ist, so zeigt man leicht[6]), daß man in K eine solche ganze Zahl ω finden kann, daß $\varphi(\omega)$ genau durch die erste Potenz von $\mathfrak{p}_i$ teilbar ist, während keine anderen Primidealteiler von p in $\varphi(\omega)$ aufgehen. Es soll nun die Gleichung $F(x) = 0$ untersucht werden, welcher die Zahl ω genügt. Es folgt sofort, daß man

$$F(x) \equiv \pi(x)\, \varphi(x)^e \pmod p$$

haben muß, wobei $\pi(x) \pmod p$ nicht durch $\varphi(x)$ teilbar ist. Daraus folgt aber weiter aus dem Satze von Schönemann (Kap. I, § 3), daß für alle α auch eine Zerlegung

$$F(x) \equiv \Pi(x)\, \Phi(x) \pmod{p^\alpha}$$

bestehen muß, wobei

$$\Pi(x) \equiv \pi(x), \quad \Phi(x) \equiv \varphi(x)^e \pmod p$$

ist. Das Primideal $\mathfrak{p}_i$ entspricht also im Sinne des Hauptsatzes dem Faktor $\Phi(x)$, der $(\mathrm{mod}\, p^\alpha)$ für $\alpha > \varkappa$ irreduzibel werden muß. Aus

$$n_i = e_i f_i = e f_i$$

folgt dann sofort $e = e_i$, und man kann daher

$$\Phi(x) = \varphi(x)^{e_i} + p\, M(x)$$

setzen. Nach dem Hauptsatze wird auch die Zahl $\Phi(\omega)$ durch beliebig hohe, nur von α abhängige Potenzen von $\mathfrak{p}_i$ teilbar, und daraus folgt leicht, daß die Zahl $M(\omega)$ nicht durch $\mathfrak{p}_i$ teilbar ist, d. h. $M(x)$ ist $(\mathrm{mod}\, p)$ nicht durch $\varphi(x)$ teilbar. Man kann dies folgendermaßen ausdrücken:

Satz 3. *Es sei* ω *eine ganze Körperzahl, welche der Gleichung* $F(x) = 0$ *genügt. Man kann dann* ω *so bestimmen, daß für ein bestimmtes Primideal* $\mathfrak{p}_i$ *der entsprechende irreduzible Faktor* $F_i(x)$ *von* $F(x) \pmod{p^\alpha}$ *die Form*

$$F_i(x) = \varphi(x)^{e_i} + p\, M(x)$$

---

[6]) Man sehe z. B. D. Hilbert, Zahlenbericht § 9. Jahresber. d. Deutschen Mathematikervereinigung **4** (1894).

erhält, wobei $\varphi(x) \pmod p$ *eine Primfunktion* f_i*-ten Grades ist,* $M(x) \pmod p$ *nicht durch* $\varphi(x)$ *teilbar ist, und weiter die übrigen irreduziblen Faktoren* $F_j(x)$ $(j \neq i)$ *von* $F(x)$ *nicht* $\pmod p$ *durch* $\varphi(x)$ *teilbar sind.*

An einer späteren Stelle werde ich zeigen, wie man im vorgelegten Falle wirklich eine solche Zahl ω finden kann. Aus den Eigenschaften von ω folgt sofort, daß man das Primideal $\mathfrak{p}_i$ immer in der Normalform

$$\mathfrak{p}_i = (p, \varphi(\omega))$$

darstellen kann.

Man sieht nun leicht ein, da $\varphi(\omega)$ nur die erste Potenz von $\mathfrak{p}_i$ enthält, daß die Zahlen

$$\omega^r \varphi(\omega)^s \qquad (r = 0, 1, \ldots, f_i - 1;\ s = 0, 1, \ldots, e_i - 1)$$

ein Fundamentalsystem für die Potenzen von $\mathfrak{p}_i$ bilden, d. h. jede Körperzahl ist $(\bmod p_i^a)$ kongruent einem linearen Ausdrucke mit ganzen rationalen Koeffizienten von diesen Zahlen. Daher ist jede Körperzahl $(\bmod p_i^a)$ kongruent einer Ringzahl, d. h. der Partialführer des Ringes $R(\omega)$ in bezug auf $\mathfrak{p}_i$ ist gleich dem Einheitsideal.

Aus Satz 3 folgt weiter, daß alle charakteristischen Zahlen in bezug auf $\mathfrak{p}_i$ verschwinden, es ist also

$$\gamma_{i1} = \cdots = \gamma_{i,i-1} = \gamma_{i,i+1} = \cdots = \gamma_{i,r} = 0,$$

woraus nach (12) $\gamma_i = 0$ folgt. Aus den Sätzen 2 und 3 schließt man dann weiter, daß der Führer $\mathfrak{f}$ von $R(\omega)$ nicht durch $\mathfrak{p}_i$ teilbar ist, woraus nach (5) sofort der bekannte Satz folgt:

Die Körperdifferente ist der größte gemeinsame Faktor von den Differenten der Zahlen des Körpers.

Man kann auch in jedem Körper eine solche Zahl Θ bestimmen, daß alle Partialführer $\mathfrak{f}_{\mathfrak{p}_i}$ Einheitsideale werden. Denn es ist zunächst möglich, Θ so zu bestimmen [7]), daß für alle i die Zahl $\varphi_i(\Theta)$ genau durch die erste Potenz von $\mathfrak{p}_i$ teilbar wird, wobei allgemein $\varphi_i(x) \pmod p$ eine Primfunktion vom Grade f_i ist. Diese Primfunktion kann übrigens beliebig gewählt werden, wenn sie nur vom Grade f_i ist. Der entsprechende

[7]) Unter Anwendung der Methode, die ich in meiner Arbeit: Weitere Untersuchungen zur Theorie der algebraischen Körper, Acta Math. **45** (1924), S. 145—160 benutzt habe, zeigt man leicht die Richtigkeit des folgenden Hilfssatzes, den ich auch später anwenden werde:

Man kann immer eine solche Zahl ω des Körpers bestimmen, daß eine Zahl $\varphi_i(\omega)$ genau durch $\mathfrak{p}_i^{h_i}$ teilbar wird. Dabei bedeutet $\varphi_i(x)$ eine Primfunktion $(\bmod p)$ f_i-ten Grades, und die $\varphi_i(x)$ können, wenn mehrere Primideale von demselben Grade f_i existieren, beliebig, gleich oder verschieden unter den Primfunktionen f_i-ten Grades gewählt werden. Die Zahlen h_i können beliebig gewählt werden.

Faktor $f_i(x)$ von $f(x)$ muß dann $(\mathrm{mod}\, p)$ durch $\varphi_i(x)$ teilbar sein, und aus dem Hauptsatze folgt leicht

$$f_i(x) \equiv \varphi_i(x)^{e_i} \,(\mathrm{mod}\, p),$$

also

$$f_i(x) = \varphi_i(x)^{e_i} + p\, M_i(x).$$

Genau wie früher folgt hier, daß $M_i(x)\,(\mathrm{mod}\, p)$ nicht durch $\varphi_i(x)$ teilbar sein kann. Da nun $\varphi_i(\Theta)$ genau die erste Potenz von $\mathfrak{p}_i$ enthält, so bilden die Zahlen

$$\Theta^r \varphi_i(\Theta)^s \qquad (r = 0, 1, \ldots, f_i - 1;\ s = 0, 1, \ldots, e_i - 1)$$

ein Fundamentalsystem für die Potenzen von $\mathfrak{p}_i$, d. h. jede Körperzahl ist $(\mathrm{mod}\, \mathfrak{p}_i^{\alpha})$ kongruent einer Ringzahl $R(\Theta)$, und folglich ist $\mathfrak{f}_{\mathfrak{p}_i} = 1$. Im Falle $e_i = 1$ braucht man aber nicht vorauszusetzen, daß $\varphi_i(\Theta)$ genau die erste Potenz von $\mathfrak{p}_i$ enthält, um $\mathfrak{f}_{\mathfrak{p}_i} = 1$ zu machen; denn in diesem Falle enthält p genau die erste Potenz von $\mathfrak{p}_i$, so daß schon die Zahlen Θ^r $(r = 0, \ldots, f_i - 1)$ ein Fundamentalsystem bilden. Wenn daher $e_i = 1$ ist, braucht also die Bedingung $M(x) \not\equiv 0\ (\mathrm{modd}\, p, \varphi_i(x))$ nicht zu gelten.

Satz 4. *Man kann immer eine solche Zahl Θ bestimmen, daß $\mathfrak{f}_{\mathfrak{p}_i} = 1$ für alle Partialführer des Ringes $R(\Theta)$ wird. Die Gleichung $f(x) = 0$ der Zahl Θ hat dann die Form*

$$f(x) \equiv \prod_{i=1}^{r} (\varphi_i(x)^{e_i} + p\, M_i(x)) \,(\mathrm{mod}\, p^{\alpha}),$$

wobei $\varphi_i(x)$ eine Primfunktion vom Grade f_i ist, während $M_i(x)\,(\mathrm{mod}\, p)$ nicht durch $\varphi_i(x)$ teilbar ist, wenn $e_i > 1$ ist.

Dieser Satz gibt eine Normalform für die definierende Gleichung des Körpers; später soll noch eine andere Normalform angegeben werden.

Es folgt aus diesen Bemerkungen sofort ein Beweis des *Dedekindschen Kriteriums* für die sogenannten *gemeinsamen außerwesentlichen Diskriminantenteiler*. Es gibt bekanntlich Körper, wobei die Indizes k der Zahlen des Körpers alle einen gemeinsamen Teiler haben. Nun folgt leicht aus den Gleichungen (4), (5) und (6), daß

$$N\mathfrak{f} = k^2 \tag{13}$$

ist, und wenn daher k nicht durch die Primzahl p teilbar sein soll, muß zuerst $\mathfrak{f}_{\mathfrak{p}_i} = 1$ für alle Partialführer, d. h. $f(x)$ muß die Form des Satzes 4 haben. Nach Satz 2 müssen auch alle charakteristischen Zahlen der Primideale verschwinden, d. h. die Primfunktionen $\varphi_i(x)$ müssen alle $(\mathrm{mod}\, p)$ verschieden sein. Daher folgt:

Die Primzahl p ist dann und nur dann ein gemeinsamer außerwesentlicher Diskriminantenteiler, wenn von den Ungleichungen

$$r_f > g(f) \qquad (f = 1, 2, \ldots, n)$$

wenigstens eine erfüllt ist. Dabei bedeutet r_f die Anzahl der Primidealteiler von p vom Grade f, während $g(f)$ die Anzahl der verschiedenen Primfunktionen $(\mathrm{mod}\, p)$ *vom Grade f angibt.* Für die Zahl $g(f)$ hat man bekanntlich eine einfache Formel. Später werde ich noch einen Satz über gemeinsame außerwesentliche Diskriminantenteiler geben.

Es folgt auch weiter, daß eine Primzahl p nur dann kein Teiler des Index ist, wenn $f(x)$ die Form

$$f(x) = \varphi_1(x)^{e_1} \dots \varphi_r(x)^{e_r} + p\, M(x)$$

hat, wobei $M(x) (\mathrm{mod}\, p)$ nicht durch $\varphi_i(x)$ teilbar ist, wenn $e_i > 1$. Dann hat p die Primidealzerlegung

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}, \quad N\mathfrak{p}_i = p^{f_i},$$

wobei

$$\mathfrak{p}_i = (p, \varphi_i(\vartheta))$$

ist. Dies sind die Hauptresultate der Dedekindschen Arbeit: „Über den Zusammenhang zwischen der Theorie der Ideale und der höheren Kongruenzen“ [8]).

An einer späteren Stelle zeige ich, wie man immer die Primidealzerlegung von p bei gegebener Gleichung bestimmen kann.

§ 2.

Über die Abbildungskörper der Primideale.

Wenn man den Körper nicht durch die Zahl ϑ, sondern durch eine andere primitive Zahl ϑ_1 mit der Gleichung $F(x) = 0$ definiert, so bestehen wegen der Eindeutigkeit der Primidealzerlegung nach dem Hauptsatz gleichzeitig die beiden Zerlegungen

$$\begin{matrix} f(x) \equiv f_1(x) \dots f_r(x) \\ F(x) \equiv F_1(x) \dots F_r(x) \end{matrix} (\mathrm{mod}\, p^\alpha),$$

wobei $f_i(x)$ und $F_i(x) (\mathrm{mod}\, p^\alpha)$ irreduzible Funktionen vom selben Grade n_i sind. Weiter besteht zwischen $f_i(x)$ und $F_i(x)$ der Zusammenhang, daß

$$f_i(\vartheta) \equiv 0 (\mathrm{mod}\, \mathfrak{p}_i^{e_i(\alpha - \varrho')})$$
$$F_i(\vartheta_1) \equiv 0 (\mathrm{mod}\, \mathfrak{p}_i^{e_i(\alpha - \varrho'')})$$

ist, wobei $\varrho' \leqq \frac{\delta}{2}$ und entsprechend $\varrho'' \leqq \frac{\delta_1}{2}$, wenn die Diskriminante von $F(x)$ genau durch p^{δ_1} teilbar ist.

Es soll nun untersucht werden, wie sich ein Faktor $F_i(x)$ aus dem

[8]) Abhandlungen der Kgl. Gesellschaft d. Wissenschaften zu Göttingen 1878.

entsprechenden $f_i(x)$ ableitet. Nach § 1, Kap. II kann man immer ϑ_1 in der Form

$$k\,\vartheta_1 = a_0 + a_1\,\vartheta + \ldots + a_{n-1}\,\vartheta^{n-1}$$

annehmen, wobei alle a_i ganz rational sind. Da man weiter nur ϑ_1 für Moduln untersuchen soll, welche Potenzen von $\mathfrak{p}_i$ sind, so besteht auch sicher eine Kongruenz von der Form

$$p^{\varkappa}\vartheta_1 \equiv b_1 + b_2\,\vartheta + \ldots + b_{n_i}\,\vartheta^{n_i-1} \pmod{\mathfrak{p}^{e_i(\alpha-\varrho')}}.$$

Multipliziert man diese Kongruenz nacheinander mit $1, \vartheta, \ldots, \vartheta^{n_i-1}$ und reduziert alle Potenzen von ϑ größer als ϑ^{n_i-1} nach der Relation

$$f_i(\vartheta) = \vartheta^{n_i} + c_1\,\vartheta^{n_i-1} + \ldots + c_{n_i} \equiv 0 \pmod{\mathfrak{p}_i^{e_i(\alpha-\varrho')}},$$

so erhält man das folgende System von Kongruenzen

$$\left.\begin{aligned} p^{\varkappa}\vartheta_1 &\equiv a_1^{(1)} + a_2^{(1)}\,\vartheta + \ldots + a_{n_i}^{(1)}\,\vartheta^{n_i-1} \\ p^{\varkappa}\vartheta_1\,\vartheta &\equiv a_1^{(2)} + a_2^{(2)}\,\vartheta + \ldots + a_{n_i}^{(2)}\,\vartheta^{n_i-1} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ p^{\varkappa}\vartheta_1\,\vartheta^{n_i-1} &\equiv a_1^{(n_i)} + a_2^{(n_i)}\,\vartheta + \ldots + a_{n_i}^{(n_i)}\,\vartheta^{n_i-1} \end{aligned}\right\} \pmod{\mathfrak{p}_i^{e_i(\alpha-\varrho')}}.$$

Durch Elimination von ϑ erhält man dadurch die Kongruenz

$$\Delta(\vartheta_1) = \begin{vmatrix} a_1^{(1)} - p^{\varkappa}\vartheta_1, & a_2^{(1)}, & \ldots a_{n_i}^{(1)} \\ a_1^{(2)}, & a_2^{(2)} - p^{\varkappa}\vartheta_1, & \ldots a_{n_i}^{(2)} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_1^{(n_i)}, & a_2^{(n_i)}, & \ldots a_{n_i}^{(n_i)} - p^{\varkappa}\vartheta_1 \end{vmatrix} \equiv 0 \pmod{\mathfrak{p}_i^{e_i(\alpha-\varrho')}}.$$

Aus dieser Kongruenz folgt dann nach Satz 4, Kap. II, daß die Determinante $\Delta(x) \pmod{p^{\alpha-\varrho'-\varrho''-\varkappa_1}}$ durch $F_i(x)$ teilbar sein muß, und da $\varrho' \leqq \frac{\delta}{2}$, $\varrho'' \leqq \frac{\delta_1}{2}$, $\varkappa_1 \leqq \frac{\delta_1}{2}$ ist, so folgt leicht die Kongruenz

$$p^{n_i\varkappa}F_i(x) \equiv \Delta(x) \pmod{p^{\alpha-\delta-\delta_1}}.$$

Es folgt auch natürlich, daß im Polynom $\Delta(x)$ alle Koeffizienten durch $p^{n_i\varkappa}$ teilbar sein müssen; setzt man daher $p^{n_i\varkappa}\Delta_1(x) = \Delta(x)$, so kommt

$$F_i(x) \equiv \Delta_1(x) \pmod{p^{\alpha-t}},$$

wobei der Kürze wegen $t = \delta + \delta_1 + n_i\varkappa$ gesetzt worden ist.

Als Hilfsmittel bei den folgenden Untersuchungen führe ich nun eine neue algebraische Zahl $\vartheta^{(i)}$ ein, welche im allgemeinen nicht zum Körper K gehören wird. Man wählt α fest und oberhalb einer Grenze, welche später angegeben wird; die Zahl $\vartheta^{(i)}$ ist dann eine Wurzel der irreduziblen Gleichung

$$f_i(\vartheta^{(i)}) = 0,$$

und der aus $\vartheta^{(i)}$ gebildete Körper $K^{(i)}$ vom Grade n_i heißt der *Abbildungskörper des Primideals* $\mathfrak{p}_i$.

Ich führe weiter zwischen den Körpern K und $K^{(i)}$ eine Korrespondenz ein, indem man zu jeder Zahl

$$\vartheta_1 = R(\vartheta)$$

in K die Zahl

$$\vartheta_1^{(i)} = R(\vartheta^{(i)})$$

in $K^{(i)}$ zuordnet.

Bildet man nun die Gleichung $\Phi(x) = 0$, welcher die Zahl $\vartheta_1^{(i)}$ genügt, so folgt leicht nach derselben Methode, daß man $\Delta_1(\vartheta_1^{(i)}) = 0$ hat, woraus natürlich $\Delta_1(x) = \Phi(x)$ folgt. $\Delta_1(x)$ war nämlich $(\mathrm{mod}\, p^{\alpha-t})$ kongruent einer irreduziblen Funktion $F_i(x)$ und kann daher nicht $\Phi(x)$ als Teiler enthalten. Es folgt daher, daß, wenn die Zahl $\vartheta_1^{(i)}$ der Gleichung $\Phi(x) = 0$ genügt, so ist

$$\Phi(x) \equiv F_i(x) (\mathrm{mod}\, p^{\alpha-t}), \tag{14}$$

wobei $F_i(x)$ der Faktor des Primideals $\mathfrak{p}_i$ in der Gleichung $F(x) = 0$ der Zahl ϑ_1 ist.

Wählt man nun speziell für ϑ_1 eine Zahl ω, wofür der entsprechende Partialführer $f_{\mathfrak{p}_i}$ gleich dem Einheitsideale ist, so wird $F_i(x)$ nach Satz 3 die Form

$$F_i(x) = \varphi(x)^{e_i} + p\, M(x)$$

haben, wobei $M(x) (\mathrm{mod}\, p)$ nicht durch $\varphi(x)$ teilbar ist. Wenn daher in (14) $\alpha \geqq t + 2$ gewählt wird, so wird die zugeordnete Zahl $\omega^{(i)}$ der Gleichung $\Phi(x) = 0$ genügen, wobei auch

$$\Phi(x) \equiv \varphi(x)^{e_i} + p\, M(x) (\mathrm{mod}\, p^{\alpha-t})$$

ist. Daraus folgt sofort, daß die Primzahl p in $K^{(i)}$ die Primidealzerlegung

$$p = \mathfrak{p}^{(i)^{e_i}}, \quad N^{(i)}(\mathfrak{p}^{(i)}) = p^{f_i}$$

hat, wobei das Zeichen $N^{(i)}$ Normen in $K^{(i)}$ angibt. Die Zahl $\varphi(\omega^{(i)})$ ist weiter genau durch die erste Potenz von $\mathfrak{p}^{(i)}$ teilbar, wenn $e_i > 1$ ist, so daß die Zahlen

$$\omega^{(i)^r} \varphi(\omega^{(i)})^s \qquad (r = 0, 1, \ldots, f_i - 1;\ s = 0, 1, \ldots, e_i - 1)$$

oder auch

$$\omega^{(i)^r} \qquad (r = 0, 1, \ldots, n_i - 1)$$

ein Fundamentalsystem für die Potenzen von $\mathfrak{p}^{(i)}$ bilden, d. h. es besteht für jede Zahl $\Theta^{(i)}$ in $K^{(i)}$ eine Kongruenz

$$\Theta^{(i)} \equiv R(\omega^{(i)}) (\mathrm{mod}\, \mathfrak{p}_i^{(i)^{e_i(\alpha-t)}}), \tag{15}$$

wobei das Polynom $R(x)$ vom Grade kleiner als n_i ist.

Ebenso folgt leicht, daß die Zahlen

$$\omega^r \qquad (r = 0, 1, \ldots, n_i = 1)$$

in K ein Fundamentalsystem für die Potenzen von $\mathfrak{p}_i$ bilden und daß dann aus (15) die entsprechende Kongruenz

$$\Theta \equiv R(\omega) (\mathrm{mod}\, \mathfrak{p}^{e_i(\alpha - t)})$$

in K folgt. Ich untersuche nun, wann eine Zahl Θ in K genau durch eine Potenz $\mathfrak{p}_i^a$ teilbar ist. Man kann $a = e_i q + r$ schreiben, wobei $0 \leqq r < e_i$ ist, und es folgt leicht, daß $R(x)$ die Form

$$R(x) \equiv p^q \varphi(x)^r Q(x) (\mathrm{mod}\, p^{q+1})$$

haben muß, wobei $Q(x) (\mathrm{mod}\, p)$ nicht durch $\varphi(x)$ teilbar ist. Umgekehrt ist natürlich auch Θ genau durch $\mathfrak{p}_i^a$ teilbar, wenn $R(x)$ diese Form hat. Mehr allgemein sieht man ein, daß, wenn eine Kongruenz

$$\vartheta_1 \equiv \vartheta_2 (\mathrm{mod}\, \mathfrak{p}_i^a)$$

bestehen soll, wobei

$$\vartheta_1 \equiv R_1(\omega), \qquad \vartheta_2 \equiv R_2(\omega) (\mathrm{mod}\, \mathfrak{p}^{e_i(\alpha - t)}),$$

so muß man

$$R_1(x) - R_2(x) \equiv p^q \varphi(x)^r Q(x) (\mathrm{mod}\, p^{q+1})$$

haben. Genau das Entsprechende gilt aber für die Zahlen in $K^{(i)}$ in bezug auf ihre Teilbarkeit durch $\mathfrak{p}^{(i)}$, und man kann daher sagen:

Wenn eine Zahl Θ genau durch $\mathfrak{p}_i^a$, $a < e_i(\alpha - t)$, teilbar ist, so wird auch die entsprechende zugeordnete Zahl $\Theta^{(i)}$ genau durch $\mathfrak{p}^{(i)a}$ teilbar sein und umgekehrt.

Wenn in K eine Kongruenz

$$\vartheta_1 \equiv \vartheta_2 (\mathrm{mod}\, \mathfrak{p}_i^a) \qquad a < e_i(\alpha - t)$$

besteht, so besteht auch zwischen den zugeordneten Zahlen die entsprechende Kongruenz

$$\vartheta_1^{(i)} \equiv \vartheta_2^{(i)} (\mathrm{mod}\, \mathfrak{p}^{(i)a})$$

und umgekehrt.

Aus diesen Tatsachen über den Abbildungskörper kann man verschiedene andere Resultate ableiten.

Zunächst ist in $K^{(i)}$ der Führer der Zahl $\omega^{(i)}$ nicht durch $\mathfrak{p}^{(i)}$ teilbar und nach (5) folgt, daß die Differente $\delta^{(i)}$ von $K^{(i)}$ genau dieselbe Potenz von $\mathfrak{p}^{(i)}$ enthält, wie die Zahl $\Phi'(\omega^{(i)})$. Weiter ist in K der Führer der Zahl ω nicht durch $\mathfrak{p}_i$ teilbar und man zeigt dann leicht nach Satz 3, daß die Differente δ von K genau dieselbe Potenz von $\mathfrak{p}_i$ wie die Zahl $F_i'(\omega)$ enthält. Nach (14) folgt dann sofort, wenn man nur $\alpha - t$ hinreichend groß wählt:

Wenn die Differente des Abbildungskörpers $K^{(i)}$ genau durch $\mathfrak{p}^{(i)\Delta_i}$ teilbar ist, so wird die Differente von K genau durch $\mathfrak{p}_i^{\Delta_i}$ teilbar.

Wenn dann weiter die Körperdiskriminante von $K^{(i)}$ genau durch p^{d_i} teilbar ist, so folgt nach (6), daß

$$d_i = f_i \Delta_i$$

ist, und man sieht daher ein:

Die Körperdiskriminante von K ist genau durch

$$p^{\sum_{i=1}^{r} d_i}$$

teilbar.

Da die Diskriminante von $\vartheta^{(i)}$, also die Diskriminante von $f_i(x)$ nach den früheren Bezeichnungen durch p^{δ_i} teilbar war, so kann man nach (5), Kap. 2

$$\delta_i = 2\varkappa_i + d_i$$

setzen, wenn der Index von $\vartheta^{(i)}$ in $K^{(i)}$ genau durch $p^{\varkappa_i}$ teilbar ist. Es folgt nun leicht aus der Definition des Führers, daß, wenn der Partialführer $\mathfrak{f}_{\mathfrak{p}_i}$ von ϑ in K gleich $\mathfrak{p}_i^{\tau_i}$ ist, so wird der Führer $\mathfrak{f}_{\mathfrak{p}^{(i)}}$ von $\vartheta^{(i)}$ in $K^{(i)}$ gleich $\mathfrak{p}^{(i)\tau_i}$. Aus (13) folgt dann auch die Relation

$$2\varkappa_i = \tau_i f_i. \tag{16}$$

Man kann nun auch eine einfache Relation zwischen den charakteristischen Zahlen γ_{ij} und den Zahlen ϱ_{ij} ableiten. Die Zahl γ_{ij} war dadurch definiert, daß die Zahl $f_j(\vartheta)$ genau durch $\mathfrak{p}_i^{\gamma_{ij}}$ teilbar war; dann folgt aber auch, daß die Zahl $f_j(\vartheta^{(i)})$ im Abbildungskörper genau durch $\mathfrak{p}^{(i)\gamma_{ij}}$ teilbar wird. Die Zahl ϱ_{ij} war dagegen so definiert, daß die Resultante $R_{ij} = R(f_i(x), f_j(x))$ genau durch $\mathfrak{p}^{\varrho_{ij}}$ teilbar sein sollte. Da aber bekanntlich

$$R_{ij} = N^{(i)}(f_j(\vartheta^{(i)}))$$

ist, so muß die Resultante genau durch $p^{f_i\gamma_{ij}}$ teilbar sein. Man hat also $\varrho_{ij} = f_i\gamma_{ij}$ und ebenso beweist man auch $\varrho_{ij} = f_j\gamma_{ji}$. Es ist daher bewiesen:

Satz 5. *Zwischen den charakteristischen Zahlen γ_{ij} und den Ordnungszahlen ϱ_{ij} der Resultanten $R(f_i(x), f_j(x))$ bestehen die Relationen*

$$\varrho_{ij} = f_i\gamma_{ij} = f_j\gamma_{ji}. \tag{17}$$

Ich beweise zuletzt einen wichtigen Satz über den Index. Nach (13) folgt nämlich, wenn man für den Führer $\mathfrak{f}_p$ den Ausdruck des Satzes 2 einsetzt, daß k^2 genau durch

$$p^{\Sigma\gamma_i f_i + \Sigma\tau_i f_i}$$

teilbar sein muß. Man hat daher nach (12) die Relation

$$2\varkappa = \sum_{i=1}^{r} \sum_{j=1}^{r} f_i \gamma_{ij} + \sum_{i=1}^{r} f_i \tau_i,$$

oder nach (16) und (17)

$$2\varkappa = \sum_{i=1}^{r} \sum_{j=1}^{r} \varrho_{ij} + 2 \sum_{i=1}^{r} \varkappa_i,$$

woraus sofort folgt:

Satz 6. *Der Index der Zahl ϑ ist genau durch $p^{\varkappa}$ teilbar, wobei*

$$\varkappa = \sum_{i>j} \varrho_{ij} + \sum_{i=1}^{r} \varkappa_i.$$

Hier bedeutet ϱ_{ij} die Ordnungszahl der Resultante $R(f_i(x), f_j(x))$, während $\varkappa_i$ die Ordnungszahl des Index des Abbildungkörpers von $\mathfrak{p}_i$ ist.

Führt man hier die in Kap. 1 angewandte Zahl ϱ' ein, so ist also

$$\varkappa = \varrho' + \sum_{i=1}^{r} \varkappa_i,$$

woraus sofort $\varkappa \geqq \varrho'$ kommt.

§ 3.

Bestimmung der Körperdifferente und Körperdiskriminante.

Es sei ω eine Zahl, wofür der entsprechende Führer nicht durch $\mathfrak{p}_i$ teilbar ist. Nach Satz 3 hat dann die entsprechende Gleichung die Form

$$F(x) \equiv Q(x) F_i(x) \pmod{p^{\alpha}}, \tag{18}$$

wobei

$$F_i(x) = \varphi(x)^{e_i} + p\, M(x)$$

und $Q(x) \pmod p$ nicht durch $\varphi(x)$ teilbar ist. Nach (5) wird dann die Zahl $F'(\omega)$ dieselbe Potenz von $\mathfrak{p}_i$ enthalten wie die Körperdifferente. Man hat nun nach (18)

$$F'(\omega) \equiv Q(\omega) F_i'(\omega) + Q'(\omega) F_i(\omega) \pmod{p^{\alpha}},$$

und da hier das letzte Glied durch $\mathfrak{p}_i^{e_i \alpha}$ teilbar ist, so folgt

$$F'(\omega) \equiv Q(\omega) F_i'(\omega) \pmod{\mathfrak{p}_i^{e_i \alpha}}.$$

Die Zahl $Q(\omega)$ ist aber nach der Voraussetzung nicht durch $\mathfrak{p}_i$ teilbar, und es folgt daher, daß die Zahl

$$F_i'(\omega) = e_i \varphi(\omega)^{e_i - 1} \varphi'(\omega) + p\, M'(\omega) \tag{19}$$

genau dieselbe Potenz von $\mathfrak{p}_i$ wie die Körperdifferente enthält. Wenn hier e_i nicht durch p teilbar ist, enthält $F_i'(\omega)$ genau die Potenz $\mathfrak{p}^{e_i - 1}$, indem $\varphi(\omega)$ genau durch die erste Potenz von $\mathfrak{p}_i$ teilbar ist. Wenn aber

e_i durch p teilbar ist, wird $F_i'(\omega)$ sicher durch $\mathfrak{p}_i^{e_i}$ oder eine höhere Potenz teilbar. Man hat daher den Dedekindschen Satz[9]):

Satz 7. *Die Körperdifferente ist genau durch $\mathfrak{p}_i^{e_i-1+\varrho_i}$ teilbar, wobei $\varrho_i = 0$, wenn e_i nicht durch p teilbar ist, während $\varrho_i \geqq 1$, wenn e_i durch p teilbar ist.*

Die Zahl ϱ_i soll die *Supplementzahl des Primideals* $\mathfrak{p}_i$ heißen. Man kann die Supplementzahl folgendermaßen einfach bestimmen: Man schreibt das Polynom $F_i'(x)$ in der Form

$$F_i'(x) = \sum_{s=0}^{e_i-1} A_s(x)\, p^{\alpha_s} \varphi(x)^s, \tag{20}$$

wobei der Grad von $A_s(x)$ kleiner als f_i ist, und weiter wird α_s so gewählt, daß $A_s(x) \not\equiv 0 \pmod{p}$ ist, wenn $A_i(x) \neq 0$. (Mit der Ausdrucksweise, welche später angewandt wird, kann man kurz sagen, daß man die Entwicklung $(p, \varphi(x))$ von $F_i'(x)$ bildet.)

Setzt man in (20) $x = \omega$, so wird ein Glied

$$A_s(\omega)\, p^{\alpha_s} \varphi(\omega)^s$$

genau durch $\mathfrak{p}_i^{e_i\alpha_s+s}$ teilbar. Zwei verschiedene Glieder in (20) können nicht durch dieselbe Potenz von $\mathfrak{p}_i$ teilbar sein, denn aus

$$e_i\alpha_s + s = e_i\alpha_r + r$$

folgt $s \equiv r \pmod{e_i}$, also $s = r$. Man hat daher bewiesen:

Satz 8. *Wenn R die kleinste unter den Zahlen*

$$e_i\alpha_s + s \qquad (s = 0, 1, \ldots, e_i - 1)$$

ist, so wird die Körperdifferente genau durch $\mathfrak{p}_i^R$ teilbar. Die Supplementzahl ϱ_i ist dann durch $\varrho_i = R - e_i + 1$ bestimmt.

Wenn für alle Primideale $\mathfrak{p}_i$ die Ordnungen e_i und Supplementzahlen ϱ_i bestimmt sind, so ist auch die Körperdiskriminante d bestimmt. Es folgt nämlich aus (6), daß d genau durch

$$p^{\sum_{i=1}^{r} f_i(e_i-1+\varrho_i)} \tag{21}$$

teilbar wird.

Es sollen nunmehr eingehend die Eigenschaften der Supplementzahlen ϱ_i untersucht werden. Diese Untersuchungen beruhen alle auf dem Hilfssatz:

---

[9]) R. Dedekind, Über die Diskriminanten endlicher Körper, Abhandlungen der Kgl. Gesellschaft d. Wissenschaften zu Göttingen 29 (1882).

Satz 9. *Es gibt kein Polynom $g(x)$, so daß $g'(x)$ die Form*

$$g'(x) \equiv p^a \varphi(x)^{kp^{a+1}-1} Q(x) \pmod{p^{a+1}} \tag{22}$$

hat, wobei $Q(x) \pmod p$ nicht durch $\varphi(x)$ teilbar ist.

Es sei nämlich θ eine Wurzel der Gleichung $\varphi(x) = 0$; im Körper $k(\theta)$ wird die Primzahl p unzerlegbar und selbst ein Primideal. Weiter wird

$$\varphi(x) = (x-\theta)\varphi'(\theta) + \frac{(x-\theta)^2}{2!}\varphi''(\theta) + \dots$$

und

$$Q(x) = Q(\theta) + (x-\theta)Q'(\theta) + \dots,$$

wobei die Zahlen $\varphi'(\theta)$ und $Q(\theta)$ nicht durch p teilbar sind. Setzt man diese Ausdrücke in (22) ein, erhält man für $g'(x)$ eine Entwicklung

$$g'(x) \equiv p^a \varphi'(\theta)^{kp^{a+1}-1} Q(\theta)(x-\theta)^{kp^{a+1}-1} + A_1(x-\theta)^{kp^{a+1}} + \dots \pmod{p^{a+1}},$$

und hier ist also der Koeffizient zu $(x-\theta)^{kp^{a+1}-1}$ nicht durch p^{a+1} teilbar. Entwickelt man aber auch $g(x)$ nach Potenzen von $x-\theta$, so kann das erste Glied in $g'(x)$ nur durch Differentiation eines Gliedes $B(x-\theta)^{kp^{a+1}}$ in $g(x)$ entstehen; dadurch erhält man aber offenbar immer ein durch p^{a+1} teilbares Glied.

Unter Anwendung dieses Hilfssatzes beweise ich zuerst die sogenannte Dedekind-Henselsche Ungleichung, welche eine obere Grenze für die Zahlen ϱ_i gibt. Wenn nämlich die Zahl e_i genau durch p^{s_i} teilbar ist, kann man $e_i = p^{s_i} e_i'$ setzen, und es gilt der Satz:

Satz 10. *Es ist*

$$\varrho_i \leqq s_i e_i. \tag{23}$$

Diese Ungleichung ist zuerst von Dedekind[10]) vermutet, später von Herrn Hensel[11]) bewiesen. Vereinfachte Beweise sind von Herrn Bauer[12]) geliefert worden. A. a. O.[13]) habe ich auch einen anderen einfachen Beweis von (23) gegeben; der folgende Beweis scheint mir aber der einfachst mögliche zu sein.

---

[10]) Man sehe die in [9]) zitierte Arbeit (Schlußbemerkung).

[11]) K. Hensel, Über die Entwicklung der algebraischen Zahlen in Potenzreihen, Math. Ann. **55** (1902) S. 301—336.

[12]) M. Bauer, Über die Differente eines algebraischen Zahlkörpers, Math. Ann. **83** (1921), S 74—76. M. Bauer, Verschiedene Bemerkungen über die Differente und Diskriminante eines algebraischen Zahlkörpers, Math. Zeitschr. **16** (1923), S. 1—12.

[13]) Man sehe die Arbeiten: Ö. Ore, Bemerkungen zur Theorie der Differente, Math. Zeitschr. **25** (1926), S. 1—8; Ö. Ore, Über die Bedeutung der Fundamentalgleichung in der Theorie der algebraischen Körper, Math. Ann. **95** (1925), S. 239—246.

Soll nämlich $\varrho_i > s_i e_i$ sein, so wird die Körperdifferente sicher durch $\mathfrak{p}_i^{e_i-1+s_i e_i+1} = \mathfrak{p}_i^{(s_i+1)e_i}$ teilbar, und man hat daher nach (19) die Kongruenz

$$F_i'(\omega) = e_i \varphi(\omega)^{e_i-1} \varphi'(\omega) + p M'(\omega) \equiv 0 \pmod{\mathfrak{p}_i^{(s_i+1)e_i}},$$

woraus, wie in § 2, leicht die identische Kongruenz

$$e_i \varphi(x)^{e_i-1} \varphi'(x) + p M'(x) \equiv 0 \pmod{p^{s_i+1}}$$

oder

$$M'(x) \equiv -e_i' p^{s_i-1} \varphi(x)^{e_i' p^{s_i}-1} \varphi'(x) \pmod{p^{s_i}}$$

folgt. Diese Kongruenz ist aber nach Satz 9 nicht möglich, wodurch (23) bewiesen ist.

Ich untersuche weiter, welche Zahlen ϱ_i, wofür $1 \leqq \varrho_i \leqq s_i e_i$ wirklich als Supplementzahlen vorkommen können, wenn die Ordnung e_i des Primideals $\mathfrak{p}_i$ gegeben ist. Man beweist dann den Satz:

Satz 11. *Es sei ϱ_i eine Zahl, wofür $1 \leqq \varrho_i \leqq s_i e_i$. Es gibt dann immer solche Körper n-ten Grades, daß die Körperdifferente genau durch $\mathfrak{p}_i^{e_i-1+\varrho_i}$ teilbar ist, außer wenn ϱ_i die folgenden Ausnahmewerte annimmt:*

$$(24)\quad \begin{cases} & p, & 2p, \ldots, & e_i - p, \\ e_i, & e_i + p^2, & e_i + 2p^2, \ldots, & 2e_i - p^2, \\ 2e_i, & 2e_i + p^3, & 2e_i + 2p^3, \ldots, & 3e_i - p^3, \\ \cdots & \cdots & \cdots & \cdots \\ (s_i-1)e_i, & (s_i-1)e_i + p^s, & (s_i-1)e_i + 2p^s, \ldots, & s_i e_i - p^s. \end{cases}$$

Es folgt zunächst leicht, daß ϱ_i den maximalen Wert $s_i e_i$ annehmen kann[14]); man braucht nämlich nur in (19) $M(x) = m$ zu setzen, wo m ganz rational ist. Dann ist $M'(x) = 0$ und daher die Körperdifferente genau durch $\mathfrak{p}_i^{e_i-1+s_i e_i}$ teilbar.

Wenn aber $\varrho_i < s_i e_i$ ist, so ist also in (19) das erste Glied durch $\mathfrak{p}_i^{e_i-1+s_i e_i}$ teilbar, und daher muß die Zahl $p M'(\omega)$ genau durch $\mathfrak{p}_i^{e_i-1+\varrho_i}$ teilbar sein, d. h. die Zahl $M'(\omega)$ wird genau durch $\mathfrak{p}_i^{\varrho_i-1}$ teilbar.

Wenn ϱ_i zu den Ausnahmezahlen (24) gehört, kann man

$$\varrho_i = \alpha e_i + k p^{\alpha+1}, \quad k p^{\alpha+1} < e_i$$

schreiben. Dann besteht also die Kongruenz

$$M'(\omega) \equiv 0 \pmod{\mathfrak{p}_i^{\varrho_i-1}},$$

[14]) Diese Tatsache ist schon von Herrn Bauer in seiner Arbeit: Verschiedene Bemerkungen über die Differente usw., Math. Zeitschr. **16** (1923), S. 1—12, bewiesen worden. Weiter ist auch bewiesen, daß $\varrho_i = 1$ sein kann; man sehe die Arbeit: M. Bauer, Bemerkungen zur Theorie der Differente, Acta litt. ac. scient. reg. univ. Hungaricae **1** (1923), S. 195—198.

woraus, wie in § 2 leicht folgt, daß $M'(x)$ die Form

$$M'(x) \equiv p^{\alpha}\varphi(x)^{kp^{\alpha+1}-1}Q(x) \pmod{p^{\alpha+1}}$$

haben muß, was nach Satz 9 nicht möglich ist.

Wenn aber ϱ_i nicht zu den Ausnahmezahlen gehört, kann man

$$\varrho_i = \alpha e_i + kp^{\beta}, \qquad \beta \leqq \alpha, \quad k \not\equiv 0 \pmod{p}$$

schreiben. Wird dann

$$M(x) = m + p^{\alpha-\beta}\varphi(x)^{kp^{\beta}} \tag{25}$$

gesetzt, so ist

$$M'(\omega) = p^{\alpha-\beta}kp^{\beta}\varphi(\omega)^{kp^{\beta}-1}\varphi'(\omega)$$

genau durch $\mathfrak{p}_i^{\alpha e_i + kp^{\beta}-1} = \mathfrak{p}_i^{\varrho_i - 1}$ teilbar.

Den Satz 11 kann man auch auf eine andere einfachere Form bringen.

Die Zahl $\varrho_i = s_i e_i$ ist, wie schon bemerkt, immer als Supplementzahl möglich. Wenn dagegen $1 \leqq \varrho_i < s_i e_i$ ist, dividiert man ϱ_i durch e_i:

$$\varrho_i = ae_i + b, \qquad 0 \leqq a < s_i, \qquad 0 \leqq b < e_i, \tag{26}$$

wobei also $a = \left[\frac{\varrho_i}{e_i}\right]$ wird, und wenn in diesem Falle die Zahl ϱ_i genau durch p^{r_i} teilbar ist, so folgt leicht aus Satz 11, daß sicher $r_i < s_i$ sein muß, wenn ϱ_i für das gegebene e_i als Supplementzahl möglich sein soll. Die Gleichung (26) zeigt dann, daß die Zahl b auch genau durch p^{r_i} teilbar wird. Die Ausnahmezahlen des Satzes 11 sind aber eben diejenigen Zahlen (26), wofür b durch eine höhere Potenz als p^a teilbar ist. Die notwendige und hinreichende Bedingung dafür, daß ϱ_i als Supplementzahl möglich ist, wird daher $r_i \leqq a = \left[\frac{\varrho_i}{e_i}\right]$.

Satz 12. *Es sei ϱ_i eine genau durch p^{r_i} teilbare Zahl, wofür $1 \leqq \varrho_i \leqq s_i e_i$ ist. Wenn dann ϱ_i in bezug auf e_i als Supplementzahl möglich ist, so ist entweder $\varrho_i = s_i e_i$ oder $1 \leqq \varrho_i < s_i e_i$, und in diesem Falle muß $r_i \leqq \left[\frac{\varrho_i}{e_i}\right]$ sein.*

§ 4.

Einige Existenzsätze für algebraische Körper.

Man kann unter Anwendung dieser Untersuchungen einige wichtige Existenztheoreme für algebraische Körper mit gegebenen Eigenschaften beweisen.

Satz 13. *Wenn zwei Systeme*

$$e_1, e_2, \ldots, e_r,$$
$$f_1, f_2, \ldots, f_r$$

von ganzen rationalen und positiven Zahlen so gegeben sind, daß

$$e_1 f_1 + e_2 f_2 + \ldots + e_r f_r = n$$

ist, so kann man immer einen solchen algebraischen Körper K n-ten Grades bestimmen, daß die Primzahl p in K die Primidealzerlegung

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_r^{e_r}, \qquad N\mathfrak{p}_i = p^{f_i}$$

hat[15]).

Man bestimmt bloß zu jedem Primideale eine Primfunktion $\varphi_i(x) \pmod p$ vom Grade f_i und bildet das Polynom

$$f_i(x) = \varphi_i(x)^{e_i} + p M_i(x), \tag{27}$$

wobei alle $M_i(x)$ voneinander verschieden sein sollen und $M_i(x) \pmod p$ nicht durch $\varphi_i(x)$ teilbar. Die Diskriminante des Produkts

$$\Pi(x) = f_1(x) f_2(x) \ldots f_r(x)$$

ist dann von Null verschieden und genau durch p^δ teilbar. Das Polynom

$$f(x) = \Pi(x) + p^{\delta+1} M(x)$$

zerfällt daher $(\mathrm{mod}\ p^{\delta+1})$ in die r-irreduziblen Faktoren $f_i(x)$, und die Gleichung $f(x) = 0$ definiert folglich den gewünschten Körper, wenn sie irreduzibel ist. Die Irreduzibilität von $f(x)$ erreicht man aber leicht dadurch, daß man $M(x)$ so wählt, daß $f(x)$ in bezug auf einer anderen Primzahl den Bedingungen des Eisensteinschen Irreduzibilitätssatzes genügt.

Es seien nun die Systeme e_i und f_i des Satzes 13 gegeben. Wenn dann weiter die Zahlen

$$\varrho_1, \varrho_2, \ldots, \varrho_r$$

so gegeben sind, daß $\varrho_i = 0$ ist, wenn e_i nicht durch p teilbar ist, während $1 \leqq \varrho_i \leqq s_i e_i$, wenn e_i genau durch p^{s_i} teilbar ist, ϱ_i soll aber in diesem Falle nicht zu den Ausnahmezahlen (24) gehören, so sage ich kurz, daß die Zahlen ϱ_i *in bezug auf p ein System von möglichen Supplementzahlen zu den Zahlen e_i bilden*. Es kann nun bewiesen werden:

---

[15]) Diesen Satz habe ich zuerst in meiner Arbeit: Zur Theorie der algebraischen Körper, Acta math. **44** (1923), S. 219—314, bewiesen. Man vgl. auch die Arbeit: Zur Theorie der Eisensteinschen Gleichungen, Math. Zeitschr. **20** (1924), S. 267—279. Ein Beweis desselben Satzes, aber auf Relativkörper erweitert, ist später von Herrn H. Hasse, Zwei Existenztheoreme über algebraische Zahlkörper, Math. Annalen **95** (1925), S. 229—238, gegeben worden. Man zeigt leicht, daß man mittels der hier gegebenen Untersuchungen dieselbe Erweiterung beweisen kann; diese Methode hat weiter den Vorteil, daß man *alle* Zahlkörper mit dieser Eigenschaft bestimmen kann; man vgl. die Note: Ö. Ore, Ein Problem von Dedekind, Acta litt. ac. scient. reg. univ. Hungaricae **2** (1924), S. 15—17.

Satz 14. *Es seien*

$$e_1, e_2, \ldots, e_r,$$
$$f_1, f_2, \ldots, f_r,$$
$$\varrho_1, \varrho_2, \ldots, \varrho_r$$

drei Systeme von Zahlen, wo $\sum_{i=1}^{r} e_i f_i = n$ *ist, und die Zahlen* ϱ_i *in bezug auf* p *ein mögliches System von Supplementzahlen zu den Zahlen* e_i *bilden. Man kann dann immer einen solchen Körper* K *n-ten Grades bestimmen, daß in* K *die Primzahl* p *die Primidealzerlegung*

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_r^{e_r}, \qquad N\mathfrak{p}_i = p^{f_i}$$

besitzt, und weiter die Körperdifferente von K *genau durch* $\mathfrak{p}_i^{e_i - 1 + \varrho_i}$ *teilbar ist.*

Die beiden letzten Sätze lassen sich einfach auf eine beliebige endliche Anzahl von Primzahlen ausdehnen. Die Richtigkeit des letzten Satzes folgt sofort dadurch, daß man in (27) für $M_i(x)$ nach (25) Ausdrücke von der Form

$$M_i(x) = m_i + p^{\alpha - \beta} \varphi(x)^{k p^{\beta}}$$

einsetzen kann.

Zuletzt soll noch ein Problem bei der Körperdiskriminante erwähnt werden. Nach (21) enthält die Körperdiskriminante von p genau die Potenz von dem Exponenten

$$\sum_{i=1}^{r} f_i (e_i - 1 + \varrho_i). \tag{28}$$

In diesem Ausdrucke können die Zahlen e_i und f_i beliebig variieren, wenn nur vorausgesetzt wird, daß der Grad des Körpers ungeändert gleich n, also $\sum_{i=1}^{r} e_i f_i = n$ ist, und weiter immer ϱ_i eine mögliche Supplementzahl zu e_i bildet. Es wird dann immer nach Satz 14 entsprechende Körper n-ten Grades geben, wofür die Körperdiskriminante genau diese Potenz von p enthält.

Ich habe für gegebene n und p den größten Wert des Ausdruckes (28) gesucht und zwar gefunden[16]):

Satz 15. *Man schreibt die Zahl* n *als* p*-adische Zahl*

$$n = a_1 p^{\alpha_1} + a_2 p^{\alpha_2} + \ldots + a_s p^{\alpha_s} \qquad (\alpha_1 > \alpha_2 > \ldots > \alpha_s),$$
$$p - 1 \geqq a_i \geqq 1.$$

[16]) Für den Beweis dieses Satzes verweise ich auf die Arbeit: Ö. Ore, Existenzbeweise in der Theorie der algebraischen Zahlkörper, Math. Zeitschr. **25** (1926), S. 474—489.

Die höchste Potenz von p, welche als Teiler der Diskriminante eines Zahlkörpers n-ten Grades vorkommt, hat dann den Exponent

$$N(n, p) = (\alpha_1 + 1)\, a_1 p^{\alpha_1} + (\alpha_2 + 1)\, a_2 p^{\alpha_2} + \ldots + (\alpha_s + 1)\, a_s p^{\alpha_s} - s.$$

Man zeigt leicht an Beispielen, daß nicht alle Zahlen unterhalb $N(n, p)$ wirklich als Diskriminantenexponenten vorkommen können. Es wäre von Interesse zu untersuchen, welche Zahlen überhaupt vorkommen, d. h. zu untersuchen, welche Werte der Ausdruck (28) unter den angegebenen Bedingungen annehmen kann.

(Eingegangen am 3. 11. 1925.)