BESTIMMUNG DER DIFFERENTE EINES ALGEBRAISCHEN ZAHLKÖRPERS.

Von

ÖYSTEIN ORE

in Oslo.

Inhaltsverzeichnis.

Einleitung.

In den früheren Arbeiten: „Zur Theorie der algebraischen Zahlkörper“ [1], „Weitere Untersuchungen zur Theorie der algebraischen Körper“ [2] und „Bestimmung der Diskriminante eines algebraischen Zahlkörpers“ [3] habe ich eine neue Methode in der Theorie der algebraischen Zahlkörper angegeben und zwar gezeigt, wie man für die zentralen Probleme der Körpertheorie eine einfache und besonders praktisch anwendbare Auflösung geben kann. Unter Anwendung der Newtonschen Polygone kann man für jede Primzahl die zugehörige Primidealzerlegung bestimmen, und weiter kann man für die Primzahl und alle ihre Primidealteiler einfache Fundamentalsysteme aufstellen. Daraus leitet man die Zusammensetzung der Körperdiskriminante ab, und erhält eine einfache Formel,

[1] Acta mathematica, Bd. 44. Diese Abhandlung wird im Folgenden mit A bezeichnet.
[2] Acta mathematica, Bd. 45. Diese Abhandlung wird im Folgenden mit B bezeichnet.
[3] Acta mathematica, Bd. 45. Diese Abhandlung wird im Folgenden mit C bezeichnet.

die auch für die sogenannten Ausnahmeprimzahlen richtig bleibt. Zuletzt bemerke ich, daß man auch für die große Klasse der regulären Gleichungen einfache Formeln für die Zusammensetzung des Index und der Gleichungsdiskriminante erhält.

Die vorliegende Arbeit bildet eine direkte Fortsetzung der Arbeit C, und ich wende die Bezeichnungen dieser Abhandlung an. Ich behandle erstens die Führer der natürlichen Ordnungen, d. h. Ringe, welche aus n algebraischen Zahlen

$$1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$$

gebildet sind. Unter Anwendung dieser Untersuchungen auf reguläre Gleichungen wird für jede solche Gleichung der zugehörige Führer bestimmt; der Führer wird nur von den geometrischen Verhältnissen der zugehörigen Polygone abhängig.

Aus der Bestimmung des Führers folgt dann auch die Zusammensetzung der *Körperdifferente*, indem ich in C die Gleichungsdifferente einer regulären Gleichung bestimmt habe.

Aus dieser Herleitung der Körperdifferente folgt natürlich auch ein neuer Beweis für den Dedekindschen Satz über die Äquivalenz der Körperdiskriminante mit der Norm der Körperdifferente. Es mag von theoretischem Interesse sein, daß dieser Beweis nicht auf der Anwendung der Theorie der komplementären Systeme beruht. Weiter gebe ich eine einfache Herleitung der Dedekind-Henselschen Ungleichheiten für die Primidealexponenten in der Zerlegung der Körperdifferente, wenn die zugehörige Primzahl zu den Ausnahmeprimzahlen gehört. Alle Beweise werden im vorgelegten Körper geführt; Hilfskörper, auch Galois'sche Körper, sind nicht erforderlich.

Ich habe hier immer nur algebraische Körper in Bezug auf den rationalen Bereich behandelt. Die Methode läßt sich aber ohne weiteres auf Relativkörper übertragen und man erhält für Relativkörper die entsprechenden Sätze über Primidealzerlegung, Relativdiskriminante und Relativdifferente.

§ 1. Fundamentalsysteme für die Multipla eines Ideals.

In der Arbeit C, Kap. I, § 1 habe ich *Fundamentalsysteme für Primzahlen und Primidealpotenzen definiert.* Für die folgenden Untersuchungen brauche ich den allgemeineren Begriff der *Fundamentalsysteme für die Multipla eines Ideals,* welcher hier definiert werden soll.

Es sei p eine Primzahl und $\mathfrak{p}$ ein Primideal f ten Grades, das in p aufgeht. Weiter seien

$$\omega_1, \omega_2, \ldots, \omega_f \tag{1}$$

f ganze Zahlen des Körpers, welche sämtlich durch das Ideal $\mathfrak{p}^r$ teilbar sein sollen. Ich sage dann, daß die Zahlen (1) ein *Fundamentalsystem für die Zahlen des Ideals* $\mathfrak{p}^r$ *in Bezug auf den Modul* $\mathfrak{p}^{r+1}$ bilden, wenn jede Zahl α des Ideals $\mathfrak{p}^r$ kongruent einer linearen Summe mit ganzen rationalen Koeffizienten von den Zahlen (1) ist, also

$$\alpha \equiv a_1\omega_1 + a_2\omega_2 + \cdots + a_f\omega_f \pmod{\mathfrak{p}^{r+1}}, \tag{2}$$

wo die Koeffizienten $a_i \pmod p$ eindeutig bestimmt sind. Die notwendige und hinreichende Bedingung dafür, daß die Zahlen (1) ein Fundamentalsystem für die Zahlen des Ideals $\mathfrak{p}^r$ in Bezug auf den Modul $\mathfrak{p}^{r+1}$ bilden, wird dadurch ausgedrückt, daß eine Kongruenz

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_f\omega_f \equiv 0 \pmod{\mathfrak{p}^{r+1}}$$

mit ganzen rationalen a_i nur dann bestehen kann, wenn

$$a_1 \equiv a_2 \equiv \cdots \equiv a_f \equiv 0 \pmod p$$

ist. Denn in diesem Falle erhält man, wenn man in (2) die Koeffizienten a_i vollständige Restsysteme $\pmod p$ unabhängig durchlaufen läßt, eben p^f verschiedene inkongruente Zahlen $\pmod{\mathfrak{p}^{r+1}}$ und es gibt auch im Ideale $\mathfrak{p}^r$ genau p^f verschiedene inkongruente Zahlen $\pmod{\mathfrak{p}^{r+1}}$.

Man bemerkt weiter leicht, daß wenn eine Zahl β durch $\mathfrak{p}$ genau in der Potenz $\mathfrak{p}^b$ teilbar ist, so bilden die Zahlen

$$\beta\omega_1, \beta\omega_2, \ldots, \beta\omega_f$$

ein Fundamentalsystem für die Zahlen des Ideals $\mathfrak{p}^{r+b}$ in Bezug auf den Modul $\mathfrak{p}^{r+b+1}$, indem nämlich aus einer Kongruenz

$$a_1\beta\omega_1 + a_2\beta\omega_2 + \cdots + a_f\beta\omega_f \equiv 0 \pmod{\mathfrak{p}^{r+b+1}}$$

notwendigerweise

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_f\omega_f \equiv 0 \pmod{\mathfrak{p}^{r+1}}$$

folgen würde. Eine solche Kongruenz ist aber nicht möglich, außer wenn alle Koeffizienten a_i durch p teilbar sind.

Es sei nun p genau durch $\mathfrak{p}^e$ teilbar. Ein System von ef Zahlen des Ideals $\mathfrak{p}^r$

$$\omega_1, \omega_2, \ldots, \omega_{ef} \tag{3}$$

soll dann ein *Fundamentalsystem für die Zahlen des Ideals* $\mathfrak{p}^r$ *in Bezug auf* $\mathfrak{p}$ heißen, wenn jede Zahl α in $\mathfrak{p}^r$ kongruent einer linearen Summe von diesen Zahlen mit ganzen rationalen Koeffizienten ist, also

$$\alpha \equiv a_1\omega_1 + a_2\omega_2 + \cdots + a_{ef}\omega_{ef} \pmod{\mathfrak{p}^{r+e}}, \tag{4}$$

wobei die Koeffizienten $a_i \pmod p$ eindeutig bestimmt sind. Man zeigt leicht, daß die notwendige und hinreichende Bedingung dafür, daß Zahlen (3) des Ideals $\mathfrak{p}_r$ ein Fundamentalsystem in Bezug auf $\mathfrak{p}$ für dieses Ideal bilden, dadurch ausgedrückt wird, daß eine Kongruenz

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_{ef}\omega_{ef} \equiv 0 \pmod{\mathfrak{p}^{r+e}}$$

nur dann bestehen kann, wenn die ganzen rationalen Koeffizienten a_i die Bedingung

$$a_1 \equiv a_2 \equiv \cdots \equiv a_{ef} \equiv 0 \pmod p$$

erfüllen.

Man kann nun weiter zeigen:

Satz 1. *Wenn die Zahlen* (3) *ein Fundamentalsystem für die Zahlen des Ideals* $\mathfrak{p}^r$ *in Bezug auf* $\mathfrak{p}$ *bilden, so besteht immer, wenn* M *eine beliebige ganze rationale Zahl ist, für jede Zahl* α *des Ideals eine Darstellung von der Form*

$$\alpha \equiv a_1\omega_1 + a_2\omega_2 + \cdots + a_{ef}\omega_{ef} \pmod{\mathfrak{p}^M},$$

wo alle Koeffizienten a_i *ganz rational sind.*

Nach (4) hat man nämlich

$$\alpha \equiv a_1^{(0)}\omega_1 + a_2^{(0)}\omega_2 + \cdots + a_{ef}^{(0)}\omega_{ef} + \beta_{r+e},$$

wo β_{r+e} zum Ideale $\mathfrak{p}^{r+e}$ gehört. Da nun, wie man einfach bemerkt, die Zahlen $p\omega_i$ ein Fundamentalsystem für das Ideal $\mathfrak{p}^{r+e}$ in Bezug auf $\mathfrak{p}$ bilden, kann man weiter

$$\beta_{r+e} = pa_1^{(1)}\omega_1 + pa_2^{(1)}\omega_2 + \cdots + pa_{ef}^{(1)}\omega_{ef} + \beta_{r+2e}$$

schreiben, wo alle $a_i^{(1)}$ ganz rational sind und β_{r+2e} zum Ideale $\mathfrak{p}^{r+2e}$ gehört. Fährt man so fort, erhält man im allgemeinen

$$\beta_{r+te} = p^t a_1^{(t)}\omega_1 + p^t a_2^{(t)}\omega_2 + \cdots + p^t a_{ef}^{(t)}\omega_{ef} + \beta_{r+(t+1)e}$$

woraus durch Addition

$$\alpha \equiv b_1\omega_1 + b_2\omega_2 + \cdots + b_{ef}\omega_{ef} \pmod{\mathfrak{p}^{r+(t+1)e}}$$

folgt, wo alle b_i ganz rational sind, und wo t beliebig groß gewählt werden kann, also sicher größer als eine beliebig bestimmte Zahl M.

Ein Fundamentalsystem für $\mathfrak{p}^r$ in Bezug auf $\mathfrak{p}$ kann in der folgenden Weise konstruiert werden. Man bildet für alle Ideale

$$\mathfrak{p}^r,\ \mathfrak{p}^{r+1},\ \ldots,\ \mathfrak{p}^{r+e-1}$$

entsprechende Fundamentalsysteme

$$(\mathrm{mod}\ \mathfrak{p}^{r+1}),\ (\mathrm{mod}\ \mathfrak{p}^{r+2}),\ \ldots,\ (\mathrm{mod}\ \mathfrak{p}^{r+e})$$

und bezeichnet diese mit

$$(5)\qquad \begin{cases} \omega_1, & \omega_2, & \ldots, \omega_f & (\mathfrak{p}^r), \\ \omega_{f+1}, & \omega_{f+2}, & \ldots, \omega_{2f} & (\mathfrak{p}^{r+1}), \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ \omega_{(e-1)f+1}, & \omega_{(e-1)f+2}, & \ldots, \omega_{ef} & (\mathfrak{p}^{r+e-1}). \end{cases}$$

Dann bildet die Gesamtheit der Zahlen (5) ein Fundamentalsystem für $\mathfrak{p}^r$ in Bezug auf $\mathfrak{p}$, denn eine Kongruenz

$$a_1\omega_1 + \cdots + a_f\omega_f + a_{f+1}\omega_{f+1} + \cdots + a_{ef}\omega_{ef} \equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{r+e})$$

kann nur dann bestehen, wenn alle a_i durch p teilbar sind. Man hat nämlich dann auch

$$a_1\omega_1 + \cdots + a_f\omega_f \equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{r+1}),$$

und folglich müssen $a_1, a_2, \ldots, a_f$ durch p teilbar sein. Daraus folgt weiter

$$a_{f+1}\omega_{f+1} + \cdots + a_{2f}\omega_{2f} \equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{r+2}),$$

und aus dieser Kongruenz folgt natürlich, daß $a_{f+1}, a_{f+2}, \ldots, a_{2f}$ alle durch p teilbar sein müssen, usw.

Es sei nun

$$\mathfrak{p} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_s^{e_s}, \quad N\mathfrak{p} = p^{f_i}$$

die Primidealzerlegung von p und weiter

$$(6)\qquad \mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\ldots\mathfrak{p}_s^{r_s}$$

ein Ideal, das keinen zu p relativ primen Idealteiler besitzt. Einige oder sogar alle Exponenten r_i dürfen gleich 0 sein. Ich sage dann, daß ein System von n Zahlen

$$(7)\qquad \eta_1,\ \eta_2,\ \ldots,\ \eta_n,$$

welche alle zum Ideale $\mathfrak{a}$ gehören, ein *Fundamentalsystem für die Zahlen des Ideals* $\mathfrak{a}$ *in Bezug auf* p bilden, wenn jede Zahl in $\mathfrak{a}$ kongruent einer linearen

Summe mit ganzen rationalen Koeffizienten von diesen Zahlen ist, also

$$\alpha \equiv a_1\eta_1 + a_2\eta_2 + \cdots + a_n\eta_n \pmod{\mathfrak{a}p}, \tag{8}$$

wobei die Koeffizienten $a_i \pmod p$ eindeutig bestimmt sind. Man bemerkt einfach, daß die notwendige und hinreichende Bedingung für ein solches Fundamentalsystem ist, daß eine Kongruenz

$$a_1\eta_1 + a_2\eta_2 + \cdots + a_n\eta_n \equiv 0 \pmod{\mathfrak{a}p} \tag{9}$$

nur dann bestehen kann, wenn alle Koeffizienten a_i durch p teilbar sind.

Es folgt weiter die Richtigkeit des folgenden Satzes:

Satz 2. *Wenn die Zahlen* (7) *ein Fundamentalsystem für die Zahlen des Ideals* $\mathfrak{a}$ *in Bezug auf* p *bilden, so besteht, wenn* M *eine beliebige ganze rationale Zahl bezeichnet, für jede Zahl* α *des Ideals eine Darstellung von der Form*

$$\alpha \equiv a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n \pmod{p^M},$$

wo alle Koeffizienten a_i *ganz rational sind.*

Aus (8) folgt nämlich

$$\alpha = a_1^{(0)}\eta_1 + a_2^{(0)}\eta_2 + \cdots + a_n^{(0)}\eta_n + p\alpha_1,$$

wo auch α_1 zu $\mathfrak{a}$ gehört. Dann kommt weiter

$$\alpha_1 = a_1^{(1)}\eta_1 + a_2^{(1)}\eta_2 + \cdots + a_n^{(1)}\eta_n + p\alpha_2,$$

wo α_2 zu $\mathfrak{a}$ gehört. Im allgemeinen erhält man

$$\alpha_t = a_1^{(t)}\eta_1 + a_2^{(t)}\eta_2 + \cdots + a_n^{(t)}\eta_n + p\alpha_{t+1},$$

woraus, wenn man diese Gleichungen bzw. mit $1, p, p^2, \ldots, p^t$ multipliziert und dann addiert, eine Gleichung von der Form

$$\alpha = b_1\eta_1 + b_2\eta_2 + \cdots + b_n\eta_n + p^{t+1}\alpha_{t+1}$$

folgt, wobei alle Koeffizienten b_i ganz rational sind, und der Exponent $t+1$ beliebig groß gewählt werden kann.

Kennt man für alle Teiler $\mathfrak{p}_i^{r_i}$ von $\mathfrak{a}$ entsprechende Fundamentalsysteme in Bezug auf $\mathfrak{p}_i$:

$$\omega_1^{(i)}, \omega_2^{(i)}, \ldots, \omega_{e_if_i}^{(i)},$$

so kann man einfach ein Fundamentalsystem für $\mathfrak{a}$ in Bezug auf p ableiten. Man bestimmt nämlich für alle i eine Zahl γ_i, welche nicht durch $\mathfrak{p}_i$ teilbar

ist, aber für alle $j \neq i$ soll γ_i durch $\mathfrak{p}_j^{r_j+e_j}$ teilbar sein. Dann gehören die Zahlen

$$\eta_{i,j} = \gamma_i \omega_j^{(i)} \quad (i = 1, 2, \ldots s,\ j = 1, 2, \ldots e_i f_i)$$

alle zum Ideale $\mathfrak{a}$ und bilden in der Tat ein Fundamentalsystem für die Zahlen in $\mathfrak{a}$ in Bezug auf p. Denn eine Kongruenz

$$\sum_{i,j} a_{i,j} \eta_{i,j} \equiv 0 \pmod{\mathfrak{a} p} \tag{10}$$

kann nur dann bestehen, wenn alle $a_{i,j}$ durch p teilbar sind. Aus (10) wird nämlich für alle i

$$\sum_{j=1}^{e_i f_i} a_{i,j} \eta_{i,j} \equiv 0 \pmod{\mathfrak{p}_i^{r_i+e_i}}$$

folgen, aber nach den Eigenschaften der $\eta_{i,j}$ müssen dann alle $a_{i,j}$ durch p teilbar sein.

Man kann die notwendige und hinreichende Bedingung für ein Fundamentalsystem für die Zahlen des Ideals $\mathfrak{a}$ in Bezug auf p etwas umformen. Es sei nämlich

$$\omega_1, \omega_2, \ldots, \omega_n$$

eine Basis des Ideals $\mathfrak{a}$. Dann bestehen Gleichungen von der Form

$$\left\{\begin{array}{l} \eta_1 = a_1^{(1)} \omega_1 + a_2^{(1)} \omega_2 + \cdots + a_n^{(1)} \omega_n \\ \cdots\cdots\cdots\cdots\cdots \\ \eta_n = a_1^{(n)} \omega_1 + a_2^{(n)} \omega_2 + \cdots + a_n^{(n)} \omega_n, \end{array}\right. \tag{11}$$

wo die Koeffizienten $a_i^{(j)}$ ganz rational sind. Die Diskriminante der n Basiszahlen ist von der speziellen Wahl der Basis unabhängig und bekanntlich gleich

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = (N\mathfrak{a})^2 d,$$

wobei d die Körperdiskriminante bezeichnet. Die Diskriminante $\Delta(\omega_1, \omega_2, \ldots \omega_n)$ werde ich die *Diskriminante des Ideals* nennen. Man zeigt dann leicht:

Satz 3. *Die notwendige und hinreichende Bedingung für ein Fundamentalsystem in Bezug auf p ist, daß die Diskriminante $\Delta(\eta_1, \eta_2, \ldots, \eta_n)$ durch genau dieselbe Potenz von p teilbar ist wie die Diskriminante des Ideals $\mathfrak{a}$.*

Aus (11) folgt nämlich die Beziehung

$$\Delta(\eta_1, \eta_2, \ldots, \eta_n) = |a_i^{(j)}|^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n),$$

und daraus nach der Bedingung, daß die Determinante $|a_i^{(j)}|$ nicht durch p teilbar sein kann. Soll aber eine Kongruenz von der Form (9) bestehen, so kann man darin die Werte (11) eintragen, und erhält

$$\begin{aligned}&(b_1 a_1^{(1)} + b_2 a_1^{(2)} + \cdots + b_n a_1^{(n)})\,\omega_1\\ &+ (b_1 a_2^{(1)} + b_2 a_2^{(2)} + \cdots + b_n a_2^{(n)})\,\omega_2\\ &+ \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad .\\ &+ (b_1 a_n^{(1)} + b_2 a_n^{(2)} + \cdots + b_n a_n^{(n)})\,\omega_n \equiv 0 \pmod{\mathfrak{a}p},\end{aligned}$$

und da die Zahlen ω_i eine Basis des Ideals $\mathfrak{a}$ bilden, bestehen auch die Kongruenzen

$$\begin{aligned}&b_1 a_1^{(1)} + b_2 a_1^{(2)} + \cdots + b_n a_1^{(n)} \equiv 0 \pmod{p}\\ &\quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad .\\ &b_1 a_n^{(1)} + b_2 a_n^{(2)} + \cdots + b_n a_n^{(n)} \equiv 0 \pmod{p},\end{aligned}$$

und die notwendige und hinreichende Bedingung für die Auflösbarkeit dieser Kongruenzen ist, daß die Determinante $|a_i^{(j)}|$ des Systems durch p teilbar ist.

Wenn man in diesen Untersuchungen für $\mathfrak{a}$ das Einheitsideal setzt, bilden die Zahlen (7) ein Fundamentalsystem in Bezug auf p für alle ganzen Zahlen des Körpers, wie ich dies in C, Kap. I, § 1 definiert habe.

§ 2. Bemerkungen über Führer.

Im folgenden werde ich mit $\mathfrak{o}$ den *Ring*

$$\mathfrak{o} = [1, \vartheta^2, \ldots, \vartheta^{n-1}]$$

bezeichnen, d. h. $\mathfrak{o}$ ist die Menge aller ganzen Zahlen η des Körpers, welche in der Form

$$\eta = a_0 + a_1\vartheta + a_2\vartheta^2 + \cdots + a_{n-1}\vartheta^{n-1}$$

mit ganzen rationalen Koeffizienten a_i geschrieben werden können.

Bekanntlich gibt es, wenn die Zahlen

$$1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$$

keine Basis des Körpers bilden, auch ganze Zahlen des Körpers, welche nicht zum Ringe $\mathfrak{o}$ gehören. Bezeichnet man aber mit $\mathfrak{g}$ die Gesamtheit aller ganzen Zahlen des Körpers, so gibt es solche Zahlen φ des Körpers, daß das Produkt von φ mit einer beliebigen Zahl aus $\mathfrak{g}$ immer eine Zahl des Ringes ist. Man sieht leicht ein, daß die Zahlen φ ein Ideal $\mathfrak{f}$ bilden, und daß alle Zahlen φ und also auch das Ideal $\mathfrak{f}$ zum Ringe gehört. Dieses Ideal wird nach Dedekind der *Führer des Ringes* genannt.

Zwischen der Differente $f'(\vartheta)$ von ϑ und dem Führer des entsprechenden Ringes besteht die leicht zu beweisende Relation

$$f'(\vartheta) = \mathfrak{f}.\mathfrak{d}, \tag{12}$$

wo das Ideal $\mathfrak{d}$ von der speziellen Wahl der Zahl ϑ unabhängig ist, und die *Körperdifferente* genannt wird. Im folgenden werde ich die Zusammensetzung des Führers untersuchen, und da ich früher (man sehe C, Kap. II, § 3) für die sogenannten *regulären* Gleichungen die vollständige Zusammensetzung der Differente $f'(\vartheta)$ ermittelt habe, folgt daraus auch die Zusammensetzung der Körperdifferente.

Ich gehe nun zu einem anderen Führerbegriff über, welcher für die folgenden Untersuchungen von Wichtigkeit ist. Es sollen alle Zahlen $\varphi_p^{(\alpha)}$ ermittelt werden, welche die folgende Eigenschaft besitzen: Wenn ω eine beliebige ganze Körperzahl ist, so besteht immer eine Kongruenz

$$\omega\,\varphi_p^{(\alpha)} \equiv R(\vartheta) \pmod{p^\alpha},$$

wobei $R(\vartheta)$ eine Zahl des Ringes ist. Die Zahlen $\varphi_p^{(\alpha)}$ bilden für ein beliebig fest gewähltes α ein Ideal $\mathfrak{f}_p^{(\alpha)}$. Denn wenn $\varphi_p^{(\alpha)}$ und $\psi_p^{(\alpha)}$ zur Menge $\mathfrak{f}_p^{(\alpha)}$ gehören, so hat auch $\varphi_p^{(\alpha)} \pm \psi_p^{(\alpha)}$ diese Eigenschaft, und wenn ω_1 eine beliebige ganze Körperzahl ist, so gehört auch $\omega_1 \varphi_p^{(\alpha)}$ zu $\mathfrak{f}_p^{(\alpha)}$. Denn man hat nach der Definition von $\varphi_p^{(\alpha)}$

$$\omega\,\omega_1\,\varphi_p^{(\alpha)} \equiv R_1(\vartheta) \pmod{p^\alpha},$$

wo $R_1(\vartheta)$ zum Ringe gehört, wie auch ω gewählt wird.

Das Ideal $\mathfrak{f}_p^{(\alpha)}$ soll als *Partialführer in Bezug auf den Modul* p^α bezeichnet werden.

$\mathfrak{f}_p^{(\alpha)}$ hängt natürlich von α ab. Man kann aber beweisen, daß $\mathfrak{f}_p^{(\alpha)}$ von α unabhängig ist, wenn α oberhalb einer bestimmten endlichen Grenze liegt.

Es sei nämlich

$$\omega_1,\ \omega_2,\ \ldots,\ \omega_n$$

eine Basis des Körpers, und es sei weiter k der Index der Zahl ϑ. Dann folgt nach A, Kap. 3, § 4, daß die Zahlen

$$k\omega_1,\ k\omega_2,\ \ldots,\ k\omega_n$$

immer Zahlen des Ringes sind, und wenn ω eine beliebige ganze Körperzahl bezeichnet, so ist folglich $k\omega$ sicher eine Zahl des Ringes.

Wenn daher k nicht durch p teilbar ist, kann man eine solche Zahl l bestimmen, daß

$$kl \equiv 1 \pmod{p^\alpha}$$

ist, und daraus folgt

$$\omega \equiv k\omega . l \equiv l . R(\vartheta) \pmod{p^\alpha},$$

also ω immer kongruent einer Zahl des Ringes $(\mathrm{mod}\, p^\alpha)$. Man hat also in diesem Falle $\mathfrak{f}_p^{(\alpha)} = 1$, und es gibt daher nur endlich viele Primzahlen, nämlich solche, welche Teiler von k sind, wofür $\mathfrak{f}_p^{(\alpha)}$ vom Einheitsideale verschieden sein kann.

Wenn nun k genau durch die Potenz p^ϱ teilbar ist, so werde ich zeigen, daß man immer, wenn $\alpha > \varrho$ gewählt wird,

$$\mathfrak{f}_p^{(\alpha)} = \mathfrak{f}_p^{(\varrho)}$$

hat. Dies folgt, indem man zeigt: wenn eine ganze Zahl ω einer Kongruenz

$$\omega \equiv P_\varrho(\vartheta) \pmod{p^\varrho} \tag{13}$$

genügt, so gibt es immer auch eine Zahl $P_\alpha(\vartheta)$ des Ringes, so daß

$$\omega \equiv P_\alpha(\vartheta) \pmod{p^\alpha} \qquad \alpha > \varrho$$

ist. Setzt man

$$k = k_1 p^\varrho,$$

wo k_1 zu p relativ prim ist, und schreibt man nach (13)

$$\omega - P_\varrho(\vartheta) = p^\varrho \Omega,$$

wo Ω eine ganze Zahl ist, so folgt durch Multiplikation mit k_1

$$k_1\omega - k_1 P_\varrho(\vartheta) = k\Omega, \tag{14}$$

wo nach einer früheren Bemerkung $k\Omega = Q(\vartheta)$ eine Zahl des Ringes ist. Bestimmt man weiter eine ganze rationale Zahl l_1, so daß

$$k_1 l_1 \equiv 1 \pmod{p^\alpha},$$

so folgt, wenn man (14) mit l_1 multipliziert,

$$\omega \equiv k_1 l_1 \omega \equiv P_\varrho(\vartheta) + l_1 Q(\vartheta) \pmod{p^\alpha},$$

w. z. b. w.

Das von α unabhängige Ideal

$$\mathfrak{f}_p = \mathfrak{f}_p^{(\varrho)} = \mathfrak{f}_p^{(\alpha)}, \qquad \alpha > \varrho$$

soll der *Partialführer des Ringes in Bezug auf* p heißen. Wie man sieht, sind alle anderen Partialführer $\mathfrak{f}_p^{(\alpha)}$ Teiler von $\mathfrak{f}_p$.

Es soll zugleich bemerkt werden, daß $\mathfrak{f}_p$ durch keine anderen Primideale teilbar sein kann, als solche, welche auch in p vorkommen. Denn schreibt man

$$\mathfrak{f}_p = \mathfrak{f}'_p \mathfrak{h}_p, \tag{15}$$

wo $\mathfrak{f}'_p$ nur Primideale enthält, welche in p aufgehen und $\mathfrak{h}_p$ zu p relativ prim ist, so kann man eine solche Potenz p^α, $\alpha \geqq \varrho$ bestimmen, daß $\mathfrak{f}'_p$ in p^α aufgeht. Dann ist $\mathfrak{f}'_p$ der größte gemeinsame Faktor von den Idealen $[p^\alpha]$ und $\mathfrak{f}_p$, und jede Zahl φ' von $\mathfrak{f}'_p$ kann dann als eine Summe von zwei Zahlen aus diesen Idealen geschrieben werden, also

$$\varphi' = \gamma p^\alpha + \varphi,$$

wo γ eine ganze Zahl ist und φ zum Ideale $\mathfrak{f}_p$ gehört. Daraus folgt aber einfach, daß für eine beliebige ganze Körperzahl ω stets

$$\omega\varphi' = \gamma . p^\alpha \omega + \omega\varphi \equiv \omega\varphi \pmod{p^\alpha}$$

ist, also $\omega\varphi'$ immer kongruent einer Zahl $\omega\varphi$ des Ringes. Alle Zahlen des Ideals $\mathfrak{f}'_p$, das umfassender als $\mathfrak{f}_p$ ist, sollten daher zum Partialführer in Bezug auf p gehören. Man muß folglich in (15) $\mathfrak{h}_p = 1$ und $\mathfrak{f}'_p = \mathfrak{f}_p$ haben.

Es soll nun der folgende wichtige Satz bewiesen werden:

Satz 4. *Der Führer* $\mathfrak{f}$ *des Ringes ist gleich dem Produkte aller Partialführer* $\mathfrak{f}_p$ *in Bezug auf* p, *indem* p *alle verschiedene Primzahlteiler des Index* k *des Ringes durchläuft; in Zeichen:*

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

Ich zeige erstens: wenn φ eine Zahl des Produktideals $\prod \mathfrak{f}_p$ ist, so ist $\omega\varphi$ immer eine Zahl des Ringes. Daraus folgt sofort, daß $\prod \mathfrak{f}_p$ durch den Führer $\mathfrak{f}$ teilbar sein muß.

Man hat, da φ auch zum Ideale $\mathfrak{f}_p$ gehört,

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

wo $\alpha > \varrho$ beliebig fest gewählt wird. Daraus folgt also

$$\omega\varphi = P_p(\vartheta) + p^\alpha \omega_p, \tag{16}$$

wo ω_p eine ganze Körperzahl ist. Da aber φ auch zum Ideale $\mathfrak{f}_q$ gehört, wenn q einen anderen Primzahlteiler von k bezeichnet, so ist in (16) $\omega\varphi$ auch kongruent einer Zahl des Ringes $(\mathrm{mod}\, q^\beta)$ und daraus folgt, daß $p^\alpha \omega_p$ und also auch ω_p kongruent einer Zahl des Ringes $(\mathrm{mod}\, q^\beta)$ ist. Man kann also

$$\omega_p = Q(\vartheta) + q^\beta \omega_{p,q}$$

setzen, wodurch (16) in

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

übergeht, wobei $P_{p,q}(\vartheta)$ eine Zahl des Ringes bezeichnet. Wenn daher

$$p,\ q,\ \ldots,\ r$$

die verschiedenen Primzahlen bezeichnen, welche in k aufgehen, so erhält man durch Fortsetzung dieser Methode

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

wobei $\alpha, \beta, \ldots, \gamma$ feste, beliebig groß wählbare Zahlen bezeichnen. Man kann aber diese Exponenten so groß wählen, daß $p^\alpha q^\beta \ldots r^\gamma$ durch k teilbar wird, woraus eine Darstellung

$$\omega\varphi = P_{p,q,\ldots,r}(\vartheta) + k\omega'$$

folgt, und hier ist nach einer früheren Bemerkung $k\omega'$ sicher eine Zahl des Ringes.

Ist aber andererseits φ eine Zahl des Führers $\mathfrak{f}$, so ist immer

$$\omega\varphi \equiv P(\vartheta)$$

und daher bestehen auch entsprechende Kongruenzen für den Modulu $p^\alpha, q^\beta, \ldots, r^\gamma$, d. h. φ muß auch zu allen Idealen $\mathfrak{f}_p, \mathfrak{f}_q, \ldots, \mathfrak{f}_r$ gehören, also ist auch $\mathfrak{f}$ durch das Produkt $\prod \mathfrak{f}_p$ teilbar. Der Satz 4 ist daher bewiesen.

Im Folgenden werde ich den Führer $\mathfrak{f}$ des Ringes bestimmen, und dies geschieht nach Satz 4 so, daß ich die Partialführer $\mathfrak{f}_p$ bestimme.

Ich erwähne zuletzt noch einen weiteren Führerbegriff. Es sei $\mathfrak{p}$ ein beliebiges Primideal, das in p aufgeht. Dann bilden alle Zahlen φ mit der Eigenschaft, daß eine Kongruenz

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

besteht, wobei ω eine beliebige ganze Körperzahl ist, ein Ideal $\mathfrak{f}_\mathfrak{p}^{(\alpha)}$. Dieses Ideal wird natürlich ein Teiler des Ideals $\mathfrak{f}_p^{(\alpha)}$. Weiter folgt, daß $\mathfrak{f}_\mathfrak{p}^{(\alpha)}$ von α unabhängig ist, wenn α oberhalb einer bestimmten Grenze liegt. Wenn nämlich p genau durch $\mathfrak{p}^e$ teilbar ist, so wird

$$\mathfrak{f}_\mathfrak{p} = \mathfrak{f}_\mathfrak{p}^{(e\varrho)} = \mathfrak{f}_\mathfrak{p}^{(\alpha)}, \qquad \alpha > e\varrho \tag{17}$$

und das Ideal $\mathfrak{f}_\mathfrak{p}$ soll der *Partialführer des Ringes in Bezug auf* $\mathfrak{p}$ heißen.

Die Richtigkeit von (17) ist bewiesen, wenn man zeigt, daß aus einer Kongruenz

(18) $$\omega\varphi \equiv P_{e\varrho}(\vartheta) \pmod{\mathfrak{p}^{e\varrho}}$$

auch eine Kongruenz

$$\omega\varphi \equiv P_{\alpha}(\vartheta) \pmod{\mathfrak{p}^{\alpha}} \qquad (\alpha > e\varrho)$$

abgeleitet werden kann. Man hat nun

$$k = \mathfrak{p}^{e\varrho}\mathfrak{a},$$

wo das Ideal $\mathfrak{a}$ nicht durch $\mathfrak{p}$ teilbar ist. Daher kann man immer eine solche Zahl ψ bestimmen, daß die Kongruenzen

$$\psi \equiv 1 \pmod{\mathfrak{p}^{\alpha}},$$
$$\psi \equiv 0 \pmod{\mathfrak{a}}$$

erfüllt sind. Wenn man dann nach (18)

$$[\omega\varphi - P_{e\varrho}(\vartheta)] = \mathfrak{p}^{e\varrho}\mathfrak{b}$$

schreibt, so folgt, wenn man mit ψ multipliziert,

$$[\psi(\omega\varphi - P_{e\varrho}(\vartheta))] = \mathfrak{p}^{e\varrho}\mathfrak{a}\mathfrak{c}$$

oder

$$\psi(\omega\varphi - P_{e\varrho}(\vartheta)) = k\omega_1 = Q(\vartheta),$$

woraus

$$\omega\varphi \equiv P_{e\varrho}(\vartheta) + Q(\vartheta) \pmod{\mathfrak{p}^{\alpha}}$$

folgt.

Weiter beweist man, daß $\mathfrak{f}_{\mathfrak{p}}$ keine andere Primideale als $\mathfrak{p}$ enthalten kann, d. h. der Partialführer in Bezug auf $\mathfrak{p}$ ist gleich einer Potenz von $\mathfrak{p}$. Wäre nämlich

$$\mathfrak{f}_{\mathfrak{p}} = \mathfrak{p}^{s}\mathfrak{q},$$

so wäre $\mathfrak{p}^{s}$ der größte gemeinsame Faktor von $\mathfrak{f}_{\mathfrak{p}}$ und einem Ideal $\mathfrak{p}^{\alpha}$, wo $\alpha > e\varrho$ genügend groß gewählt wird. Man hätte daher für jede Zahl σ in $\mathfrak{p}^{s}$ eine Darstellung

$$\sigma = \varphi + \gamma$$

gefunden, wo φ und γ bzw. Zahlen aus $\mathfrak{f}_{\mathfrak{p}}$ und $\mathfrak{p}^{\alpha}$ sind. Daraus folgt aber immer $\sigma \equiv \varphi \pmod{\mathfrak{p}^{\alpha}}$, und jede Zahl σ würde also zum Führer $\mathfrak{f}_{\mathfrak{p}}$ gehören. Also muß $\mathfrak{q} = 1$ sein.

Zwischen den Partialführern $\mathfrak{f}_{\mathfrak{p}}$ und $\mathfrak{f}_{p}$ besteht ein gewisser Zusammenhang, den ich in einer späteren Arbeit über die allgemeinen Eigenschaften der Zahlenkörper behandeln werde.

§ 3. Untersuchung der Körperzahlen für einen Primidealpotenzmodul.

Ich werde in diesem Abschnitte die Körperzahlen in Bezug auf Moduln, speziell Primidealpotenzmoduln, untersuchen. U. a. werde ich angeben, wie man die in § 1 erwähnten Fundamentalsysteme wirklich aufstellen kann.

Es sei im folgenden ϑ eine ganze, algebraische Zahl, welche einer regulären Gleichung genügt. Die regulären Gleichungen in Bezug auf eine Primzahl sind in der Arbeit B, § 1 und C, Kap. I, § 2 definiert worden. Weiter habe ich in B die Existenz der regulären Gleichungen für jeden Körper nachgewiesen.

Es sollen hier die Bezeichnungen der Arbeit C angewandt werden. Das Primideal $\mathfrak{p}_j^{(i)}$ soll ein Primideal der i-ten Seite sein, d. h. p soll genau durch $\mathfrak{p}_j^{(i)\lambda_i}$ und $\varphi(\vartheta)$ genau durch $\mathfrak{p}_j^{(i)\varkappa_i}$ teilbar sein. Weiter sei

$$\Phi_j^{(i)}(x) = \varphi(x)^{\varepsilon_j^{(i)}\lambda_i} + a_{1,j}^{(i)}(x)\,p^{\overline{\frac{\varkappa_i}{\lambda_i}}}\varphi(x)^{\varepsilon_j^{(i)}\lambda_i - 1} + \cdots + a_{\varepsilon_j^{(i)}\lambda_i,\,j}^{(i)}(x)\,p^{\varepsilon_j^{(i)}\varkappa_i} \tag{19}$$

der Faktor in der Zerlegung von $f(x) \pmod{p^M}$, welcher dem Primideale $\mathfrak{p}_j^{(i)}$ entspricht. (Man sehe C, Satz 1 und Satz 5.) Wenn man den Exponenten M genügend groß wählt, kann man erreichen, daß die Zahl $\Phi_j^{(i)}(\vartheta)$ durch eine beliebig hohe (von M abhängige) Potenz von $\mathfrak{p}_j^{(i)}$ teilbar wird. (C, Satz 5.)

Im folgenden werde ich alle Indizes weglassen und schreibe für den Augenblick kurz $\mathfrak{p} = \mathfrak{p}_j^{(i)}$ und $\varepsilon = \varepsilon_j^{(i)}$. Dann ist $N\mathfrak{p} = \mathfrak{p}^{\varepsilon m}$, p wird durch $\mathfrak{p}^{\lambda}$ und $\varphi(\vartheta)$ durch $\mathfrak{p}^{\varkappa}$ genau teilbar. Weiter geht (19) in

$$\Phi(x) = \varphi(x)^{\varepsilon\lambda} + a_1(x)\,p^{\overline{\frac{\varkappa}{\lambda}}}\varphi(x)^{\varepsilon\lambda-1} + a_2(x)\,p^{\overline{\frac{2\varkappa}{\lambda}}}\varphi(x)^{\varepsilon\lambda-2} + \cdots + a_{\varepsilon\lambda}(x)\,p^{\varepsilon\varkappa} \tag{20}$$

über.

In C, Kap. I, § 5 habe ich ein Fundamentalsystem für alle Körperzahlen $(\mathrm{mod}\ \mathfrak{p})$ gebildet. Die εm ganzen Körperzahlen

$$N_{i-1}\vartheta^r,\quad N_{i-1}\vartheta^r\frac{\varphi(\vartheta)^{\lambda}}{p^{\varkappa}},\quad \cdots,\quad N_{i-1}\vartheta^r\frac{\varphi(\vartheta)^{(\varepsilon-1)\lambda}}{p^{(\varepsilon-1)\varkappa}} \tag{21}$$
$$r = 0, 1, \ldots, m-1$$

bilden nämlich ein solches System, d. h. jede ganze Körperzahl ist kongruent einer linearen Summe mit ganzen rationalen Koeffizienten von diesen Zahlen. Hier ist nach C, Satz 3

$$N_{i-1} = \prod(\mathfrak{d}) \frac{\Phi_1(\vartheta) \dots \Phi_{i-1}(\vartheta)}{p^{h_1+h_2+\cdots+h_{i-1}}}, \tag{22}$$

und diese Zahl ist ganz und zu $\mathfrak{p}$ relativ prim.

Aus (21) leitet man einfach ein Fundamentalsystem für die Zahlen eines Ideals $\mathfrak{p}^s$ in Bezug auf den Modul $\mathfrak{p}^{s+1}$ ab. Nach § 1 braucht man nämlich nur um dies zu erreichen, eine Körperzahl ω so zu bestimmen, daß ω genau durch $\mathfrak{p}^s$ teilbar ist, und dann alle Zahlen (21) mit ω zu multiplizieren.

Da $\varkappa$ zu λ relativ prim ist, kann man solche ganze rationale Zahlen x und y bestimmen, daß

$$x\varkappa + y\lambda = s \tag{23}$$

ist. Unter den Lösungen (x, y) dieser Gleichung kann man weiter eine solche (x_s, y_s) finden, daß $0 \leqq x_s < \lambda$ ist. Diese Lösung werde ich *die kleinste positive Lösung* x nennen. Dann sind alle anderen Lösungen von (23) in der Form

$$x = x_s + i\lambda, \quad y = y_s - i\varkappa$$

enthalten, wobei i eine ganze rationale Zahl ist. Für ein gegebenes ε werde ich die Lösungen

$$(x_s, y_s),\ (x_s+\lambda, y_s-\varkappa),\ (x_s+2\lambda, y_s-2\varkappa),\ \dots\ (x_s+(\varepsilon-1)\lambda, y_s-(\varepsilon-1)\varkappa) \tag{24}$$

als *die* ε *kleinsten positiven Lösungen* x bezeichnen. Dabei sind alle x positiv, unter den y können aber auch negative Werte vorkommen.

Die Zahl

$$\omega = N_{i-1}\varphi(\mathfrak{d})^{x_s} p^{y_s}$$

wird dann ganz und durch $\mathfrak{p}^s$ genau teilbar, was man analog wie in C, Kap. I, § 6 beweist. Der Faktor N_{i-1} ist hier zugesetzt, damit man eine ganze Zahl erhalte, indem y_s negativ sein kann.

Multipliziert man nun die Zahlen (21) mit ω, erhält man das System

$$N_{i-1}^2 \mathfrak{d}^r \varphi(\mathfrak{d})^{x_s} p^{y_s},\quad N_{i-1}^2 \mathfrak{d}^r \varphi(\mathfrak{d})^{x_s+\lambda} p^{y_s-\varkappa},\quad N_{i-1}^2 \mathfrak{d}^r \varphi(\mathfrak{d})^{x_s+2\lambda} p^{y_s-2\varkappa},\quad \dots,$$
$$N_{i-1} \mathfrak{d}^r \varphi(\mathfrak{d})^{x_s+(\varepsilon-1)\lambda} p^{y_s-(\varepsilon-1)\varkappa},$$

und diese Zahlen bilden also ein Fundamentalsystem für die Zahlen des Ideals, $\mathfrak{p}^s$ in Bezug auf den Modul $\mathfrak{p}^{s+1}$. Man kann aber dieses System etwas vereinfachen. N_{i-1} ist nämlich nicht durch $\mathfrak{p}$ teilbar, und folglich bilden auch die Zahlen

$$N_{i-1} \mathfrak{d}^r \varphi(\mathfrak{d})^{x_s} p^{y_s},\quad N_{i-1} \mathfrak{d}^r \varphi(\mathfrak{d})^{x_s+\lambda} p^{y_s-\varkappa},\quad \dots,\quad N_{i-1} \mathfrak{d}^r \varphi(\mathfrak{d})^{x_s+(\varepsilon-1)\lambda} p^{y_s-(\varepsilon-1)\varkappa}$$
$$(r = 0, 1, \dots, m-1)$$

ein solches Fundamentalsystem. Weiter sind die Exponenten

$$(x_s, y_s),\ (x_s+\lambda, y_s-\varkappa),\ \ldots (x_s+(\varepsilon-1)\lambda, y_s-(\varepsilon-1)\lambda)$$

eben gleich den Zahlen (24), so daß man einfach sagen kann:

Satz 5. *Die Zahlen*

$$N_{i-1}\vartheta^r\varphi(\vartheta)^a p^b, \qquad (r=0,1,\ldots,m-1) \tag{25}$$

wobei

$$a\varkappa+b\lambda = s \tag{26}$$

ist, und wo a die ε kleinsten positiven Lösungen dieser Gleichung durchläuft, bilden ein Fundamentalsystem für die Zahlen des Ideals $\mathfrak{p}^s$ in Bezug auf den Modul $\mathfrak{p}^{s+1}$.

Die Zahlen (25) gehören gewiß nicht zu dem von ϑ abgeleiteten Ringe, indem nach (22) N_{i-1} gleich einem Polynome in ϑ dividiert durch eine Potenz von p ist. Weiter wird auch in (25) die Zahl b negativ ausfallen können. Ich werde nun untersuchen, wann in einem Fundamentalsysteme (25) alle b nicht negativ sind. Diese Untersuchung kann man mittels einer geometrischen Hilfsbetrachtung sehr vereinfachen.

Bildet man nämlich die Zahl

$$\varphi(\vartheta)^a p^b$$

durch den Gitterpunkt (a, b) in einem rechtwinkligen Koordinatensysteme ab, so sieht man ein, daß die in (21) vorkommenden Glieder

$$1,\ \frac{\varphi(\vartheta)^\lambda}{p^\varkappa},\ \frac{\varphi(\vartheta)^{2\lambda}}{p^{2\varkappa}},\ \ldots,\ \frac{\varphi(\vartheta)^{(\varepsilon-1)\lambda}}{p^{(\varepsilon-1)\varkappa}}$$

durch die Punkte

$$(0,0),\ (\lambda,-\varkappa),\ (2\lambda,-2\varkappa),\ \ldots((\varepsilon-1)\lambda,-(\varepsilon-1)\varkappa)$$

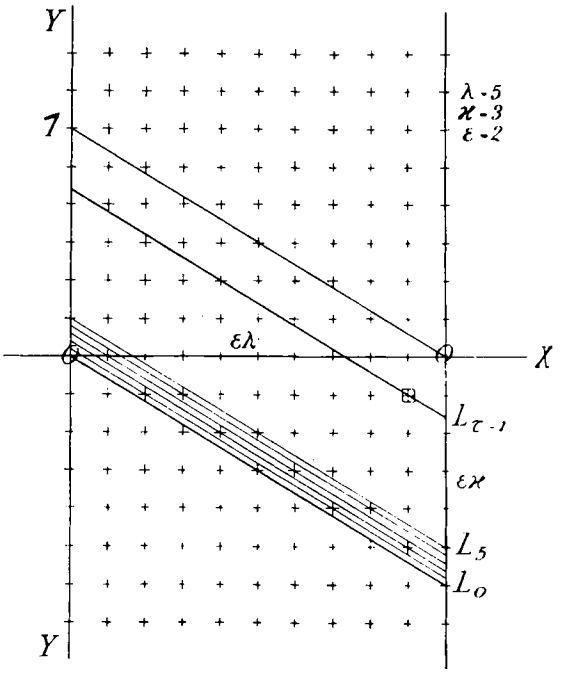
abgebildet werden. Diese liegen alle auf einer Geraden L_0, die durch den Anfangspunkt geht und die Neigungszahl $-\frac{\varkappa}{\lambda}$ hat. Teilt man nun jede Einheitsstrecke auf der positiven Y-Achse in λ Teile, und zieht man durch diese Teilpunkte Parallelen zu L_0, erhält man ein System von Geraden, welche ich mit $L_1, L_2, \ldots$ bezeichne. Diese Geraden teilen jede Einheitsstrecke der positiven X-Achse in $\varkappa$ Teilstrecken.

Man findet ohne Schwierigkeiten, daß die Gerade L_s die Gleichung

$$x\varkappa+y\lambda = s$$

hat, und folglich werden die Glieder $\varphi(\vartheta)^a p^b$, welche in (25) vorkommen, durch

Gitterpunkte auf L_s abgebildet. Da a die ε kleinsten positiven Lösungen dieser Gleichung (26) durchlaufen sollte, werden die entsprechenden Gitterpunkte innerhalb eines Streifens zwischen der Y-Achse und der Parallelen dazu in dem Abstand $\varepsilon\lambda$ liegen.



Es sollte nun untersucht werden, wann die Exponenten b in (25) positiv sind, d. h. wann die entsprechenden Gitterpunkte oberhalb der X-Achse liegen. Dies folgt aber leicht aus der Figur, indem die letzte Gerade L_s welche noch nicht ε Gitterpunkte oberhalb der X-Achse enthält, notwendigerweise durch den Punkt $(\varepsilon\lambda-1, -1)$ gehen muß, und folglich die Gleichung

$$x\varkappa + y\lambda = \varepsilon\varkappa\lambda - \varkappa - \lambda$$

hat. Wenn daher in Satz 5

$$s \geqq \varepsilon\varkappa\lambda - \varkappa - \lambda + 1$$

ist, werden alle $b \geqq 0$. Im folgenden werde ich der Kürze wegen

$$\tau = \varepsilon\varkappa\lambda - \varkappa - \lambda + 1 \tag{27}$$

setzen. Wenn also $s \geqq \tau$ ist, kann man in dem Fundamentalsysteme (25) die Zahl N_{i-1} weglassen, indem sie nicht durch $\mathfrak{p}$ teilbar ist.

Man kann daher sagen:

Satz 6. *Wenn*

$$s \geqq \tau = \varepsilon \varkappa \lambda - \varkappa - \lambda + 1$$

ist, so bilden die Zahlen

$$\vartheta^r \varphi(\vartheta)^a p^b, \qquad (r = 0, 1, \ldots, m-1)$$

wo

$$a\varkappa + b\lambda = s$$

ist, und wo a die ε kleinsten positiven Lösungen dieser Gleichung durchläuft, ein Fundamentalsystem für die Zahlen des Ideals $\mathfrak{p}^s$ in Bezug auf den Modul $\mathfrak{p}^{s+1}$.

Wenn also $s \geqq \tau$ ist, kann man für $\mathfrak{p}^s$ ein Fundamentalsystem (mod $\mathfrak{p}^{s+1}$) aufstellen, worin alle Basiszahlen zum Ringe $\mathfrak{o}$ gehören.

Wegen der späteren Anwendungen erwähne ich hier noch kurz, wie man allgemein die Potenz bestimmen kann, in welcher eine Zahl $\psi(\vartheta)$ des Ringes das Primideal $\mathfrak{p}$ enthält.

Man kann hier voraussetzen, daß der Grad von $\psi(x)$ kleiner als der Grad $\varepsilon\lambda m$ von $\Phi(x)$ ist. Denn sonst braucht man nur $\psi(x)$ durch $\Phi(x)$ zu dividieren und erhält

$$\psi(x) = \Phi(x)\, g(x) + r(x), \tag{28}$$

wo der Grad von $r(x)$ kleiner als der Grad von $\Phi(x)$ ist. Wenn nun $\psi(\vartheta)$ genau durch $\mathfrak{p}^\varrho$ teilbar ist, kann man, wenigstens theoretisch, erreichen, daß $\Phi(\vartheta)$ durch eine Potenz $\mathfrak{p}^\alpha$ teilbar wird, wo $\alpha > \varrho$ ist. Daher kommt nach (28)

$$\psi(\vartheta) \equiv r(\vartheta) \pmod{\mathfrak{p}^\alpha},$$

und die Zahlen $\psi(\vartheta)$ und $r(\vartheta)$ sind durch dieselbe Potenz von $\mathfrak{p}$ teilbar.

Um nun die Teilbarkeit einer Zahl $r(\vartheta)$ durch $\mathfrak{p}$ zu untersuchen, bilde ich die Entwicklung $(p, \varphi(x))$ von $r(x)$, also

$$r(x) = \sum Q_i(x)\, \varphi(x)^{\alpha_i} p^{\beta_i}, \tag{29}$$

wo

$$Q_i(x) \not\equiv 0 \ (\mathrm{modd}\, p, \varphi(x))$$

ist. Setzt man hier $x = \vartheta$, wird ein Glied $Q_i(\vartheta)\varphi(\vartheta)^{\alpha_i} p^{\beta_i}$ genau durch

$$\mathfrak{p}^{\alpha_i \varkappa + \beta_i \lambda}$$

teilbar. Ist nun ϱ die kleinste unter den Zahlen

$$\alpha_i \varkappa + \beta_i \lambda,$$

so werde ich zeigen, daß $r(\vartheta)$ genau durch $\mathfrak{p}^\varrho$ teilbar ist. Denn ist

$$\sum Q(\vartheta)\,\varphi(\vartheta)^\alpha p^\beta$$

die Summe derjenigen Glieder in (29), wofür $\alpha\varkappa+\beta\lambda=\varrho$ ist, kann diese Summe nicht durch eine höhere Potenz als $\mathfrak{p}^\varrho$ teilbar sein. Denn aus einer Kongruenz

$$\sum Q(\vartheta)\,\varphi(\vartheta)^\alpha p^\beta \equiv 0 \pmod{\mathfrak{p}^{\varrho+1}}$$

würde auch

$$\sum Q(\vartheta)\,N_{i-1}\,\varphi(\vartheta)^\alpha p^\beta \equiv 0 \pmod{\mathfrak{p}^{\varrho+1}}$$

folgen, was aber nicht möglich ist, indem nach Satz 5 die Zahlen

$$N_{i-1}\,\vartheta^\nu\,\varphi(\vartheta)^\alpha p^\beta$$

ein Fundamentalsystem für die Zahlen des Ideals $\mathfrak{p}^\varrho$ in Bezug auf den Modul $\mathfrak{p}^{\varrho+1}$ bilden. Man hat daher den Satz:

Satz 7. *Es sei der Grad des Polynoms $r(x)$ kleiner als der Grad von $\Phi(x)$, und die Entwicklung $(p, \varphi(x))$ von $r(x)$ sei durch*

$$r(x) = \sum Q_i(x)\,\varphi(x)^{\alpha_i} p^{\beta_i}$$

gegeben. Dann ist $r(\vartheta)$ genau durch $\mathfrak{p}^\varrho$ teilbar, wenn ϱ die kleinste unter den Zahlen $\alpha_i\varkappa+\beta_i\lambda$ ist.

§ 4. Bestimmung des Partialführers in Bezug auf $\mathfrak{p}$.

In Satz 6 ist gezeigt worden, wie jede Zahl des Ideals $\mathfrak{p}^s$, wo

$$s \geqq \varepsilon\varkappa\lambda-\varkappa-\lambda+1$$

ist, kongruent einer Zahl des Ringes $(\mathrm{mod}\,\mathfrak{p}^{s+1})$ ist. Nach § 1 kann man ein Fundamentalsystem für $\mathfrak{p}^s$ in Bezug auf $\mathfrak{p}$ aufstellen, indem ein solches Fundamentalsystem einfach aus den Fundamentalsystemen für die Ideale $\mathfrak{p}^s$, $\mathfrak{p}^{s+1}$, …, $\mathfrak{p}^{s+\lambda-1}$ in Bezug auf bzw. den Moduln $(\mathrm{mod}\,\mathfrak{p}^{s+1})\ldots(\mathrm{mod}\,\mathfrak{p}^{s+\lambda})$ zusammengesetzt ist. Daher wird jede Zahl, welche zum Ideale

$$\mathfrak{p}^\tau = \mathfrak{p}^{\varepsilon\varkappa\lambda-\varkappa-\lambda+1}$$

gehört, kongruent einer Zahl des Ringes für eine beliebig große Potenz $\mathfrak{p}^\alpha$ als Modul. Der Partialführer $\mathfrak{f}_\mathfrak{p}$ in Bezug auf $\mathfrak{p}$ ist daher $\mathfrak{p}^\tau$ oder eine niedrigere Potenz von $\mathfrak{p}$. Um nun

$$\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^\tau = \mathfrak{p}^{\varepsilon\varkappa\lambda-\varkappa-\lambda+1}$$

zu beweisen, braucht man nur zu zeigen, daß nicht alle Zahlen des Ideals $\mathfrak{p}^{\tau-1}$

Zahlen des Ringes kongruent sein können, wenn der Modul $\mathfrak{p}^\alpha$ hinreichend groß gewählt wird.

Wären nämlich alle Zahlen des Körpers, welche durch $\mathfrak{p}^{\tau-1}$ teilbar sind, kongruent Zahlen des Ringes (mod $\mathfrak{p}^\tau$), so müßte es unter den Zahlen des Ringes εm solche Zahlen

$$\psi_1(\vartheta),\ \psi_2(\vartheta),\ \ldots,\ \psi_{\varepsilon m}(\vartheta) \tag{30}$$

geben, die ein Fundamentalsystem für die Zahlen des Ideals in Bezug auf den Modul $\mathfrak{p}^\tau$ bilden. Dann könnte aber nach § 1 keine Kongruenz

$$a_1\psi_1(\vartheta)+a_2\psi_2(\vartheta)+\cdots+a_{\varepsilon m}\psi_{\varepsilon m}(\vartheta)\equiv 0 \pmod{\mathfrak{p}^\tau} \tag{31}$$

bestehen, wobei alle a_i ganz rational sind, außer wenn alle a_i durch p teilbar sind.

Ich werde aber zeigen, daß ein solches Fundamentalsystem (30) nicht möglich ist. Zunächst kann man voraussetzen, daß ein $\psi(\vartheta)$ in (30) einen Grad in ϑ hat, der kleiner als der Grad von $\Phi(\vartheta)$ ist. Denn wenn man $\psi(x)$ durch $\Phi(x)$ dividiert, erhält man

$$\psi(x) = \Phi(x)g(x)+r(x).$$

Wird hier $x=\vartheta$ gesetzt, so erhält man

$$\psi(\vartheta)\equiv r(\vartheta) \pmod{\mathfrak{p}^\tau},$$

indem man immer erreichen kann, daß $\Phi(\vartheta))$ durch $\mathfrak{p}^\alpha$, $\alpha \geqq \tau$, teilbar wird. Eine Zahl $r(\vartheta)$ kann man aber in der Form

$$r(\vartheta) = \sum Q(\vartheta)\varphi(\vartheta)^\alpha p^\beta \tag{32}$$

schreiben, wo $Q(x)\not\equiv 0 \pmod{p, \varphi(x)}$ und also $Q(\vartheta)$ nicht durch $\mathfrak{p}$ teilbar ist. Da $r(\vartheta)$ genau durch $\mathfrak{p}^{\tau-1}$ teilbar ist, muß in (32) immer nach Satz 7

$$\alpha\varkappa+\beta\lambda \geqq \tau-1$$

sein. Da man aber die Zahlen $\psi(\vartheta)$ oder $r(\vartheta)$ nur (mod $\mathfrak{p}^\tau$) untersuchen soll, kann man in (32) alle Glieder weglassen, wofür $\alpha\varkappa+\beta\lambda \geqq \tau$ ist. Eine Zahl $r(\vartheta)$ wird also immer kongruent einer linearen Summe der Glieder

$$\vartheta^\nu\varphi(\vartheta)^\alpha p^\beta, \tag{33}$$

für die $\alpha\varkappa+\beta\lambda = \tau-1 = \varepsilon\varkappa\lambda-\varkappa-\lambda$ ist. Weiter müssen natürlich die Exponenten α und β beide nicht negativ sein. Nun gibt es aber nach § 3 auf $L_{\tau-1}$ nur $\varepsilon-1$ Gitterpunkte oberhalb der X-Achse, und folglich gibt es nur $(\varepsilon-1)m$ verschiedene Zahlen der Form (33).

Es ist daher bewiesen, daß alle Zahlen $\psi_i(\vartheta)$ in (30) sich linear (mod $\mathfrak{p}^\tau$) durch die $(\varepsilon-1)$ Zahlen in (33) ausdrücken lassen, und nach der Theorie der linearen Kongruenzen folgt daraus, daß die $\psi_i(\vartheta)$ (mod $\mathfrak{p}^\tau$) linear abhängig sind, d. h. es besteht eine Kongruenz von der Form (31). Die Zahlen (30) bilden daher kein Fundamentalsystem für $\mathfrak{p}^{\tau-1}$ (mod $\mathfrak{p}^\tau$).

Es folgt daher:

Satz 8. *Der Partialführer des Ringes in Bezug auf $\mathfrak{p}$ ist*

$$\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^{\varepsilon\varkappa\lambda-\varkappa-\lambda+1}. \tag{34}$$

Weiter werde ich ein Fundamentalsystem für die Zahlen des Ideals $\mathfrak{f}_\mathfrak{p}$ in Bezug auf $\mathfrak{p}$ aufstellen. Ein solches Fundamentalsystem besteht, wie schon bemerkt, aus den Fundamentalsystemen der Ideale $\mathfrak{p}^\tau$, $\mathfrak{p}^{\tau+1}$, ..., $\mathfrak{p}^{\tau+\lambda-1}$ in Bezug auf den Moduln (mod $\mathfrak{p}^{\tau+1}$) ... (mod $\mathfrak{p}^{\tau+\lambda}$), d. h. aus den Zahlen

$$\vartheta^r \varphi(\vartheta)^a p^b,$$

wo (a, b) Gitterpunkte auf den Geraden L_τ, $L_{\tau+1}$, ..., $L_{\tau+\lambda-1}$ sind. Diese Punkte (a, b) sind dann, wie man aus der Figur ersieht, diejenigen Gitterpunkte, welche auf oder am nächsten unter der Geraden $L_{\tau+\lambda-1}$ liegen.

Die Gerade $L_{\tau+\lambda-1}$ hat die Gleichung

$$x\varkappa + y\lambda = \tau+\lambda-1 = \varepsilon\varkappa\lambda-\varkappa.$$

woraus

$$y = -\frac{\varkappa}{\lambda}x + \varepsilon\varkappa - \frac{\varkappa}{\lambda}.$$

Daher sind

$$\left(i, \left[\varepsilon\varkappa - \frac{\varkappa}{\lambda} - \frac{\varkappa}{\lambda}i\right]\right) \qquad (i = 0, 1, \ldots, \varepsilon\lambda-1)$$

diejenigen Gitterpunkte, welche am nächsten unter $L_{\tau+\lambda-1}$ liegen. Daher wird also

$$\vartheta^r \varphi(\vartheta)^i p^{\overline{\varepsilon\varkappa - \frac{\varkappa}{\lambda}(i+1)}} \qquad (i = 0, 1, \ldots, \varepsilon\lambda-1)$$

das gewünschte Fundamentalsystem[1].

[1] Es bedeutet überall $\overline{i}$ die kleinste ganze rationale Zahl, welche $\geqq i$ ist. Wie gewöhnlich ist $[i]$ die größte ganze rationale Zahl, welche $\leqq i$ ist. Wenn a eine ganze rationale Zahl ist, bemerkt man leicht, daß für alle i

$$\overline{a-i} = a-[i]$$

und

$$[a-t] = a-\overline{i}$$

ist.

Vertauscht man hier i mit $\varepsilon\lambda - i - 1$, so erhält man:

Satz 9. *Die Zahlen*

$$\vartheta^r \varphi(\vartheta)^{\varepsilon\lambda-i-1} p^{\left[\frac{i\varkappa}{\lambda}\right]} \quad (r = 0, 1, \ldots, m-1,\ i = 0, 1, \ldots, \varepsilon\lambda - 1)$$

bilden ein Fundamentalsystem für $\mathfrak{f}_\mathfrak{p}$ *in Bezug auf* $\mathfrak{p}$.

§ 5. Bestimmung des Führers.

In § 4 ist der Partialführer $\mathfrak{f}_{\mathfrak{p}_j^{(i)}}$ in Bezug auf ein Primideal $\mathfrak{p}_j^{(i)}$ bestimmt worden, und zwar ist nach (34)

$$\mathfrak{f}_{\mathfrak{p}_j^{(i)}} = \mathfrak{p}_j^{(i)\varepsilon_j^{(i)}\varkappa_i\lambda_i - \varkappa_i - \lambda_i + 1}$$

Weiter bilden nach Satz 9 die $\varepsilon_j^{(i)}\lambda_i m$ Zahlen

$$\vartheta^r \varphi(\vartheta)^{\varepsilon_j^{(i)}\lambda_i - s - 1} p^{\left[\frac{s\varkappa_i}{\lambda_i}\right]} \quad (r = 0, 1, \ldots, m-1,\ s = 0, 1, \ldots, \varepsilon_j^{(i)}\lambda_i - 1) \tag{35}$$

ein Fundamentalsystem für $\mathfrak{f}_{\mathfrak{p}_j^{(i)}}$ in Bezug auf $\mathfrak{p}_j^{(i)}$.

Nach C, Satz 5 zerfällt $f(x) \pmod{p^M}$ in ein Produkt von verschiedenen Faktoren $\Phi_j^{(i)}(x)$, welche den verschiedenen Primidealen $\mathfrak{p}_j^{(i)}$ entsprechen. Ich bezeichne nun das Produkt von allen diesen, außer $\Phi_j^{(i)}(x)$, mit $\Pi_j^{(i)}(x)$. Dann ist nach C, Satz 1

$$\begin{aligned}\Pi_j^{(i)}(x) = \Pi(x)\Phi_1(x)\Phi_2(x)\ldots\Phi_{i-1}(x)\Phi_{i+1}(x)\ldots\Phi_k(x)\\ \Phi_1^{(i)}(x)\ldots\quad\Phi_{j-1}^{(i)}(x)\Phi_{j+1}^{(i)}(x)\ldots\Phi_{t_i}^{(i)}(x),\end{aligned}$$

wobei $\Pi(x)$ das Produkt derjenigen Faktoren bezeichnet, welche $(\mathrm{mod}\, p)$ nicht durch $\varphi(x)$ teilbar sind.

Es soll nun bestimmt werden, durch welche Potenz von $\mathfrak{p}_j^{(i)}$ die Zahl $\Pi_j^{(i)}(\vartheta)$ teilbar ist. Die Zahl $\Pi(\vartheta)$ ist nicht durch $\mathfrak{p}_j^{(i)}$ teilbar. Das Produkt

$$\Phi_1(\vartheta)\ldots\Phi_{i-1}(\vartheta)\Phi_{i+1}(\vartheta)\ldots\Phi_k(\vartheta)$$

ist nach C, Satz 2 (und folgende Bemerkung) genau durch

$$\mathfrak{p}_j^{(i)(h_1+h_2+\cdots+h_{i-1})\lambda_i+(l_{i+1}+\cdots+l_k)\varkappa_i}$$

teilbar. Das Produkt

$$\Phi_1^{(i)}(\vartheta)\ldots\Phi_{j-1}^{(i)}(\vartheta)\Phi_{j+1}^{(i)}(\vartheta)\ldots\Phi_{t_i}^{(i)}(\vartheta)$$

ist nach C, Kap. II, § 3 (Gleichung (49)) genau durch

$$\mathfrak{p}_j^{(i)\lambda_i \varkappa_i(\varepsilon_i - \varepsilon_j^{(i)})} = \mathfrak{p}_j^{(i)h_i\lambda_i - \varepsilon_j^{(i)}\lambda_i\varkappa_i}$$

teilbar. Daher wird $\Pi_j^{(i)}(\vartheta)$ genau durch $\mathfrak{p}_j^{(i)}$ in einer Potenz mit dem Exponenten

$$\pi = (h_1 + h_2 + \cdots + h_i)\lambda_i + (l_{i+1} + \cdots + l_k)\varkappa_i - \varepsilon_j^{(i)}\lambda_i\varkappa_i$$

teilbar.

Der Kürze wegen bezeichne ich die $\varepsilon_j^{(i)}\lambda_i m$ Zahlen (35) in irgend einer Ordnung mit

$$T_{r,j}^{(i)}(\vartheta) \qquad (r = 1, 2, \ldots, \varepsilon_j^{(i)}\lambda_i m).$$

Dann bilden die Zahlen

$$\Pi_j^{(i)}(\vartheta)\, T_{r,j}^{(i)}(\vartheta) \qquad (r = 1, 2, \ldots \varepsilon_j^{(i)}\lambda_i m) \tag{36}$$

ein Fundamentalsystem in Bezug auf $\mathfrak{p}_j^{(i)}$ für ein Ideal, das gleich einer Potenz von $\mathfrak{p}_j^{(i)}$ mit dem Exponenten

$$\pi + \tau = (h_1 + h_2 + \cdots + h_i)\lambda_i + (l_{i+1} + \cdots + l_k)\varkappa_i - \varkappa_i - \lambda_i + 1. \tag{37}$$

ist.

Bildet man weiter die Zahlen (36) für alle verschiedenen Primidealteiler von p, so erhält man, da $\varepsilon_j^{(i)}\lambda_i m$ der Grad von $\Phi_j^{(i)}(x)$ ist, ein System von n Zahlen, und diese n Zahlen bilden nach § 1 ein Fundamentalsystem für ein Ideal $\mathfrak{a}$ in Bezug auf p, weil $\Pi_j^{(i)}(\vartheta)$ durch eine beliebig hohe Potenz von allen von $\mathfrak{p}_j^{(i)}$ verschiedenen Primidealen teilbar ist. Das Ideal $\mathfrak{a}$ wird nach (37) allgemein durch ein Ideal $\mathfrak{p}_j^{(i)}$ in der Potenz mit dem Exponenten

$$F = (h_1 + \cdots + h_i)\lambda_i + (l_{i+1} + \cdots + l_k)\varkappa_i - \varkappa_i - \lambda_i + 1.$$

teilbar.

Da die Zahlen (36) alle zum Ringe gehören, wird jede zu $\mathfrak{a}$ gehörige Zahl kongruent einer Zahl des Ringes für eine beliebig hohe Potenz von p. Daher wird der Partialführer $\mathfrak{f}_p$ in Bezug auf p sicher ein Teiler von $\mathfrak{a}$. Ich werde aber zeigen, daß man eben $\mathfrak{f}_p = \mathfrak{a}$ hat.

Wäre nämlich $\mathfrak{f}_p$ durch eine niedrigere Potenz von $\mathfrak{p}_j^{(i)}$ teilbar als $\mathfrak{a}$, so würden schon alle Zahlen des Ideals $\frac{\mathfrak{a}}{\mathfrak{p}_j^{(i)}}$ kongruent Zahlen des Ringes für eine beliebig hohe Potenz von p. Dies ist aber nicht der Fall, wie man leicht zeigen kann.

Die Zahl

$$\omega = \frac{A(\vartheta)}{p} = \Pi_j^{(i)}(\vartheta)\frac{\varphi(\vartheta)^{\varepsilon_j^{(i)}\lambda_i - 1}}{p}$$

ist, wie man leicht bemerkt, ganz und gehört zum Ideale $\frac{\mathfrak{a}}{\mathfrak{p}_j^{(i)}}$. Denn $\Pi_j^{(i)}(\vartheta)$ ist durch alle von $\mathfrak{p}_j^{(i)}$ verschiedenen Primideale in einer beliebig hohen Potenz teilbar, während $\mathfrak{p}_j^{(i)}$ in ω in genau der Potenz

$$F-1 = (h_1+\cdots+h_i)\lambda_i+(l_{i+1}+\cdots+l_k)\varkappa_i-\varkappa_i-\lambda_i$$

enthalten ist. Die Zahl ω kann aber nicht kongruent einer Zahl des Ringes für eine beliebig hohe Potenz von p als Modul sein. Denn zunächst ist der Grad von $A(\vartheta)$ in ϑ kleiner als n. Wenn man nämlich eine Kongruenz

$$\omega \equiv B(\vartheta) \pmod{p^M}$$

hätte, so würde daraus

$$\omega = B(\vartheta)+p^M\gamma \tag{38}$$

folgen, wo γ eine ganze Körperzahl ist. Wenn nun der Index k der Zahl ϑ durch p^ϱ genau teilbar ist, kann man

$$k = p^\varrho k_1$$

setzen, wobei k_1 nicht durch p teilbar ist. Man kann hier natürlich $\varrho \leqq M$ voraussetzen und multipliziert man dann (38) mit k_1, erhält man

$$k_1\omega = \frac{k_1 A(\vartheta)}{p} = k_1 B(\vartheta)+k\gamma_1,$$

wo auch γ_1 eine ganze Körperzahl ist. Nach § 2 ist $k\gamma_1$ immer eine Zahl des Ringes, also wird auch

$$\frac{k_1 A(\vartheta)}{p}$$

eine Zahl des Ringes, was offenbar unmöglich ist. Man muß also $\mathfrak{a} = \mathfrak{f}_p$ haben.

Satz 10. *Der Partialführer $\mathfrak{f}_p$ in Bezug auf p ist durch das Primideal $\mathfrak{p}_j^{(i)}$ genau in der Potenz*

$$\mathfrak{p}_j^{(i)(h_1+\cdots+h_i)\lambda_i+(l_{i+1}+\cdots+l_k)\varkappa_i-\varkappa_i-\lambda_i+1} \tag{39}$$

teilbar.

Nach Satz 4, § 2 ist damit die vollständige Zusammensetzung des Führers $\mathfrak{f}$ des Ringes ermittelt.

§ 6. Bestimmung der Körperdifferente.

Die Bestimmung der Körperdifferente kann nun leicht geschehen. In C, Satz 9 ist nämlich gezeigt worden, daß die Differente $f'(\vartheta)$ der Zahl ϑ durch das Primideal $\mathfrak{p}_j^{(i)}$ genau in der Potenz mit dem Exponenten

$$(40) \qquad (h_1+\cdots+h_i)\lambda_i+(l_{i+1}+\cdots+l_k)\varkappa_i-\varkappa_i+\varrho_j^{(i)}$$

teilbar ist. Hier bedeutet $\varrho_j^{(i)}$ eine ganze rationale Zahl, welche gleich Null ist, wenn λ_i nicht durch p teilbar ist. In jedem Falle kann $\varrho_j^{(i)}$ nach C, Kap. II, § 3 einfach bestimmt werden; ich werde übrigens am Schlusse dieses Abschnittes noch einmal die Bestimmung dieser Zahlen $\varrho_j^{(i)}$ behandeln.

Der Führer des Ringes enthält nach Satz 10, (39) die Potenz von $\mathfrak{p}_j^{(i)}$ mit dem Exponenten

$$(41) \qquad (h_1+\cdots+h_i)\lambda_i+(l_{i+1}+\cdots+l_k)\varkappa_i-\varkappa_i-\lambda_i+1.$$

Aus der Gleichung (12) folgt dann, wenn man also (41) von (40) abzieht, daß die Körperdifferente genau durch

$$\mathfrak{p}_j^{(i)\lambda_i-1+\varrho_j^{(i)}}$$

teilbar ist.

Satz 11. *Die Körperdifferente ist genau durch*

$$\mathfrak{p}_j^{(i)\lambda_i-1+\varrho_j^{(i)}}$$

teilbar. Hier ist $\varrho_j^{(i)}=0$, *wenn* λ_i *nicht durch* p *teilbar ist, und* $\varrho_j^{(i)}>0$, *wenn* λ_i *durch* p *teilbar ist, und in jedem Falle einfach bestimmbar.*

Man kann diesen Satz etwas umformen, indem man annimmt, daß

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

die Primidealzerlegung von p ist. Dann folgt:

Satz 12. *Die Körperdifferente ist durch*

$$\mathfrak{p}_i^{e_i-1+\varrho_i}$$

genau teilbar, wobei $\varrho_i=0$, *wenn* e_i *nicht durch* p *teilbar, und* $\varrho_i>0$, *wenn* e_i *durch* p *teilbar ist.*

In C, Kap. II, § 4 ist gezeigt worden, daß die Körperdiskriminante genau durch

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

teilbar ist, und daraus folgt sofort die Richtigkeit des *Dedekindschen Hauptsatzes:*

Die Körperdiskriminante ist, vom Vorzeichen abgesehen, gleich der Norm der Körperdifferente, also

$$|d| = N\mathfrak{d}.$$

Die Zahlen ϱ, welche für die Bestimmung der Körperdifferente von der größten Wichtigkeit sind, werden nach C, Kap. II, § 3 dadurch definiert, daß die Zahl $\Phi_j^{(i)}(\vartheta)$ genau durch $\mathfrak{p}_j^{(i)\varepsilon_j^{(i)}\lambda_i\varkappa_i-\varkappa_i+\varrho_j^{(i)}}$ teilbar ist. Praktisch kann man die Zahl $\varrho_j^{(i)}$ folgendermaßen einfach bestimmen. Indem ich wieder die Indizes weglasse, ist

$$\Phi(x) = \varphi(x)^{\varepsilon\lambda} + a_1(x)p^{\left[\frac{\varkappa}{\lambda}\right]}\varphi(x)^{\varepsilon\lambda-1} + a_2(x)p^{\left[\frac{2\varkappa}{\lambda}\right]}\varphi(x)^{\varepsilon\lambda-1} + \cdots + a_{\varepsilon\lambda}(x)p^{\varepsilon\varkappa},$$

wo für alle Glieder

$$\left[\frac{i\varkappa}{\lambda}\right] + (\varepsilon\lambda - i)\varkappa \geqq \varepsilon\lambda\varkappa$$

ist. Diejenigen Glieder, für die das Gleichheitszeichen gilt, sind

$$\varphi(x)^{\varepsilon\lambda} + a_\lambda(x)p^{\varkappa}\varphi(x)^{(\varepsilon-1)\lambda} + \cdots + a_{\varepsilon\lambda}(x)p^{\varepsilon\varkappa}. \tag{42}$$

Man kann also kurz

$$\Phi(x) = \sum a(x)\varphi(x)^\alpha p^\beta \tag{43}$$

setzen, wobei

$$\alpha\varkappa + \beta\lambda \geqq \varepsilon\lambda\varkappa \tag{44}$$

ist. Differentiiert man (43), so erhält man

$$\Phi'(x) = \sum a'(x)\varphi(x)^\alpha p^\beta + \varphi'(x)\sum \alpha a(x)\varphi(x)^{\alpha-1}p^\beta$$

und hier ist nach (44)

$$(\alpha-1)\varkappa + \beta\lambda = \alpha\varkappa + \beta\lambda - \varkappa \geqq \varepsilon\lambda\varkappa - \varkappa,$$

so daß $\Phi'(\vartheta)$ immer durch $\mathfrak{p}^{\varepsilon\lambda\varkappa-\varkappa}$ teilbar wird. Wenn λ nicht durch p teilbar ist, wird $\Phi'(\vartheta)$ genau durch diese Potenz von $\mathfrak{p}$ teilbar. Denn bei der Differentiation der Glieder (42) erhält man

$$\lambda\varphi'(x)[\varepsilon\varphi(x)^{\varepsilon\lambda-1} + a_\lambda(x)p^\varkappa\cdot(\varepsilon-1)\varphi(x)^{(\varepsilon-1)\lambda-1} + \cdots + a_{(\varepsilon-1)\lambda}(x)p^{(\varepsilon-1)\varkappa}\varphi(x)^{\lambda-1}]$$
$$+ a'_\lambda(x)p^\varkappa\varphi(x)^{(\varepsilon-1)\lambda} + \cdots + a'_{\varepsilon\lambda}(x)p^{\varepsilon\varkappa}.$$

Setzt man hier $x = \vartheta$, so werden die Glieder der zweiten Zeile gewiß durch $\mathfrak{p}^{\varepsilon\lambda\varkappa}$ teilbar. Wenn aber λ nicht durch p teilbar ist, wird $\lambda\varphi'(\vartheta)$ nicht durch $\mathfrak{p}$ teilbar, und daher werden alle Glieder der ersten Zeile genau durch $\mathfrak{p}^{\varepsilon\varkappa\lambda-\varkappa}$ teilbar. Man bemerkt weiter leicht, daß die Summe dieser Glieder nicht eine höhere Potenz von $\mathfrak{p}$ enthalten kann (man sehe C, Kap. II, § 3), und folglich ist $\varrho = 0$, wenn λ nicht durch p teilbar ist. Wenn λ durch p teilbar ist, so sieht man ein, daß $\Phi'(\vartheta)$ durch eine höhere Potenz als $\mathfrak{p}^{\varepsilon\varkappa\lambda-\varkappa}$ teilbar wird, und daher wird $\varrho \geqq 1$, wenn λ durch p teilbar ist.

Die wirkliche Bestimmung von ϱ erfolgt nun leicht folgendermaßen: Man bildet die Entwicklung $(p, \varphi(x))$ von $\Phi'(x)$, also

$$\Phi'(x) = \sum b_i(x)\,\varphi(x)^{\gamma_i} p^{\delta_i},$$

wo $b_i(x) \not\equiv 0 \pmod{p, \varphi(x)}$ ist. Setzt man hier $x = \vartheta$, so folgt nach Satz 7, daß $\Phi'(\vartheta)$ genau durch $\mathfrak{p}^R$ teilbar wird, wo R die kleinste unter den Zahlen $\varkappa\gamma_i + \lambda\delta_i$ ist. Daher wird also $\varrho = R - \varepsilon\varkappa\lambda + \varkappa$.

Satz 13. *Ist*

$$\Phi'(x) = \sum_i b_i(x)\,\varphi(x)^{\gamma_i} p^{\delta_i}$$

die Entwicklung $(p, \varphi(x))$ von $\Phi'(x)$, so wird, wenn R die kleinste unter den Zahlen $\varkappa\gamma_i + \lambda\delta_i$ bezeichnet, die Zahl ϱ durch

$$\varrho = R - \varepsilon\varkappa\lambda + \varkappa$$

bestimmt.

§ 7. Bestimmung einer oberen Grenze für die Zahlen ϱ.

Ich werde zuletzt zeigen, wie man eine obere Grenze für die Zahlen ϱ angeben kann. Zu diesem Zwecke werde ich aber zunächst zeigen, wie man dem zu $\mathfrak{p}_j^{(i)}$ gehörigen Faktor $\Phi_j^{(i)}(x)$ eine ganz einfache Form geben kann.

Es seien

$$\mathfrak{p}_1^{(m)}, \mathfrak{p}_2^{(m)}, \ldots, \mathfrak{p}_s^{(m)}$$

in irgend einer Reihenfolge diejenigen Primidealteiler von p, welche vom Grade m sind, für die also $N\mathfrak{p}_i^{(m)} = p^m$. Die Primzahl p soll durch $\mathfrak{p}_i^{(m)e_i^{(m)}}$ genau teilbar sein.

Zu den Zahlen

$$e_1^{(m)}, e_2^{(m)}, \ldots, e_s^{(m)}$$

kann man ein solches System von s ganzen rationalen Zahlen

$$h_1^{(m)}, h_2^{(m)}, \ldots, h_s^{(m)}$$

konstruieren, daß $h_i^{(m)}$ zu $e_i^{(m)}$ relativ prim ist, und weiter

$$\frac{h_1^{(m)}}{e_1^{(m)}} < \frac{h_2^{(m)}}{e_2^{(m)}} < \cdots < \frac{h_s^{(m)}}{e_s^{(m)}} \tag{45}$$

ist. Wenn dann $\varphi(x)$ eine Primfunktion m-ten Grades ist, so kann man nach B, § 2 eine solche Zahl ω des Körpers bestimmen, daß ω einer regulären Gleichung $F(x) = 0$ in Bezug auf p genügt, und weiter wird die Zahl $\varphi(\omega)$ durch ein Primideal $\mathfrak{p}_i^{(m)}$ genau in der Potenz $\mathfrak{p}_i^{(m)\,h_i^{(m)}}$ teilbar. Dann wird das Polygon $(p, \varphi(x))$ von $F(x)$ die Neigungszahlen (45) haben.

Speziell kann man aber $h_1^{(m)} = 1$ wählen; dann wird der Faktor $\Phi_1^{(m)}(x)$, der $\mathfrak{p}_1^{(m)}$ entspricht, die Form

$$\Phi_1^{(m)}(x) = \varphi(x)^{e_1^{(m)}} + p\,a_1(x)\,\varphi(x)^{e_1^{(m)}-1} + \cdots + p\,a_{e_1^{(m)}}(x)$$

haben, oder kurz

$$\Phi_1^{(m)}(x) = \varphi(x)^{e_1^{(m)}} + p\,A(x),$$

wobei

$$A(x) \not\equiv 0 \pmod{p, \varphi(x)}$$

ist.

Man kann also sagen:

Wenn p durch das Primideal $\mathfrak{p}$ m-ten Grades genau in der Potenz $\mathfrak{p}^e$ teilbar ist, kann man eine solche reguläre Gleichung $F(x) = 0$ finden, daß der zu $\mathfrak{p}$ entsprechende Faktor $\Phi(x)$ in der Zerlegung von $F(x) \pmod{p^M}$ die Form

$$\Phi(x) = \varphi(x)^e + p\,M(x) \tag{46}$$

hat, wobei $\varphi(x)$ eine Primfunktion m-ten Grades ist, $M(x) \not\equiv 0 \pmod{p, \varphi(x)}$ und der Grad von $M(x)$ kleiner als der Grad von $\varphi(x)^e$ ist.

Wenn man im folgenden voraussetzt, daß $\Phi(x)$ die spezielle Form (46) hat, so ist $\lambda = e$, $\varkappa = 1$ und $\varepsilon = 1$, und die Körperdifferente wird durch $\mathfrak{p}^{e-1+\varrho}$ teilbar. Die Zahl $F'(\omega)$ wird aber nach C, Kap. II, § 3 durch

$$\mathfrak{p}^{\varepsilon\lambda\varkappa-\varkappa+\varrho} = \mathfrak{p}^{e-1+\varrho}$$

genau teilbar, d. h. $F'(\omega)$ ist durch dieselbe Potenz von $\mathfrak{p}$ wie die Körperdifferente teilbar.

Weiter bilden in diesem Falle, da $\varphi(\omega)$ genau durch die erste Potenz von $\mathfrak{p}$ teilbar ist, die Zahlen

$$\omega^r\,\varphi(\omega)^s \quad (r = 0, 1, \ldots, m-1,\ s = 0, 1, \ldots, e-1)$$

ein Fundamentalsystem für alle Zahlen des Körpers in Bezug auf $\mathfrak{p}$. Daraus

folgt aber auch, daß die Zahlen

$$1,\ \omega,\ \omega^2,\ \ldots,\ \omega^{em-1}$$

ein solches Fundamentalsystem bilden, und nach § 1 kann folglich keine Kongruenz

$$a_0 + a_1\omega + \cdots + a_{m-1}\omega^{m-1} \equiv 0 \pmod{\mathfrak{p}^e}$$

bestehen, außer wenn alle a_i durch p teilbar sind, d. h. man hat identisch

$$a_0 + a_1 x + \cdots + a_{em-1}x^{em-1} \equiv 0 \pmod{p}.$$

Wie schon bewiesen worden ist, hat man nur dann $\varrho > 0$, wenn die Zahl e durch p teilbar ist. Die Zahl ϱ kann aber nicht beliebig groß werden. Ist nämlich

$$e = p^s e',$$

wo e' nicht durch p teilbar ist, so werde ich zeigen, daß man immer

$$\varrho \leqq se$$

hat.

Die Zahl

$$F'(\omega) = e\varphi'(\omega)\varphi(\omega)^{e-1} + pM'(\omega)$$

ist durch $\mathfrak{p}^{e-1+\varrho}$ teilbar. Wäre nun $\varrho \geqq se+1$, so würde $F'(\omega)$ durch $\mathfrak{p}^{(s+1)e}$ teilbar und man hätte eine Kongruenz

$$e\varphi'(\omega)\varphi(\omega)^{e-1} + pM'(\omega) \equiv 0 \pmod{\mathfrak{p}^{(s+1)e}}.$$

Eine solche Kongruenz kann aber nach der früheren Bemerkung nicht bestehen, außer wenn identisch

$$e\varphi'(x)\varphi(x)^{e-1} + pM'(x) \equiv 0 \pmod{p^{s+1}} \tag{47}$$

ist. Eine solche Kongruenz ist aber unmöglich, wie ich zeigen werde.

Allgemein kann man nämlich aus einer Kongruenz

$$H'(x) \equiv G'(x) \pmod{p}$$

auf die Kongruenz

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

schließen, wobei $A(x)$ ein Polynom ist. Ist der Modul eine Primzahlpotenz p^α, so folgt aus der Kongruenz

$$H'(x) \equiv G'(x) \pmod{p^\alpha}$$

eine Kongruenz von der Form

$$H(x) \equiv G(x) + A_0\left(x^{p^\alpha}\right) + pA_1\left(x^{p^{\alpha-1}}\right) + \cdots + p^{\alpha-1}A_{\alpha-1}(x^p) \pmod{p^\alpha},$$

wobei alle $A_i(x)$ Polynome sind.

Wendet man diese „Integration der Kongruenzen" auf die Kongruenz (47) an, folgt also

$$\varphi(x)^e + p\,M(x) \equiv A_0\left(x^{p^{s+1}}\right) + p\,A_1\left(x^{p^s}\right) + \cdots + p^s A_s(x^p) \pmod{p^{s+1}}.$$

Diese Kongruenz ist aber unmöglich, denn aus ihr würde man

$$\varphi(x)^e \equiv A_0\left(x^{p^{s+1}}\right) \pmod{p}$$

erhalten. Es ist aber bekanntlich

$$A_0\left(x^{p^{s+1}}\right) \equiv [A_0(x)]^{p^{s+1}} \pmod{p}$$

und folglich

$$\varphi(x)^e \equiv [A_0(x)]^{p^{s+1}} \pmod{p}.$$

Diese letzte Kongruenz ist nicht möglich, denn die Zerlegung in Primfaktoren $(\mathrm{mod}\, p)$ ist eindeutig, und da e nicht durch p^{s+1} teilbar ist, kann $\varphi(x)^e$ nicht $(\mathrm{mod}\, p)$ eine p^{s+1}-te Potenz sein.

Es ist daher bewiesen:

Satz 14. *Wenn e nicht durch p teilbar ist, wird $\varrho = 0$. Wenn e genau durch p^s teilbar ist, wird*

$$1 \leqq \varrho \leqq se. \tag{48}$$

Dieser Satz ist schon von Dedekind[1] vermutet worden, der erste Beweis wurde von Herrn Hensel[2] gegeben. Ein etwas anderer Beweis ist von Herrn Bauer[3] angegeben worden.

Herr Bauer[4] hat weiter gezeigt, daß für Körper, worin $p = \mathfrak{p}^s$ ist, ϱ sowohl die obere als die untere Grenze erreichen kann, d. h. man kann Körper angeben, in denen $\varrho = 1$ oder $\varrho = se$ ist. In einer anderen Arbeit (Math. Zeitschrift) bestimme ich allgemein, welche Zahlen ϱ bei einem gegebenen Exponent e vorkommen können; es stellt sich dabei heraus, daß es immer Ausnahmewerte gibt, welche nicht als Zahlen ϱ vorkommen können.

---

[1] R. Dedekind: „Über die Discriminanten endlicher Körper". Abhandlungen der Kgl. Gesellschaft der Wissenschaften zu Göttingen, 29 (1882), S. 55—56.

[2] K. Hensel: „Über die Entwicklung der algebraischen Zahlen in Potenzreihen". Mathematische Annalen, Bd. 55 (1902), S. 301—336.

[3] M. Bauer: „Verschiedene Bemerkungen über die Differente und die Diskriminante eines algebraischen Zahlkörpers". Mathematische Zeitschrift, Bd. 16 (1923), S. 1—12.

M. Bauer: „Über die Differente eines algebraischen Zahlkörpers". Mathematische Annalen, Bd. 83 (1921), S. 74—76.

[4] M. Bauer: „Verschiedene Bemerkungen usw.". Man sehe 3.

M. Bauer: „Bemerkungen zur Theorie der Differente". Acta litterarum ac scientiarum reg. universitatis hungaricae, Tom. 1 (1923), S. 195—198.