BESTIMMUNG DER DISKRIMINANTEN ALGEBRAISCHER KÖRPER.

VON

ÖYSTEIN ORE

in OSLO.

In den beiden Arbeiten: »Zur Theorie der algebraischen Körper»[1] und »Weitere Untersuchungen zur Theorie der algebraischen Körper»[2] habe ich eine algebraische Methode angegeben, wodurch man in einem vorgelegten Körper immer die Primidealzerlegung einer Primzahl bestimmen kann.

Die vorliegende Arbeit bildet eine Fortsetzung der eben erwähnten Arbeiten, indem ich mich hier zu verschiedenen anderen Aufgaben in der Theorie der algebraischen Körper wende. Es soll hier eine einfache Methode zur Bestimmung der Körperdiskriminante angegeben werden, wodurch man immer die genaue Potenz bestimmen kann, in welcher eine vorgelegte Primzahl die Körperdiskriminante teilt. Weiter soll gezeigt werden, wie man für ein jedes Primideal ein Fundamentalsystem aufstellen kann, und wie man daraus ein Fundamentalsystem für die zugehörige Primzahl ableitet. Sogleich gebe ich eine einfachere Form für die in den oben erwähnten Arbeiten gegebene Darstellung der Primideale. Aus diesen Untersuchungen folgen auch verchiedene interessante Sätze über die Zusammensetzung von Gleichungsdiskriminanten und Indizes für algebraische Zahlen.

Diese Abhandlung ist während meines Aufenthalts als Stipendiat an dem mathematischen Institute, Stockholm, geschrieben worden, und ich bringe dem Direktor des Instituts, Herrn Professor Mittag-Leffler, meinen herzlichsten Dank für die dadurch entstandene Erleichterung meiner Arbeit dar.

---

[1] Acta mathematica, 44. Diese Arbeit soll im Folgenden mit A bezeichnet werden.

[2] Acta mathematica, 45. Diese Arbeit soll im Folgenden mit B bezeichnet werden.

Kap. I. Bestimmung der Fundamentalsysteme.

§ 1.

Fundamentalsysteme für Primideale und Primzahlen.

Es sei ein algebraischer Körper $P(\vartheta)$ n^{ten} Grades gegeben. Die Zahl ϑ soll ganz algebraisch angenommen werden und genügt folglich einer Gleichung

$$f(x) = x^n + a_1 . x^{n-1} + \cdots + a_n = 0, \tag{1}$$

wo die Koeffizienten

$$a_1, a_2, \ldots a_n$$

ganze rationale Zahlen bedeuten.

Im Folgenden soll immer p eine rationale Primzahl bezeichnen und weiter $\mathfrak{p}$ ein Primideal f^{ten} Grades sein, das in p aufgeht.

Ein System von f ganzen Zahlen des Körpers

$$\eta_1, \eta_2, \ldots \eta_f$$

soll ein *Fundamentalsystem für das Primideal* $\mathfrak{p}$ *heissen*, wenn die p^f Zahlen

$$a_1 . \eta_1 + a_2 . \eta_2 + \cdots + a_f . \eta_f \qquad (a_i = 0, 1, \ldots, p-1)$$

ein vollständiges Restsystem (mod $\mathfrak{p}$) bilden, d. h. wenn α eine beliebige ganze Zahl des Körpers bedeutet, so ist

$$\alpha \equiv b_1 . \eta_1 + b_2 . \eta_2 + \cdots + b_f . \eta_f \pmod{\mathfrak{p}},$$

wo die Zahlen b_i eindeutig aus der Reihe $0, 1, \ldots p-1$ bestimmt sind.

Allgemeiner soll gesagt werden, dass, wenn P ein Idealteiler von p ist und $NP = p^k$, die k Zahlen

$$\eta_1, \eta_2, \ldots \eta_k$$

ein *Fundamentalsystem für* P bilden, wenn die p^k ganzen Zahlen

$$a_1 . \eta_1 + a_2 . \eta_2 + \cdots + a_k . \eta_k \qquad (a_i = 0, 1, \ldots p-1)$$

ein vollständiges Restsystem (mod P) bilden.

Wenn nun $\mathfrak{p}^e$ ein Idealteiler von p ist, so kann man aus einem Fundamentalsysteme für $\mathfrak{p}$ leicht auch ein Fundamentalsystem für das Ideal $\mathfrak{p}^e$ ableiten. Wenn nämlich

$$\gamma_1, \gamma_2, \ldots \gamma_{e-1} \tag{2}$$

ein System von ganzen Zahlen des Körpers bezeichnet, wo allgemein γ_i durch $\mathfrak{p}^i$ genau teilbar ist, so bilden die Zahlen

$$\eta_1, \eta_2, \ldots \eta_f, \gamma_1\eta_1, \gamma_1\eta_2, \ldots \gamma_1\eta_f, \ldots, \gamma_{e-1}\eta_1, \gamma_{e-1}\eta_2, \ldots \gamma_{e-1}\eta_f$$

ein Fundamentalsystem für $\mathfrak{p}^e$.

Um dies nachzuweisen, braucht man nur zu zeigen, dass eine lineare Summe mit ganzen rationalen Koeffizienten von diesen Zahlen, also eine Zahl von der Form

$$\alpha = \sum_{i=1}^{f} a_i\eta_i + \gamma_1 \sum_{i=1}^{f} a_i^{(1)} . \eta_i + \cdots + \gamma_{e-1} \sum_{i=1}^{f} a_i^{(e-1)} . \eta_i,$$

nur dann durch $\mathfrak{p}^e$ teilbar sein kann, wenn die ganzen rationalen Zahlen $a_i^{(j)}$ alle durch p teilbar sind. Da aber α auch durch $\mathfrak{p}$ teilbar sein muss und die Zahlen (2) alle durch $\mathfrak{p}$ teilbar sind, so folgt

$$\sum_{i=1}^{f} a_i\eta_i \equiv 0 \pmod{\mathfrak{p}},$$

und somit sind alle a_i durch p teilbar. Diese letzte Summe ist daher auch sicher durch $\mathfrak{p}^e$ teilbar. Dann folgt weiter, dass man auch

$$\gamma_1 . \sum_{i=1}^{f} a_i^{(1)} . \eta_i \equiv 0 \pmod{\mathfrak{p}^2}$$

haben muss, und da γ_1 genau durch $\mathfrak{p}$ teilbar ist, wird auch

$$\sum_{i=1}^{f} a_i^{(1)} . \eta_i \equiv 0 \pmod{\mathfrak{p}},$$

folglich werden alle $a_i^{(1)}$ durch p teilbar, usw.

Ein System

$$\lambda_1, \lambda_2, \ldots \lambda_m \tag{3}$$

von n ganzen Zahlen des Körpers soll ein *Fundamentalsystem für die Primzahl* p heissen, wenn die p^n Zahlen

$$a_1 \lambda_1 + a_2 \lambda_2 + \cdots + a_n \lambda_n \qquad (a_i = 0, 1, \ldots p-1)$$

ein vollständiges Restsystem für p bilden. Die notwendige und hinreichende Bedingung dafür, dass die Zahlen (3) ein Fundamentalsystem für p bilden, kann man auch so ausdrücken, dass sie (mod p) linear unabhängig sind, d. h. dass eine Kongruenz

$$a_1 \lambda_1 + a_2 \lambda_2 + \cdots + a_n \lambda_n \equiv 0 \pmod{p}$$

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

Man kann aber diese Bedingung etwas umformen. Wenn nämlich

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

eine Minimalbasis des Körpers ist, so hat man

$$\begin{aligned}
\lambda_1 &= b_{1,1}\,\omega_1 + b_{1,2}\,\omega_2 + \cdots + b_{1,n}\,\omega_n, \\
\lambda_2 &= b_{2,1}\,\omega_1 + b_{2,2}\,\omega_2 + \cdots + b_{2,n}\,\omega_n, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\lambda_n &= b_{n,1}\,\omega_1 + b_{n,2}\,\omega_2 + \cdots + b_{n,n}\,\omega_n,
\end{aligned}$$

wo die Koeffizienten $b_{i,j}$ ganz rational sind. Die notwendige und hinreichende Bedingung für ein Fundamentalsystem für p wird dann, dass der *Index*

$$k(\lambda_1, \lambda_2, \ldots \lambda_n) = \begin{vmatrix} b_{1,1}, & b_{1,2}, & \ldots & b_{1,n}, \\ b_{2,1}, & b_{2,2}, & \ldots & b_{2,n}, \\ \cdots & \cdots & \cdots & \cdots \\ b_{n,1}, & b_{n,2}, & \ldots & b_{n,n} \end{vmatrix}$$

nicht durch p teilbar ist. Bedeutet d die Körperdiskriminante, so folgt aus der Relation

$$\Delta(\lambda_1, \lambda_2, \ldots \lambda_n) = k(\lambda_1, \lambda_2, \ldots \lambda_n)^2 \cdot d,$$

dass die Primzahl p in der Körperdiskriminante und in der Diskriminante $\Delta(\lambda_1, \lambda_2, \ldots \lambda_n)$ des Fundamentalsystems für p in derselben Potenz aufgeht. Um daher die Potenz zu bestimmen, in welcher p in der Körperdiskriminante aufgeht, braucht man folglich nur ein Fundamentalsystem für die Primzahl p zu kennen.

Es ist eben gezeigt worden, wie man aus einem Fundamentalsysteme für das Primideal $\mathfrak{p}$ ein Fundamentalsystem für $\mathfrak{p}^e$ herleiten kann. Ist aber

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

die Primidealzerlegung von p, so kann man, wenn die Fundamentalsysteme für $\mathfrak{p}_i^{e_i}\,(i = 1, 2, \ldots s)$ bekannt sind, auch ein Fundamentalsystem für p herleiten. Man kann nämlich solche ganze Zahlen Π_i des Körpers bestimmen, dass Π_i durch das Ideal

$$\mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_{i-1}^{e_{i-1}}\mathfrak{p}_{i+1}^{e_{i+1}}\ldots\mathfrak{p}_s^{e_s},$$

aber nicht durch $\mathfrak{p}_i$ teilbar ist. Wenn dann die Zahlen

$$\eta_1^{(i)}, \eta_2^{(i)}, \ldots \eta_{e_i f_i}^{(i)} \qquad (i = 1, 2, \ldots s)$$

ein Fundamentalsystem für $\mathfrak{p}_i^{e_i}$ bilden, so sind die Zahlen

$$\Pi_i\,\eta_1^{(i)}, \Pi_i\,\eta_1^{(i)}, \ldots \Pi_i\,.\,\eta_{e_i f_i}^{(i)} \qquad (i = 1, 2, \ldots s)$$

ein Fundamentalsystem für p. Denn eine Zahl α, welche eine lineare Summe mit ganzen rationalen Koeffizienten von diesen Zahlen ist, hat die Gestalt

$$\alpha = \Pi_1\sum_{j=1}^{e_1 f_1} a_j^{(1)}\,.\,\eta_j^{(1)} + \Pi_2\sum_{j=1}^{e_2 f_2} a_j^{(2)}\,\eta^{(2)} + \cdots + \Pi_s\sum_{j=1}^{e_s f_s} a_j^{(s)}\,\eta_j^{(s)}.$$

Wenn nun α durch p teilbar sein soll, müssen alle Koeffizienten $a_j^{(i)}$ durch p teilbar sein. Da nämlich α auch durch das Ideal $\mathfrak{p}_i^{e_i}$ teilbar sein muss und da alle Zahlen $\Pi_1, \Pi_2, \ldots \Pi_s$ ausser Π_i durch $\mathfrak{p}_i^{e_i}$ teilbar sind, so folgt

$$\Pi_i\sum_{j=1}^{e_i f_i} a_j^{(i)}\,.\,\eta_j^{(i)} \equiv 0 \pmod{\mathfrak{p}_i^{e_i}}$$

und daraus, weil Π_i nicht durch $\mathfrak{p}_i$ teilbar ist,

$$\sum_{j=1}^{e_i f_i} a_j^{(i)}\,.\,\eta_j^{(i)} \equiv 0 \pmod{\mathfrak{p}_i^{e_i}}.$$

Da aber die Zahlen $\eta_j^{(i)}$ ein Fundamentalsystem für $\mathfrak{p}_i^{e_i}$ bilden, so folgt aus dieser Kongruenz, dass alle $a_j^{(i)}$ durch p teilbar sein müssen.

§ 2.

Bestimmung der Primideale.

Wie in der Arbeit A gezeigt worden ist, kann man nun die Primidealzerlegung einer vorgelegten Primzahl p in der folgenden Weise bestimmen.

Es sei

$$f(x) \equiv \varphi_1(x)^{e_1} \varphi_2(x)^{e_2} \dots \varphi_s(x)^{e_s} \pmod{p} \tag{4}$$

die Primfunktionzerlegung von $f(x) \pmod{p}$, wo die Primfunktion $\varphi_i(x)$ die Form

$$\varphi_i(x) = x^{m_i} + a_1^{(i)} . x^{m_i-1} + \dots + a_{m_i}^{(i)}$$

hat. Dann folgt zunächst aus (4), dass man für p die Idealzerlegung

$$p = \mathfrak{a}_1 . \mathfrak{a}_2 \dots \mathfrak{a}_s \tag{5}$$

hat, wo keine der Ideale $\mathfrak{a}_i$ Einheitsideale sind. Weiter ist

$$\mathfrak{a}_i = (p, \varphi_i(\vartheta)^{e_i}) \qquad (i = 1, 2 \dots s),$$

und diese Ideale sind alle zu einander relativ prim.

Um eine weitere Zerlegung des Ideals $\mathfrak{a} = (p, \varphi(\vartheta)^e)$ zu bestimmen, bildet man die *Entwicklung* $(p, \varphi(x))$ *von* $f(x)$

$$f(x) = \sum_{i=0}^{t} Q_i(x) . p^{\alpha_i} . \varphi(x)^i . \tag{6}$$

Dabei bedeutet also $\varphi(x)$ eine Primfunktion $(\mathrm{mod}\, p)$ vom Grade m und $Q_i(x)$ ein Polynom höchstens vom Grade $m-1$. Weiter soll der Exponent α_i so gewählt sein, dass $Q_i(x)$ den Zahlenfaktor p nicht enthält, und endlich ist

$$t = \left[\frac{n}{m}\right].$$

Zu den Punkten $(t-i, \alpha_i)$ konstruiert man dann das zugehörige *Newtonsche Polygon*. Da vorausgesetzt wird, dass $\varphi(x) \pmod{p}$ in $f(x)$ aufgeht, so wird sicher ein Teil dieses Polygones oberhalb der X-achse liegen. Dieser Teil soll das *Hauptpolygon* $(p, \varphi(x))$ genannt werden, und seine Seiten seien mit

$$S_1, S_2, \dots S_k$$

bezeichnet.

Weiter seien bzw.

$$l_1, l_2, \ldots l_k$$

und

$$h_1, h_2, \ldots h_k$$

die Projektionen dieser Seiten auf die X-achse und Y-achse. Die Neigung φ_r der Seite S_r gegen die X-achse ist dann durch

$$\operatorname{tg} \varphi_i = \frac{h_i}{l_i}$$

bestimmt. Der grösste gemeinsame Faktor der Zahlen l_i und h_i soll mit ε_i bezeichnet werden, folglich ist

$$\begin{aligned} l_i &= \varepsilon_i \,.\, \lambda_i, \\ h_i &= \varepsilon_i \,.\, \varkappa_i, \end{aligned} \qquad (i = 1, 2, \ldots k)$$

wo λ_i zu $\varkappa_i$ relativ prim ist. Da die Seiten des Polygones ständig wachsende Neigungen besitzen, so ist auch

$$\frac{\varkappa_1}{\lambda_1} < \frac{\varkappa_2}{\lambda_2} < \cdots < \frac{\varkappa_k}{\lambda_k}. \tag{7}$$

Weiter ist in A der Faktor $f_i(x)$ der i^{ten} Seite S_i definiert worden als

$$f_i(x) = \varphi(x)^{\varepsilon_i \cdot \lambda_i} + S_1^{(i)}(x) \,.\, p^{\varkappa_i} \,.\, \varphi(x)^{(\varepsilon_i - 1)\lambda_i} + \cdots + S_{\varepsilon_i}^{(i)}(x) \,.\, p^{\varepsilon_i \varkappa_i}\,. \tag{8}$$

Diesen leitet man nach A Kap. 2, § 4 einfach aus der Summe der Glieder in (6) ab, für welche die entsprechenden Punkte auf S_i liegen. Den Faktor (8) der Seite S_i zerlegt man dann weiter in Primfaktoren für diese Seite, also

$$f_i(x) \equiv f_1^{(i)}(x) \,.\, f_2^{(i)}(x) \ldots f_{t_i}^{(i)}(x) \pmod{S_i}, \tag{9}$$

wo allgemein

$$f_j^{(i)}(x) = \varphi(x)^{\varepsilon_j^{(i)} \cdot \lambda_i} + S_{1,j}(x) \,.\, p^{\varkappa_i} \,.\, \varphi(x)^{(\varepsilon_j^{(i)} - 1)\lambda_i} + \cdots + S_{\varepsilon_j^{(i)}, j}^{(i)}(x) \,.\, p^{\varepsilon_j^{(i)} \cdot \varkappa_i} \tag{10}$$

eine Primfunktion der i^{ten} Seite ist.

Setzt man

$$f_i(x, y) = y^{\varepsilon_i} + S_1^{(i)}(x) \,.\, y^{\varepsilon_i - 1} + \cdots + S_{\varepsilon_i}^{(i)}(x),$$

so bedeutet die Zerlegung (9), dass eine Kongruenz

$$f_i(x, y) \equiv f_1^{(i)}(x, y) \cdot f_2^{(i)}(x, y) \ldots f_{t_i}^{(i)}(x, y) \,(\mathrm{modd}\, p, \varphi(x))$$

besteht, wo allgemein

$$f_j^{(i)}(x, y) = y^{\varepsilon_j^{(i)}} + S_{1,j}^{(i)}(x)\, y^{\varepsilon_j^{(i)}-1} + \cdots + S_{\varepsilon_j^{(i)}, j}^{(i)}(x)$$

eine Primfunktion (modd p, $\varphi(x)$) bedeutet. Man sieht auch leicht ein, dass die Formeln

$$f_i\left(x, \frac{\varphi(x)^{\lambda_i}}{p^{\varkappa_i}}\right) = \frac{f_i(x)}{p^{h_i}}$$

und

$$f_j^{(i)}\left(x, \frac{\varphi(x)^{\lambda_i}}{p^{\varkappa_i}}\right) = \frac{f_j^{(i)}(x)}{p^{\varepsilon_j^{(i)} \cdot \varkappa_i}}$$

bestehen.

In der Arbeit B habe ich nun die folgende Definition gegeben: Die Gleichung $f(x) = 0$ für eine ganze Zahl des Körpers wird *regulär in Bezug auf* p genannt, wenn erstens $f(x)$ irreduzibel und vom Grade n ist, und wenn zweitens, wenn $\varphi(x)$ eine Primfunktion (mod p) bedeutet, welche in $f(x)$ (mod p) aufgeht, die Primfaktoren in der Zerlegung (9) für jede Seite verschieden sind.

In B ist weiter gezeigt worden, dass es in jedem Körper und für jede Primzahl p unendlich viele reguläre Gleichungen gibt, und es ist daher keine Einschränkung der Allgemeinheit der Untersuchungen, wenn ich im Folgenden für die Untersuchung eines algebraischen Zahlkörpers eine reguläre Gleichung zu Grunde lege.

Wenn die Gleichung $f(x) = 0$ im Folgenden als eine reguläre Gleichung in Bezug auf p angenommen wird, kann man nach A die Primidealzerlegung der Primzahl p einfach bestimmen.

Ein Idealteiler $\mathfrak{a} = (p, \varphi(\vartheta)^e)$ von p in der Zerlegung (5) hat nämlich dann die Primidealzerlegung

$$\mathfrak{a} = (\mathfrak{p}_1^{(1)} \cdot \mathfrak{p}_2^{(1)} \ldots \mathfrak{p}_t^{(1)})^{\lambda_1} \cdot (\mathfrak{p}_1^{(2)} \ldots \mathfrak{p}_{t_2}^{(2)})^{\lambda_2} \ldots (\mathfrak{p}_1^{(k)} \ldots \mathfrak{p}_t^{(k)})^{\lambda_k}, \tag{11}$$

wo das Primideal $\mathfrak{p}_j^{(i)}$ vom Grade $\varepsilon_j^{(i)} \cdot m$ ist, also

$$N(\mathfrak{p}_j^{(i)}) = p^{\varepsilon_j^{(i)} \cdot m}.$$

Aus (11) folgt dann durch Multiplikation der Ideale $\mathfrak{a}_t$ nach (5) die Primidealzerlegung von p.

In A, Kap. 4, § 4, habe ich auch eine Darstellung eines Primideals $\mathfrak{p}_j^{(i)}$ als grössten gemeinsamen Faktor von gewissen Hauptidealen gegeben. In den folgenden Paragraphen werde ich mich mit diesen Untersuchungen über Primideale beschäftigen und zwar zeigen, wie man ihnen eine einfachere und für meine folgenden Untersuchungen bequemere Form geben kann.

§ 3.

Zerlegung einer regulären Gleichung für Primzahlpotenzmoduln.

Ich werde mich hier mit der Zerlegung des regulären Polynoms $f(x)$ für einen Primzahlpotenzmodul beschäftigen, und zwar zeigen, wie man diese Zerlegung einfach aus dem Polygone und den Primfaktoren der Seiten herleiten kann.

Aus der Darstellung (4) von $f(x) \pmod p$ folgt nach einem Satze von SCHOENEMANN[1], dass auch für jeden Primzahlpotenzmodul p^M eine Zerlegung

$$f(x) \equiv F_1(x) \cdot F_2(x) \ldots F_s(x) \pmod{p^M} \tag{12}$$

besteht, wo allgemein

$$F_i(x) \equiv \varphi_i(x)^{e_i} \pmod p . \tag{13}$$

Nach (12) kann man daher immer das Polynom $f(x)$ in der Form

$$f(x) = F_1(x) \cdot F_2(x) \ldots F_s(x) + p^M \cdot N(x) \tag{14}$$

schreiben, wo $N(x)$ ein Polynom von höchstens $(n-1)^{\text{tem}}$ Grade ist. Für die folgenden Untersuchungen denke ich mir in (14) den Exponenten M fest gewählt und zwar grösser als eine gewisse untere Grenze, die durch die folgenden Untersuchungen bestimmt wird.

Es sei $F(x)$ einer der Faktoren (12) von $f(x) \pmod{p^M}$ und nach (13)

$$F(x) \equiv \varphi(x)^e \pmod p . \tag{15}$$

Ich bilde nun das Polygon $(p, \varphi(x))$ von $F(x)$. Dieses Polygon S wird, wie man leicht wegen (15) sieht, ein Hauptpolygon.

---

[1] SCHOENEMANN: Crelles Journ. 32. S. 98.

Wenn im Folgenden in (12) der Exponent M grösser als die Ordinate α_t des höchsten Punktes (t, α_t) in dem Polygone $(p, \varphi(x))$ von $f(x)$ gewählt wird, sieht man einfach nach A ein, dass das Polygon S von $F(x)(p, \varphi(x))$ gleich dem Hauptpolygone von $f(x)(p, \varphi(x))$ wird. Weiter bemerkt man auch, dass die Faktoren der Seiten gleich den entsprechenden Seitenfaktoren in dem Hauptpolygone von $f(x)(p, \varphi(x))$ sind, und folglich auch einfach aus der Entwicklung $(p, \varphi(x))$ von $f(x)$ bestimmt werden können. Für die praktische Anwendung ist diese Bemerkung insofern von Nutzen, dass man für die Bestimmung der Faktoren der Seiten die Zerlegung (12) nicht wirklich auszuführen braucht.

Die Faktoren der Seiten für $F(x)$ sollen also durch die Formel (8) gegeben sein, und die Zerlegung in Primfaktoren für die entsprechende Seite ist dann weiter durch (9) und (10) bestimmt, und da $f(x)$ regulär vorausgesetzt ist, sollen alle Primfunktionen (10) für dieselbe Seite verschieden sein.

Nach A, Satz 5, kann man daher auch schreiben,

$$F(x) \equiv f_1(x) \cdot f_2(x) \ldots f_k(x) \pmod{S}$$

indem man unter dieser Kongruenz versteht, dass in der Differenz

$$F(x) - f_1(x) \cdot f_2(x) \ldots f_k(x)$$

alle repräsentierenden Punkte oberhalb S liegen. Man kann dies auch so ausdrücken, dass für $F(x) \pmod{S}$ eine Zerlegung in Faktoren besteht und zwar derart, dass das Polygon eines Faktors gleich einer Seite S_i von S ist.

Daraus folgt aber nach A, Kap. 2, § 6, dass für alle Primzahlpotenzmoduln p^M eine Zerlegung

$$F(x) \equiv \Phi_1(x) \cdot \Phi_2(x) \ldots \Phi_k(x) \pmod{p^M} \tag{16}$$

besteht, wo auch das Polynom $\Phi_i(x)$ das geradlinige Polygon S_i besitzt und ausserdem

$$\Phi_i(x) \equiv f_i(x) \pmod{S_i}.$$

Den Faktor $\Phi_i(x)$ kann man aber weiter in Faktoren $(\mathrm{mod}\, p^M)$ zerlegen, da nach (9)

$$\Phi_i(x) \equiv f_1^{(i)}(x) \cdot f_2^{(i)}(x) \ldots f_{t_i}^{(i)}(x) \pmod{S_i}.$$

Aus dieser Kongruenz folgt nämlich nach A, Kap. 2, § 6, dass auch immer die Zerlegung

$$\Phi_i(x) \equiv \Phi_1^{(i)}(x) \cdot \Phi_2^{(i)}(x) \dots \Phi_{t_i}^{(i)}(x) \pmod{p^M}$$

besteht. Hier ist das Polygon $S_j^{(i)}$ von $\Phi_j^{(i)}(x)$ gleich dem Polygone von $f_j^{(i)}(x)$, also geradlinig und von der Neigung $\frac{\varkappa_i}{\lambda_i}$. Ausserdem sind die beiden Polynome für diese Gerade $S_j^{(i)}$ kongruent, also

$$\Phi_j^{(i)}(x) \equiv f_j^{(i)}(x) \pmod{S_j^{(i)}}. \tag{17}$$

Man sieht leicht ein, dass dadurch auch eine Zerlegung von $\Phi_i(x)$ in irreduzible Faktoren (mod p^M) gefunden ist, wenn nur der Exponent M grösser als die früher angegebene Grenze ist. Denn nach dem Satze, dass das Polygon eines Produkts aus den Polygonen der Faktoren zusammengesetzt ist,[1] folgt, dass $\Phi_j^{(i)}(x) \pmod{p^M}$ irreduzibel sein muss. Wenn nämlich $\Phi_j^{(i)}(x)$ reduzibel wäre, müsste ein Faktor auch ein Polygon $(p, \varphi(x))$ mit der Neigung $\frac{\varkappa_i}{\lambda_i}$ besitzen, und daraus würde folgen, dass $\Phi_j^{(i)}(x)$ auch für das Polygon $S_j^{(i)}$ reduzibel wäre, was nach (17) nicht möglich ist, da nach der Voraussetzung $f_j^{(i)}(x)$ eine Primfunktion für die i^{te} Seite war.

Man hat folglich den interessanten Satz:

Satz. 1. Wenn $f(x)$ in Bezug auf die Primzahl p regulär ist, besteht für jeden Primzahlpotenzmodul p^M die Zerlegung

$$f(x) \equiv F_1(x) \cdot F_2(x) \dots F_s(x) \pmod{p^M},$$

wo weiter für einen Faktor $F_t(x)$

$$F(x) \equiv \Phi_1(x) \cdot \Phi_2(x) \dots \Phi_k(x) \pmod{p^M}.$$

Ein Faktor $\Phi_i(x)$ hat dann weiter die Zerlegung

$$\Phi_i(x) \equiv \Phi_1^{(i)}(x) \cdot \Phi_2^{(i)}(x) \dots \Phi_{t_i}^{(i)}(x) \pmod{p^M},$$

wo für einen Faktor $\Phi_j^{(i)}(x)$ die Kongruenz (17) besteht. Wenn der Exponent M genügend gross gewählt wird, so ist der Faktor $\Phi_j^{(i)}(x)$ (mod p^M) irreduzibel.

Wenn

$$h = h_1 + h_2 + \cdots + h_k$$

[1] ORE, Ö: Zur Theorie der Irreduzibilitätskriterien. Math. Zeitschr. Bd. 18. S. 285.

die Ordinate des höchsten Punktes in dem Polygone $(p, \varphi(x))$ von $f(x)$ ist und H die grösste der Zahlen h, so wird, wenn $M > H$ gewählt wird, die Zerlegung des Satzes 1 eine irreduzible.

Wie man leicht einsieht, ist die Zerlegung (mod p^M) des Satzes 1 im allgemeinen nicht eindeutig für den Modul p^M. Eine genauere Untersuchung zeigt aber, dass es eine solche feste Zahl h gibt, dass diese Zerlegung (mod p^M) für den Modul p^{M-h} eindeutig wird.

§ 4.

Hilfssätze.

Aus der Kongruenz (12) folgt nun, wenn $x = \vartheta$ gesetzt wird,

$$F_1(\vartheta) \cdot F_2(\vartheta) \dots F_s(\vartheta) \equiv 0 \pmod{p^M}, \tag{18}$$

und hier können zwei Zahlen $F_i(\vartheta)$ und $F_j(\vartheta)$ keinen gemeinsamen Primidealdivisor $\mathfrak{p}$ besitzen, der gleichzeitig in p aufgeht. Denn es ist ja nach (13)

$$F_i(x) \equiv \varphi_i(x)^{e_i}, \quad F_j(x) \equiv \varphi_j(x)^{e_j} \pmod{p},$$

und der gemeinsame Primidealfaktor $\mathfrak{p}$ muss daher auch in den Zahlen $\varphi_i(\vartheta)$ und $\varphi_j(\vartheta)$ aufgehen. Dies ist aber nicht möglich, weil man immer solche Polynome $A(x)$ und $B(x)$ bestimmen kann, dass

$$\varphi_i(x) \cdot A(x) + \varphi_j(x) \cdot B(x) \equiv 1 \pmod{p},$$

woraus für $x = \vartheta$ folgen würde, dass auch 1 durch $\mathfrak{p}$ teilbar wäre.

Es sollen nun die Primideale untersucht werden, welche gleichzeitig in p und $\varphi(\vartheta)$ aufgehen, wo $\varphi(x)$ eine Primfunktion (mod p) bezeichnet, welche in $f(x)$ aufgeht. In A, Kap. 3, § 5 ist gezeigt worden, dass es immer solche gemeinsame Primideale $\mathfrak{p}$ gibt. Man erkennt ferner leicht, dass, wenn $\mathfrak{p}$ ein Primideal ist, wofür

$$\varphi(\vartheta) \equiv p \equiv 0 \pmod{\mathfrak{p}},$$

eine Zahl $h(\vartheta)$, wo $h(x)$ ein beliebiges Polynom in x bedeutet, nur dann durch $\mathfrak{p}$ teilbar sein kann, wenn $h(x) \equiv 0$ (modd $p, \varphi(x)$).

Es sei jetzt

$$p = \mathfrak{p}^s \cdot \mathfrak{p}_1$$
$$\varphi(\vartheta) = \mathfrak{p}^t \cdot \mathfrak{p}_2$$

eine Idealzerlegung von p und $\varphi(\vartheta)$, wo die Ideale $\mathfrak{p}_1$ und $\mathfrak{p}_2$ nicht durch $\mathfrak{p}$ teilbar sind. Nach A, Satz 16 folgt aber dann, dass die Relation

$$\frac{s}{t}=\frac{\lambda_i}{\varkappa_i} \tag{19}$$

besteht, wo i eine der Zahlen $1, 2, \ldots k$ bedeutet. Im Folgenden soll $\mathfrak{p}$ ein *Primideal der i^{ten} Seite* genannt werden, wenn für die Exponenten s und t die Gleichung (19) erfüllt ist. Da aber unter der Voraussetzung, dass $f(x)$ regulär ist, die Primidealzerlegung von p durch (11) bestimmt ist, wird $s=\lambda_i$ und folglich $t=\varkappa_i$. Für ein Primideal der i^{ten} Seite ist daher p durch $\mathfrak{p}^{\lambda_i}$, $\varphi(\vartheta)$ durch $\mathfrak{p}^{\varkappa_i}$ genau teilbar.

Daraus folgt nach (11), dass man für $\varphi(\vartheta)$ die Primidealzerlegung

$$\varphi(\vartheta)=(\mathfrak{p}^{(1)}, \ldots \mathfrak{p}_{t_1}^{(1)})^{\varkappa_1} \cdot (\mathfrak{p}^{(2)}, \ldots \mathfrak{p}_{t_2}^{(2)})^{\varkappa_2} \ldots (\mathfrak{p}^{(k)}, \ldots \mathfrak{p}_{t_k}^{(k)})^{\varkappa_k} \cdot \Phi \tag{20}$$

hat, wobei das Ideal Φ zu p relativ prim ist.

Aus (18) folgt nun, dass ein Primideal $\mathfrak{p}$, das gleichzeitig in p und $\varphi_i(\vartheta)$ aufgeht, auch in $F_i(\vartheta)$ in einer beliebig hohen Potenz aufgehen muss, wenn der Exponent M hinreichend gross wird.

Im Folgenden werden sehr oft Zahlen untersucht, welche von der Wahl der Exponenten M abhängen, z. B. $F_i(\vartheta)$, $\Phi_i(\vartheta)$, $\Phi_j^{(i)}(\vartheta)$ und daraus abgeleitete Grössen. *Der Kürze wegen werde ich dann sagen, dass ein Primideal $\mathfrak{p}$ in einer beliebig hohen Potenz in einer solchen Zahl A aufgeht, wenn man durch eine hinreichend grosse Wahl des Exponenten M erreichen kann, dass auch A durch eine beliebig grosse, vorgeschriebene Potenz des Primideals $\mathfrak{p}$ teilbar wird.*

In dieser Bezeichnung kann man also sagen, dass, wenn $\mathfrak{p}$ ein gemeinsames Primideal für p und $\varphi_i(\vartheta)$ ist, $F_i(\vartheta)$ durch eine beliebig hohe Potenz von $\mathfrak{p}$ teilbar ist. Aus der Kongruenz (16) folgt aber weiter

$$F(\vartheta)\equiv\Phi_1(\vartheta) \cdot \Phi_2(\vartheta) \ldots \Phi_k(\vartheta) \pmod{p^M}, \tag{21}$$

und dies zeigt, dass auch mindestens eine der Zahlen $\Phi_i(\vartheta)$ durch das Primideal $\mathfrak{p}$ in einer beliebig hohen Potenz teilbar ist. Im Folgenden soll gezeigt werden, dass allgemein die Zahl $\Phi_i(\vartheta)$ alle Primideale der i^{ten} Seite

$$\mathfrak{p}_j^{(i)} \qquad (j=1, 2, \ldots t_i)$$

in beliebig hohen Potenzen enthalten muss.

Wenn nun $\mathfrak{p}^{(i)}$ ein beliebiges Primideal der i^{ten} Seite ist, so geht also $\mathfrak{p}^{(i)}$ in p in der Potenz λ_i und in $\varphi(\vartheta)$ in der Potenz $\varkappa_i$ auf. Es soll nun untersucht werden, in welcher Potenz $\mathfrak{p}^{(i)}$ in einer Zahl $\Phi_j(\vartheta)$, $j \neq i$, aufgeht.

Da $\Phi_j(\vartheta)$ das geradlinige Polygon $S_j(p, \varphi(x))$ hat, so kann man annehmen, dass dieses Polynom die Gestalt (A. Kap. 2. § 5)

$$\Phi_j(x) = \varphi(x)^{l_j} + A_1^{(j)}(x) \cdot p^{\overline{\frac{h_j}{l_j}}} \cdot \varphi(x)^{l_j - 1} + A_2^{(j)}(x) \cdot p^{\overline{\frac{2h_j}{l_j}}} + \cdots + A_{l_j}^{(j)}(x) \cdot p^{h_j} \tag{22}$$

hat,[1] wo die Koeffizienten $A_t^{(j)}(x)$ Polynome von höchstens $(m-1)^{\text{tem}}$ Grade sind. Die Gliedersumme in $\Phi_j(x)$ für welche die repräsentierenden Punkte auf dem geradlinigen Polygone S_j für $\Phi_j(x)$ liegen, ist dann durch

$$\varphi(x)^{\varepsilon_j \cdot \lambda_j} + A_{\lambda_j}^{(j)}(x) \cdot p^{\varkappa_j} \cdot \varphi(x)^{(\varepsilon_j - 1)\lambda_j} + A_{2\lambda_j}^{(j)}(x) \cdot p^{2\varkappa_j} \cdot \varphi(x)^{(\varepsilon_j - 2)\lambda_j} + \cdots + A_{\varepsilon_j \cdot \lambda_j}^{(j)}(x) \cdot p^{\varepsilon_j \cdot \varkappa_i}$$

gegeben, und da nach § 3 diese Summe kongruent $f_j(x)$ (mod S_j) ist, so kann man allgemein

$$A_{k \cdot \lambda_j}^{(j)}(x) \equiv S_k^{(j)}(x) \pmod{p, \varphi(x)}$$

annehmen. Dies zeigt speziell, dass

$$A_{l_j}^{(j)}(x) \equiv S_{\varepsilon_j}^{(j)}(x) \not\equiv 0 \pmod{p, \varphi(x)}$$

sein muss.

Setzt man nun in (22) $x = \vartheta$, so wird ein Glied

$$A_t^{(j)}(\vartheta) \cdot p^{\overline{\frac{th_j}{l_j}}} \cdot \varphi(\vartheta)^{l_j - t}$$

durch

$$\mathfrak{p}^{(i)\ \lambda_i \cdot \overline{\frac{th_j}{l_i}} + \varkappa_i \cdot l_j - t \cdot \varkappa_i} \tag{23}$$

teilbar, und der Exponent in (23) ist grösser oder gleich

$$\lambda_i \cdot \frac{th_j}{l_j} + \varkappa_i \cdot l_j - t \cdot \varkappa_i = \varkappa_i l_j - t \cdot \lambda_i \left(\frac{\varkappa_i}{\lambda_i} - \frac{\varkappa_j}{\lambda_j} \right).$$

[1] Wenn s eine reelle positive Zahl bedeutet, soll das Symbol $\overline{s}$ die kleinste ganze rationale Zahl bezeichnen, welche grösser oder gleich s ist.

Wenn daher hier $i<j$ ist, so wird nach (7)

$$\frac{\varkappa_j}{\lambda_j}<\frac{\varkappa_i}{\lambda_i},$$

und folglich ist der Exponent in (23) für $t=0$ am kleinsten, und zwar gleich $\varkappa_i \,.\, l_j$. Da das Glied $\varphi(\vartheta)^{l_j}$ auch wirklich genau durch diese Potenz von $\mathfrak{p}^{(i)}$ teilbar ist, wird also $\Phi_j(\vartheta)$ genau durch $\mathfrak{p}^{(i)\,\varkappa_i \cdot l_j}$ teilbar.

Wenn aber $i>j$ ist, wird

$$\frac{\varkappa_i}{\lambda_i}>\frac{\varkappa_j}{\lambda_j},$$

und der Exponent in (23) ist daher für $t=l_j$ am kleinsten und zwar gleich $h_j \,.\, \lambda_i$. Da auch das Glied

$$A_{l_j}^{(i)}(\vartheta) \,.\, p^{h_j}$$

genau durch diese Potenz von $\mathfrak{p}^{(i)}$ teilbar ist, wird in diesem Falle $\Phi_j(\vartheta)$ genau durch $\mathfrak{p}^{(i)\,\lambda_j \cdot h_j}$ teilbar.

Es ist daher bewiesen:

Satz. 2. Wenn $\mathfrak{p}^{(i)}$ ein Primideal der i^{ten} Seite ist, so wird die Zahl $\Phi_j(\vartheta)$ durch $\mathfrak{p}^{(i)}$ genau in der Potenz $\mathfrak{p}^{(i)\,\lambda_i \cdot h_j}$ teilbar, wenn $i>j$. Wenn $i<j$ ist, wird $\Phi_j(\vartheta)$ genau durch $\mathfrak{p}^{(i)\,\varkappa_i \cdot l_j}$ teilbar.

Das Produkt der Zahlen

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

enthält daher $\mathfrak{p}^{(i)}$ genau in der Potenz

$$\mathfrak{p}^{(i)\,(h_1+h_2+\cdots+h_{i-1})\lambda_i \,+\, (l_{i+1}+l_{i+2}+\cdots+l_k)\varkappa_i}$$

und da der Exponent hier fest bestimmt ist, so folgt aus (21), dass man den Exponenten M so gross wählen kann, dass $\Phi_i(\vartheta)$ durch $\mathfrak{p}^{(i)}$ in einer beliebig vorgeschriebenen Potenz teilbar wird, d. h. $\Phi_i(\vartheta)$ ist durch alle Primideale der i^{ten} Seite in beliebig hohen Potenzen teilbar.

§ 5.

Bestimmung der Fundamentalsysteme für Primideale.

Zunächst werde ich hier einige Hilfsgrössen aufstellen, welche für die späteren Untersuchungen notwendig sind.

Bezeichnet man mit $\Pi(x)$ das Produkt aller Faktoren $F_i(x)$ in (12), welche nicht durch die Primfunktion $\varphi(x)$ (mod p) teilbar sind, so ist die Zahl $\Pi(\vartheta)$ ganz und durch eine beliebig hohe (von M abhängige) Potenz eines jeden Primidealfaktors $\mathfrak{p}$ von p teilbar, der nicht in dem Ideal $(p, \varphi(\vartheta))$ aufgeht.

Daraus sieht man auch leicht ein, dass die Zahl

$$N_1 = \Pi(\vartheta) \cdot \frac{\Phi_1(\vartheta)}{p^{h_1}}$$

ganz ist. Um dies zu zeigen, braucht man nur nachzuweisen, dass ein Primideal $\mathfrak{p}$ immer in einer ebenso hohen Potenz im Zähler wie im Nenner p^{h_1} aufgeht. Ein Primideal $\mathfrak{p}$ von p, das nicht in $(p, \varphi(\vartheta))$ aufgeht, geht sicher in $\Pi(\vartheta)$ in einer höheren Potenz als in p^{h_1} auf. Ein Primideal, das in $(p, \varphi(\vartheta))$ aufgeht, und zur ersten Seite gehört, geht nach § 4 in $\Phi_1(x)$ in einer beliebig hohen Potenz, im Nenner aber nur in der bestimmten Potenz $\lambda_1 . h_1$ auf. Wenn zuletzt $\mathfrak{p}^{(i)}$ ein Primideal der i^{ten} Seite ist, geht es nach Satz 2 in $\Phi_1(\vartheta)$ genau in der Potenz $\lambda_i . h_1$ auf, und da der Nenner auch genau durch diese Potenz teilbar ist, wird N_1 ganz, aber nicht durch $\mathfrak{p}^{(i)}$ teilbar.

Die Zahl N_1 ist also ganz, und wenn $\mathfrak{p}$ ein Primidealteiler von p ist, der entweder nicht in $(p, \varphi(\vartheta))$ aufgeht, oder in $(p, \varphi(\vartheta))$ aufgeht und zur ersten Seite gehört, so ist N_1 durch eine beliebig hohe Potenz von $\mathfrak{p}$ teilbar. Wenn aber $\mathfrak{p}$ in $(p, \varphi(\vartheta))$ aufgeht und zu einer der Seiten $S_2, S_3, \ldots S_k$ gehört, so ist N_1 nicht durch $\mathfrak{p}$ teilbar.

Diese Bemerkungen sollen nun in der folgenden Weise verallgemeinert werden:

Satz 3. Die Zahlen

$$N_0 = \Pi(\vartheta), \quad N_i = \Pi(\vartheta) \frac{\Phi_1(\vartheta) \cdot \Phi_2(\vartheta) \ldots \Phi_i(\vartheta)}{p^{h_1+h_2+\cdots+h_i}} \qquad (i=1, 2, \ldots k) \qquad (24)$$

sind alle ganz, und wenn $\mathfrak{p}$ ein Primideal von p ist, das entweder nicht in $(p, \varphi(\vartheta))$ aufgeht, oder in $(p, \varphi(\vartheta))$ aufgeht und zu einer der Seiten $S_1, S_2, \ldots S_i$ gehört, so ist N_i durch eine beliebig hohe Potenz von $\mathfrak{p}$ teilbar. Wenn aber $\mathfrak{p}$ in $(p, \varphi(\vartheta))$ aufgeht und zu einer der Seiten $S_{i+1}, \ldots S_k$ gehört, so ist N_i nicht durch $\mathfrak{p}$ teilbar.

Man beweist den Satz am einfachsten durch vollständige Induktion. Es ist nämlich

$$N_i = N_{i-1} \cdot \frac{\Phi_i(\vartheta)}{p^{h_i}}$$

und diese Zahl muss nun ganz sein. Denn alle Primidealteiler von p, welche nicht zu den Seiten $S_i, S_{i+1}, \ldots S_k$ gehören, gehen nach unserer Voraussetzung in N_{i-1} in einer beliebig hohen Potenz auf. Ein Ideal der i^{ten} Seite geht in $\Phi_i(\vartheta)$ nach § 4 in einer beliebig hohen Potenz auf. Ein Primideal der s^{ten} Seite, $s>i$, geht aber nicht in N_{i-1}, und in $\Phi_i(\vartheta)$ nach Satz 2 genau in der Potenz $\lambda_s \,.\, h_i$ auf, und da auch p^{h_i} genau durch dieselbe Potenz $\lambda_s \,.\, h_i$ des Primideals teilbar ist, wird N_i ganz und durch keine Ideale der s^{ten} Seite teilbar, wenn $s>i$, w. z. b. w.

Wenn man nun weiter

$$\theta_i(\vartheta) = \frac{\varphi(\vartheta)^{\lambda_i}}{p^{\varkappa_i}}$$

setzt, so sind alle Zahlen

$$N_{i-1} \,.\, \theta_i(\vartheta)^\varepsilon = N_{i-1} \cdot \frac{\varphi(\vartheta)^{\varepsilon \,.\, \lambda_i}}{p^{\varepsilon \,.\, \varkappa_i}} \qquad (\varepsilon = 1, 2, \ldots \varepsilon_i) \qquad (25)$$

ganz und durch kein Primideal der i^{ten} Seite teilbar. Denn zunächst ist für ein Primideal von p, das nicht zu einer der Seiten $S_i, S_{i+1}, \ldots S_k$ gehört, N_{i-1} sicher durch eine höhere Potenz des Primideals als $p^{\varepsilon \cdot \varkappa_i}$ teilbar. Für ein Primideal $\mathfrak{p}$ der i^{ten} Seite ist $\varphi(\vartheta)^{\varepsilon \cdot \lambda_i}$ durch $\mathfrak{p}$ in der Potenz $\varepsilon \,.\, \varkappa_i \,.\, \lambda_i$ teilbar, während $p^{\varepsilon \cdot \varkappa_i}$ genau dieselbe Potenz enthält. Für ein Primideal der Seite S_s, $s>i$ ist $\varphi(\vartheta)^{\varepsilon \cdot \lambda_i}$ durch $\mathfrak{p}$ in der Potenz $\varepsilon \,.\, \lambda_i \,.\, \varkappa_s$ genau teilbar, während $p^{\varepsilon \cdot \varkappa_i}$ durch $\mathfrak{p}$ in der Potenz $\varepsilon \,.\, \varkappa_i \,.\, \lambda_s$ teilbar ist. Da aber

$$\varepsilon \,.\, \varkappa_s \,.\, \lambda_i - \varepsilon \,.\, \varkappa_i \,.\, \lambda_s = \varepsilon \,.\, \lambda_i \,.\, \lambda_s \left(\frac{\varkappa_s}{\lambda_s} - \frac{\varkappa_i}{\lambda_i} \right) > 0$$

ist, geht $\mathfrak{p}$ im Zähler in einer höheren Potenz als im Nenner auf.

Es sollen nun alle ganzen Zahlen von der Form

$$N_{i-1} \,.\, F(\vartheta, \theta_i(\vartheta)) = N_{i-1} (A_1(\vartheta) \,.\, \theta_i(\vartheta)^\varepsilon + A_2(\vartheta) \,.\, \theta_i(\vartheta)^{\varepsilon-1} + \cdots + A_\varepsilon(\vartheta)) \qquad (26)$$

untersucht werden, wo die Koeffizienten $A(\vartheta)$ Polynome in ϑ sind, welche (modd $p, \varphi(x)$) reduziert sein sollen, folglich höchstens vom Grade $m-1$ in ϑ sind; weiter soll $\varepsilon < \varepsilon_i$ vorausgesetzt werden.

Ich werde nun bestimmen, unter welcher Bedingung eine Zahl von der Form (26) durch alle Primideale der i^{ten} Seite teilbar sein kann. Nach A, Satz 17 folgt, dass jedenfalls die Zahl

$$N_{i-1}\cdot\frac{f_i(\vartheta)}{p^{h_i}} = N_{i-1}\,f_i(\vartheta,\theta_i(\vartheta)) = N_{i-1}\left(\theta_i(\vartheta)^{\varepsilon_i} + S_1^{(i)}(\vartheta)\,.\,\theta_i(\vartheta)^{\varepsilon_i-1} + \cdots + S_{\varepsilon_i}^{(i)}(\vartheta)\right)$$

durch alle Primideale der i^{ten} Seite teilbar ist.

Wenn man nun, um die Teilbarkeit einer Zahl (26) durch Primideale der i^{ten} Seite zu untersuchen, die Methode anwendet, welche ich in A. Kap. 4 § 2 angegeben habe, so ergibt sich ohne Schwierigkeiten das folgende Kriterium:

Die notwendige und hinreichende Bedingung dafür, dass eine Zahl $N_{i-1}\,.\,F(\vartheta,\theta_i(\vartheta))$ durch alle Primideale der i^{ten} Seite teilbar ist, wird dadurch ausgedrückt, dass $F(x,y)$ (modd $p,\varphi(x)$) durch $f_i(x,y)$ teilbar sein soll.

Da nun in (26) der Exponent ε kleiner als ε_i vorausgesetzt ist, so folgt, dass $F(x,y)$ in diesem Falle nur dann durch $f_i(x,y)$ (modd $p,\varphi(x)$) teilbar sein kann, wenn

$$A_1(x)\equiv A_2(x)\equiv\cdots\equiv A_\varepsilon(x)\equiv 0 \pmod{p,\varphi(x)}$$

ist, und da $A_i(x)$ (modd $p,\varphi(x)$) reduziert sein sollte, so müssen in diesen Polynomen alle Koeffizienten durch p teilbar sein.

Bezeichnet man nun mit P_i das Produkt

$$P_i = \mathfrak{p}_1^{(i)}\,.\,\mathfrak{p}_2^{(i)}\ldots\mathfrak{p}_{t_i}^{(i)} \tag{27}$$

der Primideale der i^{ten} Seite, so ist

$$N P_i = p^{\sum_{j=1}^{t_i} e_j^{(i)}\,.\,m} = p^{e_i\,.\,m}.$$

Die Zahlen

$$N_{i-1}(A_1(\vartheta)\,.\,\theta_i(\vartheta)^{e_i-1} + A_2(\vartheta)\,.\,\theta_i(\vartheta)^{e_i-2} + \cdots + A_{e_i}(\vartheta))$$

mit (modd $p,\varphi(x)$) reduzierten Koeffizienten $A(x)$ sind daher alle (mod P_i) inkongruent, und da ihre Anzahl, wie man leicht sieht, gleich $p^{e_i\,.\,m}$ ist, so bilden sie ein vollständiges Restsystem (mod P_i). Daher ist bewiesen:

Satz 4. Wenn P_i das Produkt der Primideale der i^{ten} Seite bedeutet, so bilden die $p^{e_i\,.\,m}$ Zahlen

$$N_{i-1}\theta_i(\vartheta)^t \cdot \vartheta^r \qquad (t=0, 1, \ldots \varepsilon_i-1,\ r=0, 1, \ldots m-1) \qquad (28)$$

ein Fundamentalsystem für P_i.

Man kann auch sehr einfach ein Fundamentalsystem für das Primideal $\mathfrak{p}_j^{(i)}$ aufstellen. Die Zahl

$$N_{i-1}\cdot\frac{f_j^{(i)}(\vartheta)}{p^{\varepsilon_j^{(i)}\cdot\varkappa_i}} = N_{i-1}\cdot f_j^{(i)}(\vartheta, \theta_i(\vartheta))$$

$$= N_{i-1}\left(\theta_i(\vartheta)^{\varepsilon_j^{(i)}} + S_{j,1}^{(i)}(\vartheta)\cdot\theta_i(\vartheta)^{\varepsilon_j^{(i)}-1} + \cdots + S_{j,\varepsilon_j^{(i)}}^{(i)}(\vartheta)\right)$$

ist nämlich ganz und sicher durch ein Primideal der i^{ten} Seite teilbar. Denn wäre dies nicht der Fall, würde schon die Zahl

$$N_{i-1}\cdot f_1^{(i)}(\vartheta, \theta_i(\vartheta)) \ldots f_{j-1}^{(i)}(\vartheta, \theta_i(\vartheta))\cdot f_{j+1}^{(i)}(\vartheta, \theta_i(\vartheta)) \ldots f_{t_i}^{(i)}(\vartheta, \theta_i(\vartheta))$$

durch alle Primideale der i^{ten} Seite teilbar, was nach dem oben angegebenen Kriterium nicht möglich ist. Daher ist jede Zahl

$$N_{i-1}\cdot\frac{f_j^{(i)}(\vartheta)}{p^{\varepsilon_j^{(i)}\cdot\varkappa_i}} \qquad (j=1.\ 2, \ldots t_i)$$

durch ein Primideal der i^{ten} Seite teilbar, und wie man aus A. Kap. 4 sieht, kann man die Numerierung so wählen, dass diese Zahl allgemein durch $\mathfrak{p}_j^{(i)}$ teilbar ist.

Man kann nun einfach angeben, wann eine Zahl von der Form (26) durch $\mathfrak{p}_j^{(i)}$ teilbar ist, denn man zeigt:

Die notwendige und hinreichende Bedingung dafür, dass eine Zahl (26) durch $\mathfrak{p}_j^{(i)}$ teilbar ist, wird dadurch ausgedrückt, dass $F(x, y)$ (modd p, $\varphi(x)$) durch $f_j^{(i)}(x, y)$ teilbar ist.

Es ist einleuchtend, dass diese Bedingung eine hinreichende ist. Dass sie aber auch notwendig ist, folgt daraus, dass, wenn $F(x, y)$ nicht durch $f_j^{(i)}(x, y)$ (modd p, $\varphi(x)$) teilbar ist, man solche Polynome $A(x, y)$ und $B(x, y)$ bestimmen kann, dass

$$F(x, y)\cdot A(x, y) + f_j^{(i)}(x, y)\cdot B(x, y) \equiv 1 \pmod{p, \varphi(x)}.$$

Wenn diese Kongruenz mit $N_{i-1}(x)^2$ multipliziert und $x=\vartheta$, $y=\theta_i(\vartheta)$ gesetzt wird, so folgt, dass ein gemeinsamer Primidealteiler der i^{ten} Seite für $N_{i-1}F(\vartheta, \theta_i(\vartheta))$

und $N_{i-1} f_j^{(i)}(\vartheta, \theta_i(\vartheta))$ auch in N_{i-1} aufgehen muss, was jedoch nach Satz 3 unmöglich ist.

Daher sind die ganzen Zahlen

$$N_{i-1}\left(A_1(\vartheta) \cdot \theta_i(\vartheta)^{e_j^{(i)}-1} + A_2(\vartheta) \cdot \theta_i(\vartheta)^{e_j^{(i)}-2} + \cdots + A_{\varepsilon_j^{(i)}}(\vartheta)\right),$$

wo alle Koeffizienten (modd p, $\varphi(x)$) reduziert sind, sicher (mod $\mathfrak{p}_j^{(i)}$) inkongruent, und da ihre Anzahl eben $p^{e_j^{(i)} \cdot m} = N(\mathfrak{p}_j^{(i)})$ ist, bilden sie ein vollständiges Restsystem (mod $\mathfrak{p}_j^{(i)}$). Es ist folglich bewiesen:

Satz 5. Die $p^{e_j^{(i)} \cdot m}$ Zahlen

$$N_{i-1} \cdot \theta_i(\vartheta)^t \cdot \vartheta^r \qquad (t = 0, 1, \ldots \varepsilon_j^{(i)} - 1,\ r = 0, 1, \ldots, m-1)$$

bilden ein Fundamentalsystem für das Primideal $\mathfrak{p}_j^{(i)}$.

Man kann hier noch eine andere Bemerkung machen, welche von Interesse sein mag. Da nämlich eine Zahl

$$N_{i-1} \cdot f_j^{(i)}(\vartheta, \theta_i(\vartheta)) = N_{i-1} \cdot \frac{f_j^{(i)}(\vartheta)}{p^{\varepsilon_j^{(i)} \cdot x_i}}$$

nicht durch $\mathfrak{p}_{j_1}^{(i)}$ teilbar ist, wenn $j_1 \neq j$, so wird die Zahl $f_j^{(i)}(\vartheta)$ genau durch

$$\mathfrak{p}_j^{(i)\, e_j^{(i)} \cdot x_i \cdot \lambda_i}$$

teilbar, und da

$$\Phi_j^{(i)}(x) \equiv f_j^{(i)}(x) \pmod{S_i}$$

und alle Glieder oberhalb des Polygones durch höhere Potenzen von $\mathfrak{p}_{j_1}^{(i)}$ als diejenigen Glieder, welche auf dem Polygone liegen, teilbar sind, so wird auch $\Phi_j^{(i)}(\vartheta)$ genau durch $\mathfrak{p}_{j_1}^{(i)}$ in der Potenz $\varepsilon_j^{(i)} \cdot x_i \cdot \lambda_i$ teilbar.

Da aber nach § 4 die Zahl $\Phi_i(\vartheta)$ alle Primideale der i^{ten} Seite in beliebig hohen Potenzen enthalten muss, und da wegen Satz 1

$$\Phi_i(\vartheta) \equiv \Phi_1^{(i)}(\vartheta) \cdot \Phi_2^{(i)}(\vartheta) \ldots \Phi_{t_i}^{(i)}(\vartheta) \pmod{p^M}$$

ist, so folgt, dass, wenn ein Ideal $\mathfrak{p}_j^{(i)}$ gegeben ist, dieses Ideal nur in der Zahl $\Phi_j^{(i)}(\vartheta)$ in einer beliebig hohen Potenz vorkommen kann, weil alle andere Faktoren $\Phi_{j_1}(\vartheta)$ nur fest bestimmte Potenzen dieses Ideals enthalten können.

Daraus folgt der Satz:

Satz 5. Wenn $f(x)$ regulär in Bezug auf p ist, und für den beliebig grossen Primzahlpotenzmodul p^M die Zerlegung des Satzes 1 *besitzt, so gibt es einen und nur einen Primidealteiler $\mathfrak{p}_j^{(i)}$ von p derart, dass $\Phi_j^{(i)}(\vartheta)$ durch eine beliebig hohe (von M abhängige) Potenz des Primideals teilbar wird. Alle andere Primidealteiler von p kommen in $\Phi_j^{(i)}(\vartheta)$ nur in fest bestimmten Potenzen vor.*

§ 6.

Bestimmung eines Fundamentalsystems für die Primzahl p.

Nachdem in § 5 ein Fundamentalsystem für alle Primidealteiler von p bestimmt worden ist, leitet man ziemlich einfach daraus ein Fundamentalsystem für p selbst ab.

Durch Satz 4 ist ein Fundamentalsystem für das Produkt P_i der Primideale der i^{ten} Seite bestimmt worden. Da aber nach (11) p durch P_i in der Potenz λ_i teilbar ist, werde ich zunächst ein Fundamentalsystem für $P_i^{\lambda_i}$ bestimmen. Dies geschieht aber nach § 1 in der Weise, dass man eine Reihe von Zahlen

$$K_1, K_2, \ldots K_{\lambda_i - 1}$$

so bestimmt, dass, wenn $\mathfrak{p}$ ein Primideal der i^{ten} Seite ist, K_j durch $\mathfrak{p}$ genau in der Potenz j teilbar wird.

In der Darstellung (22) von $\Phi_i(x)$ kommen allgemein die Glieder

$$A_r^{(i)}(x) \cdot p^{\left\lfloor \frac{(l_i - r)\varkappa_i}{\lambda_i} \right\rfloor} \cdot \varphi(x)^r \quad (r = 0, 1, \ldots l_j)$$

vor, und ich untersuche nun, in welcher Potenz die Zahl

$$B_r = p^{\left\lfloor \frac{(l_i - r)\varkappa_i}{\lambda_i} \right\rfloor} \cdot \varphi(\vartheta)^r$$

das Primideal $\mathfrak{p}$ der i^{ten} Seite enthält. Man sieht ein, da $\varphi(\vartheta)$ durch $\mathfrak{p}$ in der

Potenz x_i und p durch $\mathfrak{p}$ in der Potenz λ_i genau teilbar ist, dass B_r das Primideal $\mathfrak{p}$ genau in der Potenz

$$\lambda_i \underbrace{\left\lceil \frac{(l_i - r)\, x_i}{\lambda_i} \right\rceil} + r \,.\, x_i \tag{29}$$

enthalten muss. Es wird nun $0 < r < \lambda_i$ vorausgesetzt, und die Zahl ϱ eindeutig durch die Kongruenz

$$r \,.\, x_i \equiv \varrho \pmod{\lambda_i}$$

bestimmt, wenn man $0 < \varrho < \lambda_i$ annimmt. Dann ist[1]

$$\frac{(l_i - r)\, x_i}{\lambda_i} = \left[\frac{(l_i - r)\, x_i}{\lambda_i} \right] + \frac{\lambda_i - \varrho}{\lambda_i},$$

und da man für jede reelle, nicht ganze rationale Zahl i die Beziehung $\overline{i} = [i] + 1$ hat, so ist, wie man leicht sieht,

$$\underbrace{\left\lceil \frac{(l_i - r)\, x_i}{\lambda_i} \right\rceil} = \frac{(l_i - r)\, x_i}{\lambda_i} + \frac{\varrho}{\lambda_i}. \tag{30}$$

Folglich geht (29) in

$$\lambda_i \left(\frac{(l_i - r)\, x_i}{\lambda_i} + \frac{\varrho}{\lambda_i} \right) + r \,.\, x_i = h_i \,.\, \lambda_i + \varrho$$

über und die Zahl B_i ist daher durch $\mathfrak{p}$ in genau der Potenz $(h_i \,.\, \lambda_i + \varrho)$ teilbar.

Man zeigt nun leicht, dass die Zahl

$$N_{i-1} \cdot \frac{B_r}{p^{h_i}} = N_{i-1} \frac{\varphi(\vartheta)^r}{p^{h_i - \underbrace{\left\lceil \frac{(l_i - r)\, x_i}{\lambda_i} \right\rceil}}} = N_{i-1} \,.\, T_r^{(i)} = N_{i-1} \,.\, S_\varrho^{(i)}$$

ganz und durch ein Primideal der i^{ten} Seite genau in der Potenz ϱ teilbar ist. Dabei ist

$$\frac{B_r}{p^{h_i}} = \frac{\varphi(\vartheta)^r}{p^{h_i - \underbrace{\left\lceil \frac{(l_i - r)\, x_i}{\lambda_i} \right\rceil}}} = T_r^{(i)} = S_\varrho^{(i)}$$

gesetzt worden, und da man bemerkt, dass

[1] $[i]$ bezeichnet die grösste ganze rationale Zahl, welche in i enthalten ist.

$$h_i - \frac{\overline{|(l_i - r)\varkappa_i|}}{\lambda_i} = \left[h_i - \frac{(l_i - r)\varkappa_i}{\lambda_i}\right] = \left[\frac{r\varkappa_i}{\lambda_i}\right]$$

ist, so wird also

$$N_{i-1} \cdot \frac{B_r}{p^{h_i}} = N_{i-1} \,.\, T_r^{(i)} = N_{i-1} S_\varrho^{(i)} = N_{i-1} \cdot \frac{\varphi(\mathfrak{d})^r}{p^{\left[\frac{r\varkappa_i}{\lambda_i}\right]}}. \tag{31}$$

Um nun nachzuweisen, dass die Zahl (31) ganz ist, zeigt man, dass ein jeder Primidealdivisor von p^{h_i} im Zähler $N_{i-1} \,.\, B_r$ in einer höheren Potenz aufgeht. Ein Primideal, das nicht zu den Seiten $S_i, S_{i+1}, \ldots S_k$ gehört, geht nach Satz 3 sicher in N_{i-1} in einer höheren Potenz als in p^{h_i} auf. Ein Primideal der i^{ten} Seite geht in B_r in der Potenz $h_i \lambda_i + \varrho$, in p^{h_i} in der Potenz $h_i \,.\, \lambda_i$ auf, folglich ist die Differenz der Exponenten gleich ϱ. Wenn zuletzt $\mathfrak{p}$ ein Primideal der s^{ten} Seite ist, so wird in dem letzten Ausdrucke (31) $\varphi(\mathfrak{d})^r$ durch $\mathfrak{p}^{r \cdot \varkappa_s}$, der Nenner aber durch $\mathfrak{p}$ in der Potenz $\lambda_s \,.\, \left[\frac{r\varkappa_i}{\lambda_i}\right]$ teilbar, und die Differenz dieser Exponenten ist

$$r\varkappa_s - \lambda_s \,.\, \left[\frac{r\varkappa_i}{\lambda_i}\right] > r\varkappa_s - \lambda_s \cdot \frac{r\varkappa_i}{\lambda_i} = r\lambda_s \left(\frac{\varkappa_s}{\lambda_s} - \frac{\varkappa_i}{\lambda_i}\right) > 0,$$

wodurch die Behauptung erwiesen ist.

Bestimmt man nun die Zahlen r_ϱ so, dass

$$r_\varrho \,.\, \varkappa_i \equiv \varrho \pmod{\lambda_i} \qquad (\varrho = 1, 2, \ldots \lambda_i - 1) \tag{32}$$

so bilden folglich die Zahlen

$$\begin{aligned} K_1^{(i)} &= N_{i-1} \,.\, T_{r_1}^{(i)} = N_{i-1} \,.\, S_1^{(i)} \\ K_2^{(i)} &= N_{i-1} \,.\, T_{r_2}^{(i)} = N_{i-1} \,.\, S_2^{(i)} \\ &\cdots\cdots\cdots\cdots \\ K_{\lambda_i - 1}^{(i)} &= N_{i-1} \,.\, T_{r_{\lambda_i - 1}}^{(i)} = N_{i-1} \,.\, S_{\lambda_i - 1}^{(i)} \end{aligned}$$

eine Reihe von Zahlen mit den gewünschten Eigenschaften, d. h. K_ϱ ist genau durch $\mathfrak{p}^\varrho$ teilbar, wenn $\mathfrak{p}$ ein Primideal der i^{ten} Seite ist. Setzt man nun speziell $K_0 = 1$, so folgt nach Satz 4 wie in § 1, dass die $m \,.\, \varepsilon_i \,.\, \lambda_i = m \,.\, l_i$ Zahlen

$$N_{i-1} \,.\, K_\varrho^{(i)} \,.\, \theta_i(\mathfrak{d})^t \,.\, \mathfrak{d}^s \qquad (\varrho = 0, 1, \ldots \lambda_i - 1,\ t = 0, 1, \ldots \varepsilon_i - 1,\ s = 0, 1 \ldots m-1)$$

ein Fundamentalsystem für $P_i^{\lambda_i}$ bilden.

Man sieht aber ein, dass, wenn in (§ 2) ϱ ein vollständiges Restsystem (mod λ_i) durchläuft, dies auch mit den Zahlen r_ϱ der Fall ist. Da nun weiter die Ordnung der Zahlen eines Fundamentalsystems gleichgültig ist, so bilden folglich die Zahlen

$$N_{i-1} \cdot T_r^{(i)} \cdot \theta_i(\vartheta)^t \cdot \vartheta^s \qquad (r=0, 1, \ldots \lambda_i - 1,\ t=0, 1, \ldots \varepsilon_i - 1,\ s=0, 1 \ldots m-1) \tag{33}$$

dasselbe Fundamentalsystem für $P_i^{\lambda_i}$.

Wegen der späteren Anwendungen schreibe ich dieses System in der folgenden, symbolischen Weise vollständiger auf:

$$N_{i-1}\left\{\begin{array}{l} \quad 1, \vartheta, \ldots \vartheta^{m-1}, \theta_i, \theta_i \cdot \vartheta, \ldots \theta_i \vartheta^{m-1}, \ldots, \theta_i^{e_i-1}, \theta_i^{e_i-1} \cdot \vartheta, \ldots \theta_i^{e_i-1} \cdot \vartheta^{m-1} \\ T_1^{(i)} \quad (\text{———————} \rightarrow \text{———————}) \\ T_2^{(i)} \quad (\text{———————} \rightarrow \text{———————}) \\ \text{— —} \\ T_{\lambda_i-1}^{(i)} (\text{———————} \rightarrow \text{———————}) \end{array}\right\} \tag{34}$$

In den Parenthesen sollen dann dieselben Zahlen wie in der ersten Zeile stehen, und dann alle diese Zahlen mit $T_r^{(i)}$ $(r = 1, 2 \ldots \lambda_i - 1)$ multipliziert werden. Die grosse Klammer links bedeutet dabei, dass alle so entstehende Zahlen mit N_{i-1} multipliziert werden sollen.

Man kann nun den wichtigen Satz beweisen:

Wenn man für alle Seiten S_i des Polygones $(p, \varphi(x))$ und zwar für alle Primfunktionteiler $\varphi(x)$ von $f(x) \pmod p$ die Fundamentalsysteme (34) der Ideale $P_i^{\lambda_i}$ bestimmt, so bildet die Gesamtheit dieser Systeme ein Fundamentalsystem für die Primzahl p.

Die Richtigkeit dieses Satzes ist nachgewiesen, wenn man zeigt, dass eine lineare Summe dieser Zahlen mit ganzen, rationalen Koeffizienten nicht durch p teilbar sein kann, ausser wenn alle Koeffizienten durch p teilbar sind. Wenn nun $\mathfrak{a} = (p, \varphi(\vartheta)^e)$ einer der Idealdivisoren (5) von p ist, so muss also unsere lineare Summe durch $\mathfrak{a}$ teilbar sein. Wenn man aber die entsprechenden Systeme (34) für andere Primfunktionen als $\varphi(x)$ bildet, so sind nach Satz 3 alle entsprechenden Zahlen N_i sicher durch $\mathfrak{a}$ teilbar, und man braucht daher nur zu untersuchen, wann eine lineare Verbindung der Zahlen (34) $(i = 1, 2, \ldots k)$ durch $\mathfrak{a}$ teilbar sein kann. Da $\mathfrak{a}$ nach (11) durch alle Ideale $P_i^{\lambda_i}$ teilbar sein muss, untersucht man erstens, wann diese lineare Summe durch $P_1^{\lambda_1}$ teilbar ist. Nach

Satz 3 sind aber die Zahlen $N_1, N_2, \ldots N_{k-1}$ alle durch eine beliebig hohe Potenz eines jeden Primideals der ersten Seite teilbar, also sicher auch durch $P_1^{\lambda_1}$ teilbar, so dass man also nur zu untersuchen hat, wann eine lineare Verbindung der Zahlen (34) für $i = 1$ durch $P_1^{\lambda_1}$ teilbar ist. Da aber die Zahlen (34) für $i = 1$ ein Fundamentalsystem für das Ideal $P_1^{\lambda_1}$ bilden, so kann eine lineare Summe dieser Zahlen mit ganz rationalen Koeffizienten nur dann durch $P_1^{\lambda_1}$ teilbar werden, wenn alle Koeffizienten durch p teilbar sind.

Weiter untersucht man nun, wann diese lineare Summe, die wir hier betrachtet haben, durch $P_2^{\lambda_2}$ teilbar ist. Da alle Zahlen $N_2, N_3, \ldots N_{k-1}$ eine beliebig hohe Potenz von $P_2^{\lambda_2}$ enthalten, und da weiter in dem Teile der Summe, welcher den Gliedern (34) für $i = 1$ entspricht, wie eben bewiesen worden ist, alle Koeffizienten durch p teilbar sind, so braucht man um die Teilbarkeit durch $P_2^{\lambda_2}$ zu untersuchen, nur das System von Addenden in der Summe zu untersuchen, welches aus den Gliedern (34) für $i = 2$ entspringt. Da aber dieses System ein Fundamentalsystem für $P_2^{\lambda_2}$ bildet, so kann eine lineare Summe aus diesen Gliedern nicht durch $P_2^{\lambda_2}$ teilbar sein, ausser wenn alle Koeffizienten durch p teilbar sind usw. In derselben Weise beweist man dann, dass alle anderen Koeffizienten durch p teilbar sein müssen, d. h. dass die Zahlen (34), für alle Seiten und für alle Primfunktionen gebildet, zusammen ein Fundamentalsystem für p sind. W. z. b. w.

Das System (34) stimmt nun mit den Zahlen (33) vollständig überein, und da in (33)

$$T_r^{(i)} \cdot \theta_i(\vartheta)^t = \frac{\varphi(\vartheta)^r}{p^{\left\lfloor \frac{r x_i}{\lambda_i} \right\rfloor}} \cdot \frac{\varphi(\vartheta)^{t \cdot \lambda_i}}{p^{t \cdot x_i}} = \frac{\varphi(\vartheta)^{r+t\lambda_i}}{p^{\left\lfloor \frac{(r+t\lambda_i) \cdot x_i}{\lambda_i} \right\rfloor}} = T_{r+t\lambda_i}^{(i)}$$

ist, so stimmen die Zahlen (33) mit den Zahlen

$$N_{i-1} \cdot T_r^{(i)} \cdot \vartheta^s \qquad r = 0, 1, \ldots l_i - 1, (s = 0, 1, \ldots m-1)$$

vollständig überein. Daher ist bewiesen:

Satz 6. Wenn man für alle Seiten S_i des Polygones $(p, \varphi(x))$ und zwar für alle Primfunktionteiler $\varphi(x)$ von $f(x) \pmod p$ die Zahlen

$$N_{i-1} \cdot T_r^{(i)} \cdot \vartheta^s = N_{i-1} \frac{\varphi(\vartheta)^r}{p^{\left\lfloor \frac{r x_i}{\lambda_i} \right\rfloor}} \cdot \vartheta^s \qquad (r = 0, 1, 2 \ldots l_i - 1, s = 0, 1 \ldots m-1) \tag{35}$$

bestimmt, so bildet die Gesamtheit dieser Systeme ein Fundamentalsystem für die Primzahl p.

Dieser Satz gestattet also immer, wenn eine reguläre Gleichung vorliegt, ein Fundamentalsystem für die Primzahl p zu bestimmen.

§ 7.

Bestimmung des Primideals $\mathfrak{p}_j^{(i)}$.

Ich werde an dieser Stelle eine Darstellung des Primideals $\mathfrak{p}_j^{(i)}$ geben, welche man leicht aus den vorgehenden Untersuchungen ableitet. In § 5 ist gezeigt worden, dass die Zahl

$$M_i = N_{i-1} \cdot \theta_i(\vartheta) = N_{i-1} \cdot \frac{\varphi(\vartheta)^{\lambda_i}}{p^{\varkappa_i}}$$

ganz ist und durch alle Primidealteiler von p teilbar, ausser solchen, welche zur i^{ten} Seite gehören. Weiter ist auch die Zahl

$$N_{i-1} \cdot \frac{f_j^{(i)}(\vartheta)}{p^{\varepsilon_j^{(i)} \cdot \varkappa_i}} = N_{i-1}\left(\theta_i(\vartheta)^{\varepsilon_j^{(i)}} + S_{1,j}^{\varepsilon_j^{(i)}-1}(\vartheta) \cdot \theta_i(\vartheta)^{\varepsilon_j^{(i)}-1} + \cdots + S^{(i)}_{\varepsilon_j^{(i)},j}(\vartheta)\right)$$

ganz und durch das Primideal $\mathfrak{p}_j^{(i)}$, aber durch keine anderen Primideale der i^{ten} Seite teilbar. Weiter sieht man auch ein, dass diese Zahl nicht durch ein Primideal $\mathfrak{p}^{(s)}$ der s^{ten} Seite teilbar sein kann, wenn $s>i$ ist, denn alle Zahlen

$$N_{i-1} \cdot \theta_i(\vartheta)^{\varepsilon_j^{(i)}},\ N_{i-1} \cdot \theta_i(\vartheta)^{\varepsilon_j^{(i)}-1},\ \ldots\ N_{i-1} \cdot \theta_i(\vartheta)$$

sind nach § 5 durch $\mathfrak{p}^{(s)}$ teilbar, die Zahl $N_{i-1} \cdot S^{(i)}_{\varepsilon_j^{(i)},j}(\vartheta)$ ist aber sicher nicht durch $\mathfrak{p}^{(s)}$ teilbar. Nach diesen Bemerkungen sieht man leicht ein, dass das Ideal

$$\mathfrak{b} = [p, \varphi(\vartheta), M_1, M_2, \ldots M_{i-1}, N_{i-1} \cdot f_j^{(i)}(\vartheta, \theta_i(\vartheta))]$$

eine Potenz von $\mathfrak{p}_j^{(i)}$ ist. Denn $\mathfrak{b}$ kann zunächst nur durch Idealteiler von $(p, \varphi(\vartheta))$ teilbar sein, und wenn $\mathfrak{p}^{(s)}$ ein Primideal der s^{ten} Seite ist, $s<i$, so geht $\mathfrak{p}^{(s)}$ nicht in M_s auf, und wenn $s>i$ ist, geht $\mathfrak{p}^{(s)}$ nicht in $N_{i-1} S^{(i)}_{\varepsilon_j^{(i)},j}(\vartheta)$ auf. Das Ideal $\mathfrak{b}$ kann folglich nur durch Primideale der i^{ten} Seite teilbar sein, und da ausserdem das letzte Glied nur durch das Ideal $\mathfrak{p}_j^{(i)}$ der i^{ten} Seite teilbar ist, muss $\mathfrak{b}$ eine Potenz von $\mathfrak{p}_j^{(i)}$ sein.

Um daher eine Darstellung für $\mathfrak{p}_j^{(i)}$ zu gewinnen, braucht man nur eine ganze Zahl des Körpers zu bestimmen, welche nur durch die erste Potenz von $\mathfrak{p}_j^{(i)}$ teilbar ist.

Dies leistet aber nach § 6 die Zahl

$$N_{i-1} \cdot T_r^{(i)} = N_{i-1} \cdot \frac{\varphi(\vartheta)^r}{p^{\left[\frac{r\varkappa_i}{\lambda_i}\right]}},$$

wenn $0<r<\lambda_i$ so gewählt wird, dass $r\varkappa_i \equiv 1 \pmod{\lambda_i}$ ist.

Man hat daher den Satz:

Satz 7. Das Primideal $\mathfrak{p}_j^{(i)}$ ist durch

$$\mathfrak{p}_j^{(i)} = [p, \varphi(\vartheta), M_1, M_2, \ldots, M_{i-1}, N_{i-1} \cdot T_r^{(i)}, N_{i-1} \cdot f_j^{(i)}(\vartheta, \theta, (\vartheta))]$$

bestimmt, wo

$$T_r^{(i)} = \frac{\varphi(\vartheta)^r}{p^{\left[\frac{r\varkappa_i}{\lambda_i}\right]}}$$

ist und $r<\lambda_i$ der Kongruenz $r\varkappa_i \equiv 1 \pmod{\lambda_i}$ genügen soll.

Bei allen diesen Untersuchungen spielt der Exponent M, welcher durch die Kongruenzzerlegung des Satzes 1 von $f(x)$ eingeführt worden ist, eine wichtige Rolle. Man sieht aber leicht ein, dass es überall hinreichend ist, wenn man M grösser als alle Zahlen $h_1+h_2+\cdots+h_k$ wählt, welche durch die verschiedenen Polygone $(p, \varphi(x))$ von $f(x)$ definiert sind, also

$$M > \mathrm{Max}(h_1+h_2+\cdots+h_k).$$

Kap. 2. Bestimmung der Körperdiskriminante.

§ 1.

Hilfssätze über Diskriminanten.

Es sollen hier ein Paar Hilfssätze über Diskriminanten bewiesen werden, welche für die folgenden Untersuchungen notwendig sind.

Es sei wie in Kap. 1

$$f(x) \equiv F_1(x) \cdot F_2(x) \ldots F_s(x) \pmod{p^M},$$

wo

$$F_i(x) \equiv \varphi_i(x)^{e_i} \pmod{p},$$

und man setzt zur Abkürzung

$$\Pi_i(x) = F_1(x) \dots F_{i-1}(x) \cdot F_{i+1}(x) \dots F_s(x), \tag{36}$$

wo also

$$\Pi_i(x) = c_0^{(i)} + c_1^{(i)} \cdot x + \dots + c_{t_i-1}^{(i)} x^{t_i-1} + x^{t_i}$$

und

$$t_i = m_1 \cdot e_1 + m_2 \cdot e_2 + \dots + m_{i-1} \cdot e_{i-1} + m_{i+1} \cdot e_{i+1} + \dots + m_s \cdot e_s$$

ist. Der Kürze wegen soll auch

$$k_i = m_i \cdot e_i = n - t_i$$

gesetzt werden.

Weiter soll im Folgenden immer die Gleichungsdiskriminante der regulären Gleichung $f(x) = 0$ mit D bezeichnet werden.

Ich beweise dann:

Die beiden Diskriminanten

$$D = \Delta(1, \vartheta, \dots \vartheta^{n-1})$$

und

$$D' = \Delta(\dots \Pi_i(\vartheta), \Pi_i(\vartheta) \cdot \vartheta, \dots \Pi_i(\vartheta) \cdot \vartheta^{k_i-1}, \dots)$$

sind durch dieselbe Potenz der Primzahl p teilbar.

Die Diskriminante D' ist also die Diskriminante zu den n Zahlen

$$\Pi_i(\vartheta) \cdot \vartheta^t \qquad (i = 1, 2 \dots s, t = 0, 1, \dots k_i - 1).$$

Nach einem bekannten Satze über Diskriminanten ist nun

$$D' = K^2 \cdot D, \tag{37}$$

wo K die Determinante

$$K = \begin{vmatrix} c_0^{(1)}, c_1^{(1)}, \dots c_{t_1}^{(1)}, & 0, \dots 0 \\ 0, c_0^{(1)}, \dots c_{t_1-1}^{(1)}, & c_{t_1}^{(1)}, \dots 0 \\ \dots\dots\dots\dots\dots & \\ 0, \quad 0, \dots & c_t^{(1)}, \\ \dots\dots\dots\dots\dots & \\ c_0^{(i)}, c_1^{(i)}, \dots c_{t_i}^{(i)}, & 0 \dots 0 \\ 0, c_0^{(i)}, \dots c_{t_i-1}^{(i)}, & c_{t_i}^{(i)}, \dots 0 \\ \dots\dots\dots\dots\dots & \\ 0, \quad 0, \dots & c_{t_i}^{(i)} \\ \dots\dots\dots\dots\dots & \end{vmatrix}$$

bezeichnet, worin der Übersicht wegen überall $c_{i_i}^{(i)}$ an die Stelle des Koeffizienten 1 des höchsten Gliedes in $\Pi_i(x)$ gesetzt worden ist.

Um den Hilfssatz zu beweisen, braucht man daher nur zu zeigen, dass die Determinante K nicht durch p teilbar ist. Wenn aber nun K durch p teilbar wäre, so könnte man die n Zahlen

$$b_0^{(i)}, b_1^{(i)}, \ldots b_{k_i-1}^{(i)} \qquad (i = 1, 2 \ldots s)$$

so bestimmen, dass sie nicht alle durch p teilbar sind und den Kongruenzen

$$\left.\begin{array}{ll} b_0^{(1)} \cdot c_0^{(1)} + \cdots & + b_0^{(i)} \cdot c_0^{(i)} + \cdots \equiv 0 \\ b_0^{(1)} \cdot c_1^{(1)} + b_1^{(1} \cdot c_0^{(1)} + \cdots & + b_0^{(i)} \cdot c_1^{(i)} + b_1^{(i)} \cdot c_0^{(i)} + \cdots \equiv 0 \\ b_0^{(1)} \cdot c_2^{(1)} + b_1^{(1)} \cdot c_1^{(1)} + b_2^{(1)} \cdot c_0^{(1)} + \cdots & + b_0^{(i)} \cdot c_2^{(i)} + b_1^{(i)} \cdot c_1^{(i)} + b_2^{(i)} \cdot c_0^{(i)} + \cdots \equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots & \end{array}\right\} (\mathrm{mod}\ p)$$

genügen, indem nämlich die Determinante dieses Systems von linearen Kongruenzen gleich K ist. Multipliziert man aber die erste dieser Kongruenzen mit 1, die zweite mit x, die dritte mit x^2 usw., und summiert, so folgt auch die Kongruenz

$$\begin{array}{l} b_0^{(1)} \cdot \Pi_1(x) + b_1^{(1)} \cdot x \cdot \Pi_1(x) + \cdots + b_{k_1-1}^{(1)} \cdot x^{k_1-1} \cdot \Pi_1(x) \\ + \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ + b_0^{(i)} \cdot \Pi_i(x) + b_1^{(i)} \cdot x \cdot \Pi_i(x) + \cdots + b_{k_i-1}^{(i)} \cdot x^{k_i-1} \cdot \Pi_i(x) \\ + \cdots\cdots\cdots\cdots\cdots\cdots\cdots \equiv 0 \ (\mathrm{mod}\ p) . \end{array}$$

Wird nun hier

$$b_i(x) = b_0^{(i)} + b_1^{(i)} \cdot x + \cdots + b_{k_i-1}^{(i)} \cdot x^{k_i-1} \qquad (i = 1, 2 \ldots s)$$

gesetzt, so folgt also

$$b_1(x) \cdot \Pi_1(x) + b_2(x) \cdot \Pi_2(x) + \cdots + b_s(x) \cdot \Pi_s(x) \equiv 0 \ (\mathrm{mod}\ p)$$

wo die Polynome $b_i(x)$ nicht alle (mod p) verschwinden können. Das Bestehen einer solchen Kongruenz ist aber nicht möglich. Denn wenn z. B. $b_i(x)$ nicht (mod p) verschwindet, so folgt, da alle Polynome $\Pi_1(x), \ldots \Pi_{i-1}(x); \Pi_{i+1}(x) \ldots \Pi_s(x)$ (mod p) durch $\varphi_i(x)^{e_i}$ teilbar sind, dass auch das Polynom $b_i(x) \cdot \Pi_i(x)$ (mod p) durch $\varphi_i(x)^{e_i}$ teilbar sein muss. Da nun $\Pi_i(x)$ nicht durch $\varphi_i(x)$ (mod p) teilbar ist, so folgt, dass $b_i(x)$ (mod p) durch $\varphi_i(x)^{e_i}$ teilbar sein muss, was jedoch nicht möglich ist, da der Grad von $\varphi_i(x)^{e_i}$ grösser als der Grad von $b_i(x)$ ist. Daher kann also K nicht durch p teilbar sein.

Es soll nun weiter ein anderer einfacher Hilfssatz bewiesen werden:
Wenn

$$f_0(x) = 1$$
$$f_1(x) = x + a_1^{(1)}$$
$$\cdots\cdots\cdots$$
$$f_{k_i-1}(x) = x^{k_i-1} + \cdots + a_{k_i-1}^{(k_i-1)}$$

ist, und wenn die Diskriminante der n Zahlen

$$\Pi_i(\vartheta) \cdot f_t(\vartheta) \qquad (i = 1, 2 \ldots s, t = 0, 1, \ldots k_i - 1)$$

mit

$$D'' = \Delta(\ldots, \Pi_i(\vartheta) f_0(\vartheta), \Pi_i(\vartheta) \cdot f_1(\vartheta), \ldots \Pi_i(\vartheta) \cdot f_{k_i-1}(\vartheta), \ldots)$$

bezeichnet wird, so ist

$$D' = D''. \tag{38}$$

Dies sieht man einfach ein, wenn man beachtet, dass man wegen der Determinantenform der Diskriminante in einer Diskriminante $\Delta(\alpha_1, \alpha_2, \ldots \alpha_n)$ von einem Elemente α_r ein beliebiges Multiplum $k \cdot \alpha_s$ eines anderen Elements subtrahieren darf, ohne den Wert der Diskriminante zu ändern.

Multipliziert man daher $\Pi_i(\vartheta) \cdot f_0(\vartheta) = \Pi_i(\vartheta)$ mit $a_1^{(1)}$ und zieht diese Zahl von $\Pi_i(\vartheta) \cdot f_1(\vartheta)$ ab, so erhält man die Zahl $\Pi_i(\vartheta) \cdot \vartheta$. Multipliziert man weiter $\Pi_i(\vartheta)$ mit $a_2^{(2)}$ und $\Pi_i(\vartheta) \cdot \vartheta$ mit $a_1^{(2)}$ und zieht diese Glieder von $\Pi_i(\vartheta) \cdot f_2(\vartheta)$ ab, so ergibt sich $\Pi_i(\vartheta) \cdot \vartheta^2$ usw. Man hat folglich

$$D'' = \Delta(\ldots \Pi_i(\vartheta), \Pi_i(\vartheta) \cdot \vartheta, \ldots \Pi_i(\vartheta) \cdot \vartheta^{k_i-1}, \ldots) = D'.$$

§ 2.

Bestimmung des Index.

Bezeichnet man die Körperdiskriminante mit d, so besteht zwischen d und der Gleichungsdiskriminante D die Beziehung

$$D = k^2 \cdot d, \tag{39}$$

wo k der *Index* der Zahl ϑ heisst. Durch diese Gleichung soll nun die Körperdiskriminante d bestimmt werden, indem man erst die Zahlen D und k bestimmt. Zunächst soll hier die Zahl k untersucht werden, und es soll gezeigt werden,

wie man einen ganz einfachen Ausdruck für die Potenz bestimmen kann, in welcher die Primzahl p in k aufgeht.

Durch Satz 6 ist ein Fundamentalsystem (mod p) bestimmt worden, und nach Kap. 1, § 1 folgt, dass die Körperdiskriminante und die Diskriminante eines Fundamentalsystems für p durch dieselbe Potenz von p teilbar sind.

Die Diskriminante d' des Fundamentalsystems ist also die Diskriminante zu den Zahlen

$$N_{i-1}\cdot\frac{\varphi(\vartheta)^r}{p^{\left[\frac{r\varkappa_i}{\lambda_i}\right]}}\vartheta^s \qquad (r=0,1,\dots l_i-1, s=0,1,\dots m-1), \quad (40)$$

wenn diese für $i=1,2,\dots k$ und für alle Primfunktionteiler $\varphi(x)$ von $f(x)$ (mod p) gebildet werden.

Die Zahlen (40) sind ganz algebraisch, aber, wie man sieht, nicht als Polynome in ϑ ausgedrückt, indem eine gewisse Potenz der Primzahl p als Nenner in (40) vorkommt. Es soll nun d' mit einer solchen Potenz von p multipliziert werden, dass alle Elemente (40) auch Polynome in ϑ werden. Man sieht ein, dass man um dies zu erreichen, mit einer Potenz von p multiplizieren muss, welche gleich dem Quadrate des Produktes von allen Nennern in (40) ist. Um diese Potenz von p zu bestimmen, muss man daher einen Ausdruck für das Produkt der Nenner der Zahlen (40) ableiten.

Nach Satz 3 kommt in N_{i-1} die Potenz

$$p^{h_1+h_2+\cdots+h_{i-1}}$$

als Nenner vor, und der Nenner einer Zahl (40) ist daher gleich

$$p^{h_1+h_2+\cdots+h_{i-1}+\left[\frac{r\varkappa_i}{\lambda_i}\right]}.$$

Nimmt man nun erstens die Zahl r in (40) fest an, und bildet das Produkt der Nenner, wenn s die Werte $0,1,\dots m-1$ durchläuft, so wird dieses Produkt

$$p^{m\left(h_1+h_2+\cdots+h_{i-1}+\left[\frac{r\varkappa_i}{\lambda_i}\right]\right)}. \quad (41)$$

Bildet man nun weiter das Produkt aller Zahlen (41) für $r=0,1,\dots l_i-1$, so ergibt sich eine Potenz von p, wo der Exponent den Wert

$$m\,l_i\,(h_1+h_2+\cdots+h_{i-1})$$
$$+m\left(\left[\frac{x_i}{\lambda_i}\right]+\left[\frac{2\,x_i}{\lambda_i}\right]+\cdots+\left[\frac{(l_i-1)\,x_i}{\lambda_i}\right]\right) \tag{42}$$

hat. Der Summe

$$L_i=l_i\,(h_1+\cdots+h_{i-1})+\left[\frac{x_i}{\lambda_i}\right]+\left[\frac{2\,x_i}{\lambda_i}\right]+\cdots+\left[\frac{(l_i-1)\,x_i}{\lambda_i}\right] \tag{43}$$

kann man auch eine ganz einfache geometrische Deutung geben. Es ist nämlich dies die Anzahl der Gitterpunkte, welche in dem Polygone $(p, \varphi(x))$ von $f(x)$ zwischen der Seite S_i und ihrer Projektion auf die X-achse liegen. Dabei werden alle Gitterpunkte mitgerechnet, welche auf der Seite S_i oder auf der Ordinate des Anfangspunktes der Seite liegen, aber keine solche, die auf der X-achse oder auf der Ordinate des Endpunktes von S_i liegen.

Man kann aber auch einen expliziten Ausdruck für die Summe

$$M_i=\left[\frac{x_i}{\lambda_i}\right]+\left[\frac{2\,x_i}{\lambda_i}\right]+\cdots+\left[\frac{(l_i-1)\,x_i}{\lambda_i}\right]$$

bestimmen, welche in dem Ausdruck (43) für L_i vorkommt. Diese Summe bezeichnet nämlich die Hälfte der Anzahl der Gitterpunkte, welche innerhalb eines Rechtecks mit den Seiten l_i und h_i liegen, indem jedoch dabei die Anzahl der Gitterpunkte auf der einen Diagonale doppelt mitgerechnet werden. Da nun die Gesamtzahl der Gitterpunkte innerhalb des Rechtecks gleich $(h_i-1)\,(l_i-1)$ ist und die Anzahl der Gitterpunkte auf einer Diagonale (Endpunkte nicht mitgerechnet) gleich ε_i-1 ist, so wird

$$M_i=\frac{(h_i-1)\,(l_i-1)+\varepsilon_i-1}{2}=\frac{1}{2}\,(h_i\,l_i-l_i-h_i+\varepsilon_i),$$

und man hat daher für den Exponenten (42) den Ausdruck

$$m\,.\,L_i=m\left(l_i\,(h_1+\cdots+h_{i-1})+\frac{1}{2}\,(h_i\,l_i-h_i-l_i+\varepsilon_i)\right). \tag{44}$$

Bildet man nun die entsprechenden Produkte für alle Seiten und multipliziert man diese mit einander, so erhält man eine Potenz von p, wo der Exponent den Wert

$$m(L_1+L_2+\cdots+L_k)=m\Big(l_2h_1+l_3(h_1+h_2)+\cdots+l_k(h_1+h_2+\cdots+h_{k-1})+ \\ +\frac{1}{2}\Big(\sum_{i=1}^{k}h_il_i-\sum_{i=1}^{k}(l_i+h_i)+\sum_{i=1}^{k}\varepsilon_i\Big)\Big) \tag{45}$$

hat. Setzt man hier

$$L=L_1+L_2+\cdots+L_k,$$

so folgt wegen der Bedeutung der Zahlen L_i, *dass L die Anzahl der Gitterpunkte angibt, welche zwischen dem Polygone und der X-achse liegen. Dabei sollen solche Gitterpunkte nicht mitgerechnet werden, welche auf der X-achse oder auf der Ordinate des Endpunktes des Polygons liegen, wohl aber solche, die auf dem Polygone selbst liegen (vom Anfangspunkte und Endpunkte abgesehen).*

Dies zeigt also, dass das Produkt aller Nenner der Zahlen (40), wenn diese für alle Primfunktiondivisoren $\varphi(x)$ von $f(x)$ (mod p) gebildet werden, gleich $p^{\Sigma m\cdot L}$ ist, wo die Summe über alle Primfunktionen $\varphi(x)$ erstreckt werden soll. Daraus folgt, dass man die Diskriminante d' des Fundamentalsystems mit $p^{2\Sigma m\cdot L}$ multiplizieren muss, damit alle Elemente (40) Polynome in ϑ werden. Wenn man nun d' mit dieser Potenz multipliziert, geht sie nach Satz 3 in die Diskriminante der Zahlen

$$\Pi(\vartheta)\,.\,\Phi_1(\vartheta)\,.\,\Phi_2(\vartheta)\cdots\Phi_{i-1}(\vartheta)\,.\,\varphi(\vartheta)^r\,.\,\vartheta^s \tag{46}$$

$$(i=1,\,2,\cdots k,\;\; r=0,\,1,\cdots l_i-1,\;\; s=0,\,1,\cdots m-1)$$

über, wo also die Zahl $\Pi(\vartheta)$ durch (36) definiert ist. Man hat folglich

$$p^{2\Sigma m\cdot L}\,d'=d'',$$

wo d'' die Diskriminante der Zahlen (46) bezeichnet. Wendet man aber nun den zweiten Hilfssatz des Kap. 2. § 1 auf die Diskriminante d'' der Zahlen (46) an, so folgt, dass diese gleich der Diskriminante der Zahlen

$$\Pi_j(\vartheta)\,.\,\vartheta^s\;(s=0,\,1\cdots k_j)$$

ist, welche in Kap. 2. § 1 mit D' bezeichnet wurde.

Man hat folglich

$$p^{2\,.\,\Sigma m\,.\,L}\,.\,d'=D'.$$

Nach Kap. 2. § 1 ist weiter $D'=K^2\,.\,D$, wo D die Gleichungsdiskriminante und K nicht durch p teilbar ist, folglich auch

$$D \cdot K^2 = p^{2 \cdot \Sigma m \cdot L} \cdot d'.$$

Da nun d' dieselbe Potenz der Primzahl p wie die Körperdiskriminante d enthält, so folgt der Satz:

Satz 8. Der Index einer Zahl ϑ, welche der in Bezug auf p regulären Gleichung $f(x)=0$ genügt, ist durch die Potenz

$$p^{\Sigma m \cdot L}$$

der Primzahl p genau teilbar. Dabei bedeutet m den Grad der Primfunktionteiler $\varphi(x)$ von $f(x)$ (mod p), und L bedeutet die Anzahl der Gitterpunkte, welche zwischen dem Hauptpolygone $(p, \varphi(x))$ von $f(x)$ und der X-achse liegen, indem diese Anzahl in der oben angegebenen Weise berechnet wird. Für diese Zahl L hat man auch den Ausdruck

$$L = l_2 h_1 + l_3 (h_1 + h_2) + \cdots + l_k (h_1 + \cdots + h_{k-1})$$

$$+ \frac{1}{2} \sum_{i=1}^{k} (h_i l_i - h_i - l_i + \varepsilon_i).$$

§ 3.

Bestimmung der Differente der Zahl ϑ.

Durch den Satz 8 ist der Index der Zahl ϑ vollständig bestimmt, und dadurch sind auch prinzipiell die Schwierigkeiten der Bestimmung der Körperdiskriminante überwunden, da man immer die Gleichungsdiskriminante aus den Koeffizienten berechnen kann.

Es soll aber hier auch gezeigt werden, wie es möglich ist, die Gleichungsdiskriminante mittels der hier entwickelten Theorie über Polygone zu bestimmen.

Da bekanntlich

$$D = \pm N(f'(\vartheta)) \tag{47}$$

ist, sollen erstens die Primidealteiler der *Differente* $f'(\vartheta)$ von ϑ bestimmt werden. Nach Satz 1 ist

$$f'(\vartheta) \equiv F_1'(\vartheta) \cdot F_2(\vartheta) \cdots F_s(\vartheta) + F_1(\vartheta) \cdot F_2'(\vartheta) \cdots F_s(\vartheta)$$

$$+ \cdots + F_1(\vartheta) \cdot \cdots F_{s-1}(\vartheta) \cdot F_s'(\vartheta) \qquad (\text{mod } p^M),$$

und wenn $\mathfrak{p}_i$ ein Primidealteiler von $(p, \varphi_i(\vartheta))$ ist, so geht dieser in der Zahl $F_i(\vartheta)$ in einer beliebig hohen Potenz auf. Die Potenz von $\mathfrak{p}_i$, welche in $f'(\vartheta)$ aufgeht, wird daher gleich der Potenz, in welcher $\mathfrak{p}_i$ in der Zahl

$$F_1(\vartheta)\cdots F_{i-1}(\vartheta)\,F_i'(\vartheta)\,.\,F_{i+1}(\vartheta)\cdots F_s(\vartheta)$$

aufgeht. Setzt man daher wie früher

$$F(x)=F_i(x)$$
$$\Pi(x)=F_1(x)\cdots F_{i-1}(x)\,.\,F_{i+1}(x)\cdots F_s(x),$$

so soll man also die Zahl

$$\Pi(\vartheta)\,.\,F'(\vartheta)$$

untersuchen. Hier ist aber $\Pi(\vartheta)$ durch kein Primideal teilbar, das in $(p, \varphi(\vartheta))$ aufgeht, und man braucht daher nur den Faktor $F'(\vartheta)$ zu untersuchen.

Nach Satz 1 ist nun weiter

$$F'(\vartheta)\equiv \Phi'_1(\vartheta)\,.\,\Phi_2(\vartheta)\cdots\Phi_k(\vartheta)+\Phi_1(\vartheta)\,.\,\Phi'_2(\vartheta)\cdots\Phi_k(\vartheta)$$
$$+\cdots+\Phi_1(\vartheta)\cdots\Phi_{k-1}(\vartheta)\,.\,\Phi'_k(\vartheta) \qquad (\mathrm{mod}\ p^M),$$

und man soll untersuchen, in welcher Potenz $F'(\vartheta)$ durch ein Primideal $\mathfrak{p}_j^{(i)}$ der i^{ten} Seite teilbar ist. Da aber die Zahl $\Phi_i(\vartheta)$ durch eine beliebig hohe Potenz von $\mathfrak{p}_j^{(i)}$ teilbar ist, so wird durch das Glied

$$\Phi_1(\vartheta)\cdots\Phi_{i-1}(\vartheta)\,.\,\Phi'_i(\vartheta)\,\Phi_{i+1}\cdots\Phi_k(\vartheta)$$

bestimmt, in welcher Potenz $\mathfrak{p}_j^{(i)}$ in $F'(\vartheta)$ vorkommt. Nach Satz 2. § 4 folgt aber, dass die Zahl

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

durch $\mathfrak{p}_j^{(i)}$ in der Potenz

$$(h_1+h_2+\cdots+h_{i-1})\,\lambda_i+(l_{i+1}+l_{i+2}+\cdots+l_k)\,\varkappa_i \qquad (48)$$

teilbar ist.

Es bleibt daher nur übrig, die Zahl $\Phi'_i(\vartheta)$ zu untersuchen. Nach Satz 1 ist weiter

$$\Phi'_i(\vartheta)\equiv \Phi'^{(i)}_1(\vartheta)\,\Phi^{(i)}_2(\vartheta)\cdots\Phi_{t_i}(\vartheta)+\Phi^{(i)}_1(\vartheta)\,.\,\Phi'^{(i)}_2(\vartheta)\cdots\Phi_{t_i}(\vartheta)$$
$$+\cdots+\Phi^{(i)}_1(\vartheta)\cdots\Phi^{(i)}_{t_{i-1}}(\vartheta)\,.\,\Phi'^{(i)}_{t_i}(\vartheta) \qquad (\mathrm{mod}\ p^M),$$

43—2454. *Acta mathematica.* 45. Imprimé le 11 avril 1925.

und da hier $\Phi_i^{(j)}(\vartheta)$ immer durch eine beliebig hohe Potenz von $\mathfrak{p}_j^{(i)}$ teilbar ist, so bestimmt die Zahl

$$\Phi_1^{(i)}(\vartheta)\cdots\Phi_{j-1}^{(i)}(\vartheta)\,\Phi_j'^{(i)}(\vartheta)\,\Phi_{j+1}^{(i)}(\vartheta)\cdots\Phi_{t_i}^{(i)}(\vartheta),$$

in welcher Potenz $\mathfrak{p}_j^{(i)}$ in $\Phi_j^{(i)}(\vartheta)$ vorkommt. Nach § 5. Kap. 1 ist aber die Zahl $\Phi_{j_1}^{(i)}(\vartheta)$ durch das Primideal $\mathfrak{p}_j^{(i)}$ in genau der Potenz $\varepsilon_{j_1}^{(i)}\cdot\lambda_i\cdot\varkappa_i$ teilbar, und daher wird die Zahl

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

durch $\mathfrak{p}_j^{(i)}$ in genau der Potenz

$$\lambda_i\cdot\varkappa_i(\varepsilon_1^{(i)}+\varepsilon_2^{(i)}+\cdots+\varepsilon_{j-1}^{(i)}+\varepsilon_{j+1}^{(i)}+\cdots+\varepsilon_{t_i}^{(i)})=\lambda_i\cdot\varkappa_i(\varepsilon_i-\varepsilon_j^{(i)}) \tag{49}$$

teilbar.

Die Untersuchung der Zahl $f'(\vartheta)$ ist daher auf die Bestimmung der Potenz, in welcher $\mathfrak{p}_j^{(i)}$ in $\Phi_j'^{(i)}(\vartheta)$ aufgeht, vollständig zurückgeführt.

Um nun diesen Exponenten zu bestimmen, setzt man für den Augenblick $\varepsilon_j^{(i)}=\varepsilon$ und $\Phi_j^{(i)}(x)=\Phi(x)$. Da nun $\Phi(x)$ ein geradliniges Polygon mit der Neigungszahl $\frac{\varkappa_i}{\lambda_i}$ besitzt, so kann man $\Phi(x)$ in der Form

$$\Phi(x)=\varphi(x)^{\varepsilon\cdot\lambda_i}+A_1(x)\cdot p^{\overline{\frac{\varkappa_i}{\lambda_i}}}\cdot\varphi(x)^{\varepsilon\cdot\lambda_i-1}+A_2(x)\,p^{\overline{\frac{2\varkappa_i}{\lambda_i}}}\cdot\varphi(x)^{\varepsilon\cdot\lambda_i-2}+\cdots+A_{\varepsilon\cdot\lambda_i}(x)\cdot p^{\varepsilon\cdot\varkappa_i} \tag{50}$$

annehmen, wo $A_{\varepsilon\cdot\lambda_i}(x)\not\equiv 0 \pmod{p,\varphi(x)}$. Weiter hat man für das geradlinige Polygon S von $\Phi(x)$:

$$\Phi(x)\equiv f_j^{(i)}(x)\equiv\varphi(x)^{\varepsilon\cdot\lambda_i}+A_{\lambda_i}\cdot p^{\varkappa_i}\cdot\varphi(x)^{(\varepsilon-1)\lambda_i}+\cdots+A_{\varepsilon\cdot\lambda_i}(x)\cdot p^{\varepsilon\cdot\varkappa_i}\pmod{S}.$$

Man bildet nun nach (50)

$$\Phi'(x)=\varepsilon\cdot\lambda_i\cdot\varphi'(x)\cdot\varphi(x)^{\varepsilon\cdot\lambda_i-1}+(A'_1(x)\varphi,(x)+(\varepsilon\cdot\lambda_i-1)\,A_1(x)\cdot\varphi'(x))\,p^{\overline{\frac{\varkappa_i}{\lambda_i}}}\cdot\varphi(x)^{\varepsilon\cdot\lambda_i-2}+\cdots+A_{\varepsilon\cdot\lambda_i}(x)\cdot p^{\varepsilon\cdot\varkappa_i}$$

oder auch

$$\varphi(x)\cdot\Phi'(x)=\varepsilon\cdot\lambda_i\cdot\varphi'(x)\cdot\varphi(x)^{\varepsilon\cdot\lambda_i}+B_1(x)\cdot p^{\left[\frac{\varkappa_i}{\lambda_i}\right]}\cdot\varphi(x)^{\varepsilon\cdot\lambda_i-1}+B_2(x)\cdot p^{\left[\frac{2\varkappa_i}{\lambda_i}\right]}\cdot\varphi(x)^{\varepsilon\cdot\lambda_i-2}+\cdots+B_{\varepsilon\cdot\lambda_i}(x),$$

wo allgemein

$$B_t(x)=A'_t(x)\,.\,\varphi(x)+(\varepsilon\,\lambda_i-t)\,A_i(x)\,\varphi'(x)$$

gesetzt worden ist, wo also speziell

$$B_{\varepsilon\,.\,\lambda_i}(x)=A'_{\varepsilon\,.\,\lambda_i}(x)\,.\,\varphi(x)$$

ist. Das Polynom $\Phi'(x)\,\varphi(x)$ hat folglich auch das geradlinige Polygon S, und man sieht leicht ein, dass man für die Glieder, welche auf S liegen, die Kongruenz

$$K(x)\equiv\varphi(x)\,.\,\Phi'\,.(x)=\varepsilon\,.\,\lambda_i\,.\,\varphi'(x)\,\varphi(x)^{\varepsilon\,.\,\lambda_i}+(\varepsilon-1)\,\lambda_i\,.\,\varphi'(x)\,.\,A_{\lambda_i}(x)\,.\,p^{\varkappa_i}\,.\,\varphi(x)^{(\varepsilon-1)\,\lambda_i}$$
$$+\cdots+\lambda_i\,.\,\varphi'(x)\,.\,A_{(\varepsilon-1)\,\lambda_i}\,.\,p^{(\varepsilon-1)\,\varkappa_i}\,.\,\varphi(x)^{\lambda_i}\qquad(\mathrm{mod}\ S)\qquad(51)$$

hat. Setzt man nun $x=\vartheta$, so werden in $\varphi(\vartheta)\,.\,\Phi'(\vartheta)$ alle Glieder, welche auf S liegen, durch $\mathfrak{p}_j^{(i)}$ in der Potenz $\varepsilon\,.\,\varkappa_i\,.\,\lambda_i$ genau teilbar, während alle anderen Glieder durch höhere Potenzen von $\mathfrak{p}_j^{(i)}$ teilbar sind. Nach (51) ist aber die Summe der Glieder auf S gleich

$$\lambda_i\,\varphi'(\vartheta)\,(\varepsilon\,.\,\varphi(\vartheta)^{\varepsilon\,.\,\lambda_i}+(\varepsilon-1)\,A_{\lambda_i}(\vartheta)\,.\,p^{\varkappa_i}\,.\,\varphi(\vartheta)^{(\varepsilon-1)\,\lambda_i}+\cdots+A_{(\varepsilon-1)\,\lambda_i}\,.\,p^{(\varepsilon-1)\,\varkappa_i}\,.\,\varphi(\vartheta)^{\lambda_i}),$$

und wenn daher λ_i nicht durch p teilbar ist, wird diese Summe genau durch $\mathfrak{p}_j^{(i)^{\varepsilon\,.\,\lambda_i\,.\,\varkappa_i}}$ teilbar. Denn wenn diese Summe durch eine höhere Potenz von $\mathfrak{p}_j^{(i)}$ teilbar sein soll, muss $K(x)$ nach Kap. 1. § 5 durch $f_j^{(i)}(x)$ (mod S) teilbar sein, was aber nach (51) nicht möglich ist. Es folgt daher, dass $\Phi'(\vartheta)$ in diesem Falle genau durch $\mathfrak{p}_j^{(i)^{\varepsilon\,.\,\varkappa_i\,\lambda_i-\varkappa_i}}$ teilbar ist.

Wenn aber λ_i durch p teilbar ist, gibt es keine Glieder auf S, und folglich ist $\Phi'(\vartheta)\,.\,\varphi(\vartheta)$ durch $\mathfrak{p}_j^{(i)^{\varepsilon\,\varkappa_i\,\lambda_i+\varrho}}$ teilbar, wo $\varrho>0$ ist; dies zeigt, dass $\Phi'(\vartheta)$ durch $\mathfrak{p}_j^{(i)^{\varepsilon\,\varkappa_i\,\lambda_i-\varkappa_i+\varrho}}$ teilbar ist.

Addiert man nun die Zahlen (48) und (49) und noch dazu $\varepsilon_j^{(i)}\,.\,\varkappa_i\,\lambda_i-\varkappa_i+\varrho_j^{(i)}$, so erhält man die Summe

$$(h_1+h_2+\cdots+h_{i-1})\,\lambda_i+(l_{i+1}+\cdots+l_k)\varkappa_i+h_i\,.\,\lambda_i-\varkappa_i+\varrho_j^{(i)},$$

und es ist bewiesen:

Satz 9. Die Differente $f'(\vartheta)$ der Zahl ϑ ist durch das Primideal $\mathfrak{p}_j^{(i)}$ in einer Potenz mit dem Exponenten

$$(h_1+h_2+\cdots+h_i)\,\lambda_i+(l_{i+1}+\cdots+l_k)\,\varkappa_i-\varkappa_i+\varrho_j^{(i)}$$

genau teilbar, wobei $\varrho_j^{(i)}=0$ *ist, wenn* λ_i *nicht durch* p *teilbar ist, und* $\varrho_j^{(i)}>0$, *wenn* λ_i *durch* p *teilbar ist.*

Es mag nun von Interesse sein, zu untersuchen wie man die Zahl $\varrho=\varrho_j^{(i)}$ bestimmen kann, wenn also vorausgesetzt wird, dass λ_i durch p teilbar ist. Die Zahl ϱ war dadurch bestimmt, dass die Zahl $\Phi'(\vartheta).\varphi(\vartheta)$ durch $\mathfrak{p}_j^{(i)\varepsilon\cdot\varkappa_i\cdot\lambda_i+\varrho}$ genau teilbar sein sollte.

Man dividiert nun das Polynom $\Phi'(x).\varphi(x)$ durch $\Phi(x)$ und erhält

$$H(x)=\Phi'(x).\varphi(x)-C(x).\Phi(x), \tag{52}$$

wo $H(x)$ von der Form

$$H(x)=H_1(x).p^{\alpha_1}.\varphi(x)^{\varepsilon\cdot\lambda_1-1}+H_2(x).p^{\alpha_2}.\varphi(x)^{\varepsilon\cdot\lambda_2-2}+\cdots+H_{\varepsilon\cdot\lambda_i}(x).p^{\alpha_{\varepsilon\cdot\lambda_i}}$$

ist, die Koeffizienten $H_t(x)$ höchstens vom $(m-1)^{\text{ten}}$ Grade sind und die Exponenten α_t so gewählt sein sollen, dass $H_t(x)$ nicht durch p teilbar ist. Die Punkte (t, α_t) müssen alle oberhalb S liegen, wenn vorausgesetzt wird, dass λ_i durch p teilbar ist.

Da die Zahl $\Phi'(\vartheta).\varphi(\vartheta)$ jedenfalls nur eine endliche Potenz von $\mathfrak{p}_j^{(i)}$ enthalten kann, und man weiter die Zahl M so wählen kann, dass $\Phi(\vartheta)$ durch eine beliebig hohe Potenz von $\mathfrak{p}_j^{(i)}$ teilbar ist, so müssen folglich die Zahlen $\Phi'(\vartheta)\varphi(\vartheta)$ und $H(\vartheta)$ nach (52) durch dieselbe Potenz von $\mathfrak{p}_j^{(i)}$ teilbar sein.

Ein Glied

$$H_t(\vartheta).p^{\alpha_t}.\varphi(\vartheta)^{\varepsilon\cdot\lambda_i-t} \tag{53}$$

in $H(\vartheta)$ ist nun durch $\mathfrak{p}_j^{(i)}$ in genau der Potenz

$$\alpha_t.\lambda_i+(\varepsilon.\lambda_i-t)\varkappa_i=\varepsilon.\lambda_i.\varkappa_i+r \tag{54}$$

teilbar. Wenn zwei Glieder (53) durch dieselbe Potenz von $\mathfrak{p}_j^{(i)}$ teilbar sind, so muss

$$\alpha_t.\lambda_i+(\varepsilon.\lambda_i-t)\varkappa_i=\alpha_{t'}.\lambda_i+(\varepsilon.\lambda_i-t')\varkappa_i$$

oder

$$(\alpha_{t'}-\alpha_t)\lambda_i=(t'-t)\varkappa_i$$

sein, woraus

$$\alpha_{t'}=\alpha_t+e.\varkappa_i$$

$$t'=t+e.\lambda_i$$

folgt, wobei e eine ganze rationale Zahl bedeutet. Diese Relationen zeigen, dass alle Punkte (t, α_t), wofür die Zahl r in (53) denselben Wert besitzt, auf einer zu S parallelen Geraden liegen müssen, und daraus folgt leicht, dass die Summe der Glieder in $H(\vartheta)$, welche durch $\mathfrak{p}_j^{(i)\varepsilon \cdot \lambda_i \cdot \varkappa_i + r}$ genau teilbar sind, die Form

$$\frac{p^\alpha}{\varphi(\vartheta)^t}\left(B_0(\vartheta) \cdot \varphi(\vartheta)^{\varepsilon \cdot \lambda_i} + B_1(\vartheta) \cdot p^{\varkappa_i} \cdot \varphi(\vartheta)^{(\varepsilon-1)\lambda_i} + \cdots + B_{\varepsilon-1}(\vartheta)\, p^{(\varepsilon-1)\varkappa_i} \cdot \varphi(\vartheta)^{\lambda_i}\right)$$

hat. Hier ist $t<\lambda_i$ und $\alpha\lambda_i - t \cdot \varkappa_i = r$ vorausgesetzt, und nicht alle Koeffizienten $B_i(x)$ sollen $\equiv 0 \pmod{p, \varphi(x)}$ sein. Dann muss diese Summe durch $\mathfrak{p}_j^{(i)\varepsilon \cdot \lambda_i \cdot \varkappa_i + r}$ genau teilbar sein, weil das Polynom

$$B_0(x) \cdot \varphi(x)^{\varepsilon \cdot \lambda_i} + B_1(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{(\varepsilon-1)\lambda_i} + \cdots + B_{\varepsilon-1}(x) \cdot p^{(\varepsilon-1)\varkappa_i} \varphi(x)^{\lambda_i}$$

offenbar nicht durch $f_j^{(i)}(x) \pmod S$ teilbar sein kann. Ist daher ϱ die kleinste unter den Zahlen $r = \alpha_t \cdot \lambda_i - t \cdot \varkappa_i$ in der Darstellung von $H(x)$, so wird folglich $H(\vartheta)$ genau durch $\mathfrak{p}_j^{(i)\varepsilon \cdot \varkappa_i \cdot \lambda_i + \varrho}$ teilbar.

Die Zahl $\varrho_j^{(i)}$ ist gleich der kleinsten unter den Zahlen

$$\alpha_t \cdot \lambda_i - t \cdot \varkappa_i \quad (t = 1, 2, \cdots \varepsilon).$$

§ 4.

Bestimmung der Gleichungsdiskriminante und der Körperdiskriminante.

Aus dem Satze 9 folgt nun leicht auch die Zusammenzetzung die Gleichungsdiskriminante, indem diese gleich der Norm der Differente ist. Da nun weiter $N\mathfrak{p}_j^{(i)} = p^{\varepsilon_j^{(i)} \cdot m}$ ist, so folgt nach dem erwähnten Satze, dass die Norm zu der Potenz von $\mathfrak{p}_j^{(i)}$, in welcher dieses Primideal in $f'(\vartheta)$ aufgeht, gleich einer Potenz von p mit dem Exponenten

$$m \cdot \varepsilon_j^{(i)}\left[(h_1 + h_2 + \cdots + h_{i-1})\lambda_i + h_i \cdot \lambda_i + (l_{i+1} + \cdots + l_k)\varkappa_i - \varkappa_i + \varrho_j^{(i)}\right]$$

ist. Bildet man nun das Produkt aller entsprechenden Normen für die Primideale der i^{ten} Seite, so ist $\sum_{j=1}^{t_i} \varepsilon_j^{(i)} = \varepsilon_i$, und es ergibt sich eine Potenz von p, wo der Exponent gleich

$$m\left[l_i(h_1+\cdots+h_{i-1})+h_i\,.\,l_i+(l_{i+1}+\cdots+l_k)\,h_i-h_i+\sum_{j=1}^{t_i}\varrho_j^{(i)}\,.\,\varepsilon_j^{(i)}\right]$$

wird. Wenn man dann weiter diese Normen für alle Seiten multipliziert, so ergibt sich der Exponent

$$\left.\begin{aligned}&m\Big[l_2\,.\,h_1+l_3(h_1+h_2)+\cdots+l_k(h_1+\cdots+h_{k-1})\\&+h_1(l_2+\cdots+l_k)+h_2(l_3+\cdots+l_k)+\cdots+h_{k-1}\,.\,l_k\\&+\sum_{i=1}^{k}h_i\,.\,l_i-\sum_{i=1}^{k}h_i+\sum_{i=1}^{k}\sum_{j=1}^{t_i}\varrho_j^{(i)}\,.\,\varepsilon_j^{(i)}\Big]\end{aligned}\right\}\quad(55)$$

für p. Nun ist aber, wie man leicht sieht,

$$\begin{aligned}&l_2\,h_1+l_3(h_1+h_2)+\cdots+l_k(h_1+\cdots+h_{k-1})\\&=h_1(l_2+\cdots+l_k)+h_2(l_3+\cdots+l_k)+\cdots+h_{k-1}\,.\,l_k,\end{aligned}$$

und folglich geht (55) in

$$\left.\begin{aligned}&m\Big[2\,(l_2\,h_1+l_3(h_1+h_2)+\cdots+l_k(h_1+\cdots+h_{k-1}))\\&\qquad+\sum_{i=1}^{k}h_i\,l_i-\sum_{i=1}^{k}h_i+\sum_{i=1}^{k}\sum_{j=1}^{t_i}\varrho_j^{(i)}\,.\,\varepsilon_j^{(i)}\Big]\end{aligned}\right\}\quad(56)$$

über. Führt man aber hier die Zahl L des Satzes 8 ein, so ergibt sich für (56) weiter der einfache Ausdruck

$$m\left[2\,L+\sum_{i=1}^{k}\left(l_i-\varepsilon_i+\sum_{j=1}^{t_i}\varepsilon_j^{(i)}\,.\,\varrho_j^{(i)}\right)\right].\qquad(57)$$

Diesem Ausdruck kann man aber auch eine andere Form geben, indem man

$$\varepsilon_i=\sum_{j=1}^{t_i}\varepsilon_j^{(i)},\quad l_i=\sum_{j=1}^{t_i}\varepsilon_j^{(i)}\,.\,\lambda_i$$

setzt, und (57) geht dann in

$$2\,m\,L+m\sum_{i=1}^{k}\sum_{j=1}^{t_i}(\lambda_i-1+\varrho_j^{(i)})\,\varepsilon_j^{(i)}$$

über, oder wenn man

$$\delta_j^{(i)}=\lambda_i-1+\varrho_j^{(i)}$$

setzt, in

$$2mL+m\sum_{i=1}^{k}\sum_{j=1}^{t_i}\delta_j^{(i)}\cdot\varepsilon_j^{(i)}.$$

Satz 10. Die Gleichungsdiskriminante D ist durch die Primzahl p in der Potenz mit dem Exponenten

$$\sum_m\left(2mL+m\sum_{i=1}^{k}\sum_{j=1}^{t_i}\delta_j^{(i)}\cdot\varepsilon_j^{(i)}\right)$$

genau teilbar. Dabei bedeutet $\delta_j^{(i)}=\lambda_i-1+\varrho_j^{(i)}$, wo $\varrho_j^{(i)}=0$, wenn λ_i nicht durch p teilbar ist, und $\varrho_j^{(i)}>0$, wenn λ_i durch p teilbar ist; in diesem letzten Falle kann die Zahl $\varrho_j^{(i)}$ immer wie in § 3 berechnet werden.

In diesem Satze bedeutet das äussere Summenzeichen natürlich, dass für alle verschiedenen Primfunktionteiler $\varphi(x)$ von $f(x)$ (mod p) die entsprechenden Exponenten gebildet werden sollen und darüber summiert werden soll.

Durch Satz 10 und Satz 8 ist nun auch die Körperdiskriminante vollständig bestimmt. Da nämlich nach Satz 8 der Index durch $p^{\Sigma m L}$ genau teilbar ist, so wird nach Satz 10, unter Anwendung der Relation $D=k^2\cdot d$, die Körperdiskriminante durch

$$p^{\sum_m\sum_{i=1}^{k}\sum_{j=1}^{t_i}\delta_j^{(i)}\cdot\varepsilon_j^{(i)}}$$

genau teilbar. Beachtet man nun, dass $\varepsilon_j^{(i)}\cdot m=f_j^{(i)}$ der Grad des Primideals $\mathfrak{p}_j^{(i)}$ ist, so erhält man:

Satz 11. Die Körperdiskriminante ist durch die Primzahl p in der Potenz

$$p^{\Sigma f_j^{(i)}\left(\lambda_i-1+\varrho_j^{(i)}\right)}$$

genau 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 natürlich auch für diesen Satz einen etwas anderen Ausdruck angeben, wenn man annimmt, dass man für p eine Primidealzerlegung

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

hat. Dann wird die Körperdiskriminante durch

$$p^{\Sigma h_i(e_i-1+\varrho_i)}$$

genau teilbar, wo also $\varrho_i=0$ ist, wenn e_i nicht durch p teilbar ist, und $\varrho_i>0$, wenn e_i durch p teilbar ist. Um die Zahlen ϱ_i wirklich zu bestimmen, muss man eine reguläre Gleichung für die Primzahl p kennen.

Bei allen diesen Untersuchungen spielt die Zahl $M>H$, welche im Satze 1 vorkommt, eine wichtige Rolle. Man sieht ohne Schwierigkeiten ein, dass es immer genügen wird, wenn man $M>H+R$ wählt, wobei R die grösste der Zahlen ϱ bedeutet.