ZUR THEORIE DER ALGEBRAISCHEN KÖRPER.

Von

ÖYSTEIN ORE

in Kristiania.

Inhalt.

Einleitung.

Es soll in dieser Arbeit eine Methode zur Bestimmung der Primideale in algebraischen Körpern gegeben werden, welche eine weitere Ausführung der Gedanken ist, die ich in meinem Vortrage: »Über die Bestimmung der Primideale in algebraischen Körpern» 5. skand. Matematikerkongress, Helsingfors 1922 skizziert habe.

Die Dedekindsche Bestimmung der Primideale mittels höherer Kongruenzen versagt bekanntlich in dem Falle, wo die vorgelegte Primzahl ein ausserwesentlicher Teiler der Gattungsdiskriminante ist. Es wird hier gezeigt, wie man diese Dedekindschen Untersuchungen so weiterführen kann, dass man in jedem Falle, auch für gemeinsame ausserwesentliche Diskriminantenteiler eines Körpers, die Primidealzerlegung bestimmen kann. Zu diesem Zwecke werden die Newtonschen Polygone angewandt, und es ist von Interesse, dass eine gewisse Analogie mit der Bestimmung der Reihenentwickelungen einer algebraischen Funktion in der Umgebung einer singulären Stelle besteht.

Diese Methode hat weiter den Vorteil, dass man direkt aus der vorgelegten Gleichung die Primidealzerlegung bestimmen kann, ohne dass die Aufstellung einer Basis notwendig ist. Ausserdem geben die Untersuchungen eine Reihe von anderen algebraischen Sätzen über höhere Kongruenzen, Verallgemeinerung der Dumas'schen Irreduzibilitätsuntersuchungen usw. Auf andere Fragen, die durch diese Methoden behandelt werden können, u. a. die Bestimmung der Körperdiskriminante, werde ich in einer anderen Arbeit zurückkommen.

Für das Interesse und die Hilfe während der Ausarbeitung dieser Abhandlung fühle ich mich verpflichtet, Herrn Professor Mittag-Leffler meinen herzlichsten Dank auszusprechen.

Kap. 1. Höhere Kongruenzen.

§ 1. Einleitende Sätze.

Im Folgenden soll p eine rationale Primzahl und $\varphi(x)$ eine Primfunktion m^{ten} Grades für den Modul p bedeuten, und es soll weiter angenommen werden, dass der Koeffizient von x^m in $\varphi(x)$ gleich 1 ist. Für den Doppelmodul $p, \varphi(x)$ (modd $p, \varphi(x)$) gibt es dann p^m inkongruente Polynome, indem unter Polynom immer eine ganze, rationale Funktion mit ganzzahligen Koeffizienten verstanden wird.

Es sollen jetzt Funktionen von der Form

$$f(y) = A_0(x) \cdot y^n + A_1(x) \cdot y^{n-1} + \cdots + A_n(x) \tag{1}$$

untersucht werden, wo die Koeffizienten $A_i(x)$ Polynome sind. Diese Funktionen (1) sollen besonders in Bezug auf ihre Verhältnisse für den Doppelmodul $p, \varphi(x)$ untersucht werden, und wenn $f(y)$ und $f_1(y)$ zwei Funktionen dieser Art sind, soll

$$f(y) \equiv f_1(y) \pmod{p, \varphi(x)} \tag{2}$$

gesetzt werden, wenn die Differenz $f(y) - f_1(y)$ (mod p) durch $\varphi(x)$ teilbar ist. Man sieht einfach ein, dass die Kongruenz (2) dann und nur dann erfüllt ist, wenn die entsprechenden Koeffizienten der beiden Seiten einander (modd $p, \varphi(x)$) kongruent sind.

Es folgt nun ohne Schwierigkeiten für diese Kongruenzen die Richtigkeit der gewöhnlichen Rechenoperationen ganz analog wie für höhere Kongruenzen.

Für die späteren Anwendungen dieser Kongruenzen in der Theorie der algebraischen Zahlen brauche ich verschiedene Sätze, die hier entwickelt werden sollen.

Ich gehe erstens zur Aufstellung eines Euklidischen Algorithmus über und nehme an, dass zwei Funktionen gegeben sind

$$f_1(y) = A_0(x) \cdot y^{n_1} + A_1(x) \cdot y^{n_1-1} + \cdots + A_{n_1}(x),$$

$$f_2(y) = B_0(x) \cdot y^{n_2} + B_1(x) \cdot y^{n_2-1} + \cdots + B_{n_2}(x),$$

wo

$$n_1 \geq n_2, \quad A_0(x) \not\equiv 0, \quad B_0(x) \not\equiv 0 \pmod{p, \varphi(x)}.$$

Man kann dann immer ein $D_0(x)$ von höchstens $(m-1)^{\text{tem}}$ Grade derart bestimmen, dass

$$B_0(x) \cdot D_0(x) \equiv A_0(x) \pmod{p, \varphi(x)},$$

und man hat dann

$$f_1(y) \equiv D_0(x) \cdot y^{n_1-n_2} \cdot f_2(y) + R_1(y) \pmod{p, \varphi(x)},$$

wo

$$R_1(y) = C_0(x) \cdot y^{n_3} + C_1(x) \cdot y^{n_3-1} + \cdots + C_{n_3}(x)$$

und der Grad n_3 von $R_1(y)$ kleiner als n_1 ist. Daraus folgt weiter, wenn $D_1(x)$ so gewählt wird, dass

$$B_0(x) \cdot D_1(x) \equiv C_0(x) \pmod{p, \varphi(x)}$$

erfüllt ist,

$$R_1(y) \equiv D_1(x) \cdot y^{n_3-n_2} \cdot f_2(y) + R_2(y) \pmod{p, \varphi(x)},$$

wo der Grad von $R_2(y)$ kleiner als n_3 ist.

Wenn dieser Vorgang fortgesetzt wird, sieht man ein:

Man kann die Funktionen $q(y)$ und $f_3(y)$ derart bestimmen, dass

$$f_1(y) \equiv q(y) \cdot f_2(y) + f_3(y) \pmod{p, \varphi(x)}, \tag{3}$$

wo $q(y)$ vom Grade $n_1 - n_2$ und $f_3(y)$ höchstens vom Grade $n_2 - 1$ ist.

Wenn $B_0(x) = 1$ ist, hat man einfach

$$f_1(y) = q(y) \cdot f_2(y) + f_3(y).$$

Man definiert jetzt in gewöhnlicher Weise die *Teilbarkeit:* $f(y)$ ist durch $\psi(y)$ (modd $p, \varphi(x)$) teilbar, wenn

$$f(y) \equiv \psi_1(y) \cdot \psi(y) \pmod{p, \varphi(x)}$$

ist. Zwei Polynome $f_1(y)$ und $f_2(y)$ sind *relativ prim*, wenn sie (modd $p, \varphi(x)$) keinen gemeinsamen von y abhängigen Faktor besitzen.

Eine Funktion $f(y)$ von der Art (1) soll *primär* heissen wenn $A_0(x) = 1$ ist, und unter *Primfunktion* soll jede primäre Funktion verstanden werden, die ausser sich selbst keinen primären Teiler besitzt.

Aus (3) folgt jetzt eine Reihe von Kongruenzen

$$\left.\begin{aligned} f_1 &\equiv q_1 \cdot f_2 + f_3 \\ f_2 &\equiv q_2 \cdot f_3 + f_4 \\ &\cdots\cdots\cdots\cdots \\ f_{\nu-2} &\equiv q_{\nu-2} \cdot f_{\nu-1} + f_\nu \end{aligned}\right\} \pmod{p, \varphi(x)}, \tag{4}$$

wo die Grade der Funktionen $f_i(y)$ immer abnehmen. Man kann daher immer annehmen, dass f_ν von y unabhängig ist. Es folgt daher aus (4) dass die notwendige und hinreichende Bedingung für einen gemeinsamen Faktor (modd $p, \varphi(x)$) für $f_1(y)$ und $f_2(y)$ durch

$$f_\nu(y) \equiv 0 \pmod{p, \varphi(x)}$$

ausgedrückt ist. Weiter folgt in der gewöhnlichen Weise:

Satz 1. Wenn $f_1(y)$ zu $f_2(y)$ relativ prim (modd $p, \varphi(x)$) ist, kann man solche Funktionen $A(y)$ und $B(y)$ bestimmen, dass

$$A(y) \cdot f_1(y) + B(y) \cdot f_2(y) \equiv 1 \pmod{p, \varphi(x)}. \tag{5}$$

Eine beliebige Funktion $f(y)$ kann nun in ein Produkt von Primfunktionen zerlegt werden, und aus dem Bestehen des Euklidischen Algorithmus schliesst man auch, dass diese Zerlegung eine eindeutige ist.

Weiter sieht man ein, dass

$$\frac{\partial f(y)}{\partial y} = f'(y)$$

dann und nur dann mit $f(y)$ einen Faktor (modd $p, \varphi(x)$) gemeinsam hat, wenn $f(y)$ durch das Quadrat einer Primfunktion teilbar ist.

Zuletzt sei bemerkt, dass ein beliebiges Polynom $f(x)$ immer die Kongruenz

$$f(x)^p \equiv f(x) \pmod{p, \varphi(x)} \tag{6}$$

erfüllt, was genau so bewiesen wird wie in der gewöhnlichen Zahlentheorie der Satz von *Fermat*.

§ 2. Produkt der Primfunktionen.

Sei

$$\psi(y) = y^n + A_1(x) \cdot y^{n-1} + \cdots + A_n(x)$$

eine gegebene Primfunktion (modd $p, \varphi(x)$). Es sollen jetzt Funktionen $f(y)$ von der Art (1) untersucht werden, aber jetzt für einen dreifachen Modul (modd $p, \varphi(x), \psi(y)$), und zwar soll

$$f_1(y) \equiv f_2(y) \pmod{p, \varphi(x), \psi(y)}$$

gesetzt werden, wenn die Differenz $f_1(y) - f_2(y)$ (modd $p, \varphi(x)$) durch die Primfunktion $\psi(y)$ teilbar ist.

Alle Funktionen, welche (modd $p, \varphi(x), \psi(y)$) (oder kürzer (modd M)) inkongruent sind, sind in der Form

$$B_1(x) \cdot y^{n-1} + B_2(x) \cdot y^{n-2} + \cdots + B_n(x) \tag{7}$$

enthalten, wo die Koeffizienten unabhängig von einander alle (modd $p, \varphi(x)$) inkongruenten Werte annehmen. Nach § 1 gibt es daher $p^{n \cdot m}$ inkongruente Funktionen (modd M).

Sei jetzt $f(y) \not\equiv 0$ (modd M) ein bestimmter der Reste (7). Wenn dann $f_i(y) \not\equiv 0$ (modd M) einen beliebigen dieser Reste bedeutet, so ist

$$f(y) \cdot f_i(y) \equiv F_i(y) \text{ (modd } M), \tag{8}$$

wo $F_i(y)$ wieder einer der Reste (7) ist. Wenn $f_i(y)$ und $f_j(y)$ zwei solche Reste sind, so ist nur dann

$$F_i(y) \equiv F_j(y) \text{ (modd } M),$$

wenn

$$f_i(y) \equiv f_j(y) \text{ (modd } M).$$

Daraus folgt aus (8), wenn $f_i(y)$ alle Reste (7) durchläuft und diese Kongruenzen alle mit einander multipliziert werden,

$$f(y)^{p^{n \cdot m} - 1} \; \Pi f_i(y) \equiv \Pi f_i(y) \text{ (modd } M)$$

und daraus einfach

$$f(y)^{p^{n \cdot m} - 1} \equiv 1 \text{ (modd } M).$$

Es ist daher bewiesen:

Es ist für alle Funktionen $f(y)$

$$f(y)^{p^{n \cdot m}} \equiv f(y) \text{ (modd } p, \varphi(x), \psi(y)). \tag{9}$$

Weiter folgt, dass eine Kongruenz

$$F(z) \equiv 0 \text{ (modd } p, \varphi(x), \psi(y)),$$

wo die Koeffizienten alle von der Form (7) sind, höchstens n Wurzeln besitzen kann, wenn n den Grad von $F(z)$ in z angibt.

Nach (6) ist auch immer

$$f(y)^{p^m} \equiv f(y^{p^m}) \text{ (modd } p, \varphi(x))$$

oder allgemeiner

$$f(y)^{p^{h \cdot m}} \equiv f(y^{p^{h \cdot m}}) \text{ (modd } p, \varphi(x)). \tag{10}$$

Nach diesen Vorbereitungen soll jetzt der wichtige Satz bewiesen werden:

Satz 2. Es ist

$$f(y) = y^{p^{n \cdot m}} - y$$

kongruent (modd $p, \varphi(x)$) dem Produkt aller Primfunktionen $\psi(y)$ (modd $p, \varphi(x)$), deren Grade Teiler von n sind.[1]

Der Beweis wird in der folgenden Weise erbracht:

1) $f(y)$ besitzt (modd $p, \varphi(x)$) keine mehrfachen Faktoren. Es ist nämlich $f'(y) \equiv -1 \pmod{p, \varphi(x)}$.

2) Es ist $f(y)$ (modd $p, \varphi(x)$) durch alle Primfunktionen teilbar, deren Grade Teiler von n sind.

Aus (9) folgt nämlich

$$y^{p^{n \cdot m}} - y \equiv 0 \pmod{p, \varphi(x), \psi(y)}$$

für alle Primfunktionen $\psi(y)$ vom Grade n. Wenn aber der Grad n' von $\psi(y)$ ein Teiler von n ist, so folgt nach (9)

$$y^{p^{n' \cdot m}} \equiv y \pmod{p, \varphi(x), \psi(y)},$$

und wenn man diese Kongruenz nacheinander in die Potenzen

$$p^{n' \cdot m},\ p^{2n' \cdot m}, \ldots p^{n \cdot m}$$

erhebt, so kommt

$$y \equiv y^{p^{n' \cdot m}} \equiv y^{p^{2n' \cdot m}} \equiv \cdots \equiv y^{p^{n \cdot m}} \pmod{M}$$

oder

$$y^{p^{n \cdot m}} - y \equiv 0 \pmod{p, \varphi(x), \psi(y)}.$$

3) $f(y)$ kann durch keine Primfunktion von höherem Grade als n (modd $p, \varphi(x)$) teilbar sein. Denn sei $\psi(y)$ eine Primfunktion vom Grade $n' > n$, wofür

$$y^{p^{n \cdot m}} - y \equiv 0 \pmod{p, \varphi(y), \psi(y)}$$

wäre. Dann kommt für jede Funktion $f(y)$ nach (10)

$$f(y)^{p^{n \cdot m}} \equiv f(y^{p^{n \cdot m}}) \pmod{p, \varphi(x), \psi(y)},$$

[1] Dieser Satz ist für $n = 1$ schon von DEDEKIND, Crelles Journ. 54, p. 13, bewiesen worden.

und die Kongruenz

$$z^{p^{n \cdot m}} - z \equiv 0 \pmod{p, \varphi(x), \psi(y)}$$

hätte $p^{n' \cdot m} > p^{n \cdot m}$ Wurzeln, was unmöglich ist.

4) Wenn $\psi(y)$ ein Teiler von $f(y)$ ist, so ist der Grad von $\psi(y)$ ein Teiler von n. Denn wäre $n = n' \cdot q + r$, wo $n' > r > 0$ ist, so hat man gleichzeitig

$$y^{p^{n' \cdot m}} \equiv y, \quad y^{p^{n \cdot m}} \equiv y \pmod{p, \varphi(x), \psi(y)},$$

und daraus folgt leicht

$$y^{p^{r \cdot m}} - y \equiv 0 \pmod{p, \varphi(x), \psi(y)},$$

was nach 3) unmöglich ist.

Durch Zusammenfassen von 1) bis 4) ist der Satz bewiesen.

Kap. 2. Entwickelungen für Polynome.

§ 1. Kongruenzen (mod p^a).

Sei wie früher p eine rationale Primzahl und $\varphi(x)$ eine Primfunktion (mod p), worin der höchste Koeffizient gleich 1 vorausgesetzt wird. Weiter soll

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

ein gegebenes Polynom bezeichnen. Aus $f(x)$ soll später durch die Gleichung $f(\vartheta) = 0$ ein algebraischer Körper abgeleitet werden, indem $f(x)$ irreduzibel vorausgesetzt wird. Vorläufig soll aber die Irreduzibilität von $f(x)$ nicht vorausgesetzt werden.

Weiter soll

$$\varphi_1(x), \varphi_2(x), \ldots \varphi_r(x)$$

die verschiedenen Primfunktionen bezeichnen, die (mod p) in $f(x)$ aufgehen, wo

$$\varphi_i(x) = x^{m_i} + b_1^{(i)} \cdot x^{m_i - 1} + \cdots + b_{m_i}^{(i)} \quad (i = 1, 2, \ldots r).$$

Man kann dann immer $f(x)$ in der Form

$$f(x) = \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \ldots \varphi_r(x)^{e_r} + p \cdot M(x) \tag{2}$$

darstellen, wo

$$m_1 \cdot e_1 + m_2 \cdot e_2 + \cdots + m_r \cdot e_r = n$$

und $M(x)$ ein Polynom von höchstens $(n-1)^{\text{tem}}$ Grade ist.

Wir untersuchen jetzt das Polynom (1) für einen Primzahlpotenzmodul p^α. Nach einem Satze, der schon von SCHÖNEMANN[1] aufgestellt worden ist, kann man aus (2) für alle α eine Darstellung

$$f(x) = \Phi_1^{(\alpha)}(x) \cdot \Phi_2^{(\alpha)}(x) \ldots \Phi_r^{(\alpha)}(x) + p^\alpha M^{(\alpha)}(x) \tag{3}$$

herleiten, wo

$$\Phi_i^{(\alpha)}(x) \equiv \varphi_i(x)^{e_i} \pmod{p} \quad \begin{matrix} (i = 1, 2, \ldots r) \\ (\alpha = 1, 2, \ldots .), \end{matrix}$$

und diese Darstellung von $\Phi_i^{(\alpha)}(x)$ ist ausserdem für den Modul p^α eindeutig. Wie man am einfachsten diese Darstellung findet, habe ich in der Arbeit: »Zur Theorie der algebraischen Gleichungen»[2] gezeigt.

§ 2. Entwickelungen $(p, \varphi(x))$.

Es soll jetzt der Begriff *Entwickelung* $(p, \varphi(x))$ eingeführt werden. Die Primfunktion $\varphi(x)$ soll (mod p) ein Teiler von $f(x)$ sein.

Durch fortgesetzte Divisionen mit Potenzen von $\varphi(x)$ kann man immer das Polynom (1) in der Form

$$f(x) = \sum_{i=0}^{t} Q_i(x) \cdot \varphi(x)^i$$

schreiben, wo

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

und die $Q_i(x)$ Polynome von höchstens $(m-1)^{\text{tem}}$ Grade bezeichnen. Allgemein kann man nun weiter

$$Q_i(x) = A_i \cdot p^{\alpha_i} \cdot P_i(x) \qquad (i = 1, 2, \ldots l)$$

setzen, wo die Zahl $A_i \cdot p^{\alpha_i}$ derart gewählt wird, dass $P_i(x)$ primitiv wird (wenn $P_i(x) \neq 0$), und α_i derart, dass

$$A_i \not\equiv 0 \pmod{p}.$$

---

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

[2] Kristiania Videnskapsselskaps skrifter 1923, No. 1.

Speziell ist $\alpha_t = 0$ und $A_t = 1$. Man hat dann eine Entwickelung $(p, \varphi(x))$ in der Darstellung

$$f(x) = \sum_{i=0}^{t} A_i \; P_i(x) \, . \, p^{\alpha_i} \, . \, \varphi(x)^i . \tag{4}$$

Im Folgenden sollen als geometrisches Hilfsmittel die *Newton*'schen Polygone eingeführt werden.[1] In ein rechtwinkliges Koordinatensystem werden die Punkte

$$(t-i, \alpha_i) \quad (i = 0, 1, \ldots t)$$

eingezeichnet, und es entspricht einem jeden Gliede in (4) ein solcher Punkt. Wenn in (4) ein Glied $p^{\alpha_i} \, . \, A_i \, . \, P_i(x)$ verschwindet, wird kein zugehöriger Punkt eingezeichnet.

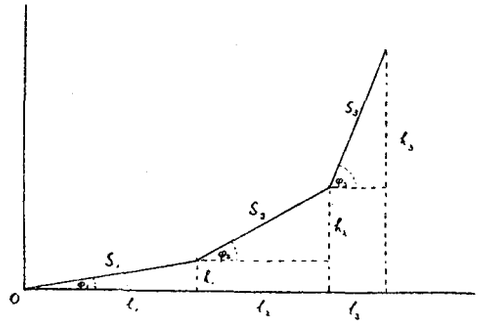

Fig. 1.

Man erhält auf diese Weise eine Gitterpunktmenge, wozu immer der Punkt (0, 0) gehört, und zu dieser Punktmenge kann man, indem man in (0, 0) anfängt, ein Newton'sches Polygon konstruieren. Für dieses Polygon wende ich im Folgenden die nachstehenden Bezeichnungen an:

Das Polygon wird aus einer gewissen Anzahl von Seiten

$$S_1, S_2, \ldots S_r$$

bestehen, deren Projektionen auf die X-achse die Längen

$$l_1, l_2, \ldots l_r,$$

auf die Y-achse die Längen

$$h_1, h_2, \ldots h_r$$

[1] Man sehe z. B. Hensel u. Landsberg: Theorie der alg. Funktionen. Vierte Vorlesung.

haben. Die Zahlen l_i und h_i sind immer ganz rational. e_i sei der grösste gemeinsame Faktor von l_i und h_i, also

$$\begin{aligned} l_i &= e_i \cdot \lambda_i \\ h_i &= e_i \cdot \varkappa_i \end{aligned} \quad (i = 1, 2, \ldots r),$$

wo λ_i zu $\varkappa_i$ relativ prim ist. Möglicherweise kann $h_1 = 0$ sein, dann wird $\lambda_1 = 1$ gesetzt. Zuletzt sei erwähnt, dass die Neigung φ_i einer Seite S_i gegen die X-achse durch

$$\operatorname{tg} \varphi_i = \frac{h_i}{l_i} = \frac{\varkappa_i}{\lambda_i} \quad (i = 1, 2, \ldots r)$$

bestimmt ist.

§ 3. Irreduzibilitätssätze.

Wie ich gezeigt habe[1], kann man nun den wichtigen Satz beweisen:

Satz 3. Sind

$$g(x) = \sum_{i=0}^{s'} a'_i \cdot Q'_i(x) \cdot p^{a'_i} \cdot \varphi(x)^i$$

$$h(x) = \sum_{i=0}^{s''} a''_i \cdot Q''_i(x) \cdot p^{a''_i} \cdot \varphi(x)^i$$

zwei Polynome mit den Polygonen S' und S'' für die Entwickelungen $(p, \varphi(x))$, dann hat das Produkt

$$f(x) = g(x) \cdot h(x) = \sum_{i=1}^{s} a_i \cdot Q_i(x) \cdot p^{a_i} \cdot \varphi(x)^i \qquad s = s' + s''$$

ein Polygon $S(p, \varphi(x))$, das aus den Seiten von S' und S'' nach steigender Neigung zusammengesetzt ist.

Dabei ist zu bemerken, dass der Grad von $Q'_{s'}(x) \cdot Q''_{s''}(x)$ auch grösser oder gleich m sein kann. In diesem Falle ist $s = s' + s'' + 1$, aber der Satz 3 bleibt doch richtig, indem man nur zu dem zusammengesetzten Polygone die Gerade von (0, 0) bis (1, 0) hinzufügt.

Für die folgenden Untersuchungen wird der Teil des Polygones von $f(x)$ von besonderer Bedeutung welcher über der X-achse liegt. Dieser Teil soll *Hauptpolygon* genannt und seine Seiten sollen wie früher mit $S_1, S_2, \ldots S_r$ bezeichnet werden.

---

[1] Kri:a Videnskapsselskaps Skr. 1923. No. 1. S. 27. Man sehe auch meine Arbeit: Zur Theorie der Irreduzibilitätskriterien. Zeitschrift f. Math. 1923.

Sei jetzt $f(x)$ von der Form

$$f(x) \equiv Q(x) \,.\, \varphi(x)^l \pmod{p},$$

wo $Q(x) \pmod{p}$ nicht durch $\varphi(x)$ teilbar ist. Man kann dann immer für die Primzahlpotenz p^a solche Polynome $Q_a(x)$ und $\Phi_a(x)$ bestimmen, dass

$$f(x) \equiv Q_a(x) \,.\, \Phi_a(x) \pmod{p^a}$$

wird, also

$$f(x) = Q_a(x) \,.\, \Phi_a(x) + p^a \,.\, M(x), \tag{5}$$

wo $M(x)$ ein Polynom von höchstens $(n-1)^{\text{tem}}$ Grade ist und

$$\Phi_a(x) \equiv \varphi(x)^l \pmod{p}.$$

Wenn jetzt (4) die Entwickelung $(p, \varphi(x))$ für $f(x)$ ist, so wird das Polygon von $f(x)$ seinen Endpunkt im Punkte (t, α_0) haben. Man sieht daher: Wenn man in (5) $\alpha > \alpha_0$ wählt, so wird das Glied $p^a \,.\, M(x)$ ohne Bedeutung für das Polygon von $f(x)$ $(p, \varphi(x))$. Das Polygon von $Q_a(x)$ wird aus einer Geraden bestehen, welche mit der X-achse zusammenfällt, und das Polygon von $\Phi_a(x)$ wird daher nach Satz 3 aus dem Hauptpolygone von $f(x)$ bestehen.

Daraus folgt ganz einfach wegen des Satzes 3[1]:

Satz 4. Ein Polynom $f(x) \equiv Q(x) \,.\, \varphi(x)^l \pmod{p}$ *kann nur dann im rationalen Gebiete einen Faktor*

$$g(x) \equiv \varphi(x)^i \pmod{p}$$

haben, wenn $g(x)$ *vom Grade*

$$q = m \,.\, \sum_{i=1}^{r} \varepsilon_i \,.\, \lambda_i$$

ist, wo m *der Grad von* $\varphi(x)$ *ist und* ε_i *eine der Zahlen* $0, 1, \ldots e_i$ *bedeutet.*

Aus diesem Satze leitet man ohne Schwierigkeiten die Irreduzibilitätssätze von KÖNIGSBERGER[2], PERRON[3], DUMAS[4] und BAUER[5] ab.

Es ist jetzt von der grössten Wichtigkeit, dass diese Sätze auch für einen beliebigen algebraischen Körper richtig bleiben. Dann müssen also die Koeffi-

---

[1] Loc. cit. S. 29.
[2] KÖNIGSBERGER, Crelles Journ. 115, S. 69.
[3] O. PERRON, Math. Ann. 60, S. 448 u. f.
[4] DUMAS, Journal de math. $6^{\text{ser.}}$ t. 2, S. 237.
[5] M. BAUER, Crelles Journ. 128, S. 87.

zienten von $f(x)$ in irgend einem Körper $P(\vartheta)$ enthalten sein und $\varphi(x)$ muss eine Primfunktion für einen Primidealmodul $\mathfrak{p}$ in $P(\vartheta)$ sein. Dann kann man aber nicht in der Entwickelung $(\mathfrak{p}, \varphi(x))$

$$f(x) = \sum_{i=0}^{t} Q_i(x) \cdot \varphi(x)^i$$

aus $Q_i(x)$ wie in (4) den Faktor $\mathfrak{p}^{\alpha_i}$ herausziehen, sondern nur $\mathfrak{p}^{\alpha_i}$ als die grösste den Koeffizienten von $Q_i(x)$ gemeinsame Potenz von $\mathfrak{p}$ bezeichnen. Der Satz 3 bleibt jedoch richtig, und daraus folgt sofort die Richtigkeit des Satzes 4 für den Körper $P(\vartheta)$.

§ 4. Zerlegung in Faktoren für ein Polygon.

Da für die Anwendung dieser Untersuchungen nur Kongruenzen für einen Primzahlpotenzmodul p^α in Betracht kommen, wo α beliebig gross gewählt werden kann, werde ich jetzt nach den Bemerkungen der Paragraphen 1 und 3 annehmen können, dass $f(x)$ (mod p) nur durch eine Primfunktion teilbar ist. Es ist also

$$f(x) \equiv \varphi(x)^t, \tag{6}$$

wo

$$n = m \cdot t$$

ist. Das Polygon S von $f(x)$ ist dann immer ein Hauptpolygon. Wenn man jetzt für $f(x)$ eine Entwickelung $(p, \varphi(x))$ hat, so gibt es in dieser Entwickelung gewisse Glieder, deren entsprechende Punkte auf dem Polygone S liegen. Dies ist besonders für die Eckpunkte des Polygons der Fall.

Es sei jetzt $\psi(x)$ ein Polynom mit demselben Polygone $S(p, \varphi(x))$ wie $f(x)$. *Durch*

$$f(x) \equiv \psi(x) \pmod{S}$$

wird bezeichnet, dass in der Differenz $f(x) - \psi(x)$ alle repräsentierenden Punkte oberhalb des Polygones S liegen.

Man setze jetzt in der Entwickelung (4)

$$A_i \cdot P_i(x) = Q_i(x),$$

wodurch die Entwickelung $(p, \varphi(x))$ von $f(x)$ in

$$f(x) = \sum_{0}^{t} Q_i(x) \cdot p^{\alpha_i} \cdot \varphi(x)^i \tag{7}$$

übergeht, wo in einem Polynom $Q_i(x)$ nicht alle Koeffizienten durch p teilbar sein können, ausser wenn $Q_i(x)$ verschwindet. Sei

$$\psi(x) = \sum_{0}^{t} Q'_i(x) \cdot p^{\alpha'_i} \cdot \varphi(x)^i \tag{8}$$

die entsprechende Entwickelung für $\psi(x)$. Dann sieht man ein:

Es ist $f(x) \equiv \psi(x) \pmod{S}$ dann und nur dann, wenn

$$Q_i(x) \equiv Q'_i(x) \pmod{p}$$

für alle i, wofür die entsprechenden Punkte $(t-i, \alpha_i)$ $(\alpha'_i = \alpha_i)$ auf S liegen. Wenn in $f(x)$ ein Glied oberhalb S liegt, muss dies natürlich auch mit dem entsprechenden Gliede in $\psi(x)$ der Fall sein. (Ich sage hier der Kürze wegen, dass ein Glied oberhalb S liegt, und meine damit, dass der repräsentierende Punkt dieses Gliedes oberhalb S liegt. Diese Bezeichnungsweise kann kaum missverstanden werden und wird im Folgenden oft angewandt.)

Es ist bisweilen nützlich, den Begriff Entwickelung $(p, \varphi(x))$ etwas weiter zu fassen. Es soll jetzt allgemeiner angenommen werden, dass in (8) die Grade der Polynome $Q'_i(x)$ nicht durch $m-1$ begrenzt sind, d. h. diese Grade dürfen auch grösser als $m-1$ sein, doch sollen sie in der Weise begrenzt sein, dass der Grad von $\psi(x)$ nicht grösser als $m \cdot t$ wird. Man sieht leicht ein, dass das Polygon $(p, \varphi(x))$ dasselbe wird, wenn man das Polygon für diese allgemeine Form konstruiert oder wenn man vorher die Entwickelung zur reduzierten Form überführt.

Nehmen wir die Entwickelung (8) von der hier erwähnten allgemeineren Art an, so folgt:

Es ist $f(x) \equiv \psi(x)$ *(mod* S*) dann und nur dann, wenn*

$$Q_i(x) \equiv Q'_i(x) \text{ (modd } p, \varphi(x))$$

für alle i*, wofür die entsprechenden Punkte* $(t-i, \alpha_i)$ $(\alpha_i = \alpha'_i)$ *auf* S *liegen.*

Es soll jetzt untersucht werden, welche Glieder überhaupt auf S liegen können. Ich betrachte die erste Seite S_1 von S. Die Gitterpunkte, welche auf dieser Geraden liegen, entsprechen den Gliedern von (7)

$$\varphi(x)^t,\ Q_{\lambda_1}(x) \cdot p^{\varkappa_1} \cdot \varphi(x)^{t-\lambda_1},\ Q_{2\lambda_1}(x) \cdot p^{2\varkappa_1} \cdot \varphi(t)^{t-2\lambda_1}, \ldots Q_{l_1}(x) \cdot p^{h_1} \cdot \varphi(x)^{t-l_1}.$$

Ebenso sind die Glieder der zweiten Seite entsprechend

$$Q_{l_1}(x) \cdot p^{h_1} \cdot \varphi(x)^{t-l_1},\ Q_{l_1+\lambda_2}(x) \cdot p^{h_1+\varkappa_2} \cdot \varphi(x)^{t-l_1-\lambda_2},\ Q_{l_1+2\lambda_2}(x) \cdot p^{h_1+2\varkappa_2} \cdot \varphi(x)^{t-l_1-2\lambda_2},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$Q_{l_1+l_2}(x) \cdot p^{h_1+h_2} \cdot \varphi(x)^{t-l_1-l_2}$$

und allgemein für die i^{te} Seite

$$\left.\begin{aligned}
&Q_{l_1+l_2+\cdots+l_{i-1}}(x) \cdot p^{h_1+h_2+\cdots+h_{i-1}} \cdot \varphi(x)^{t-l_1-l_2-\cdots-l_{i-1}},\\
&Q_{l_1+l_2+\cdots+l_{i-1}+\lambda_i}(x) \cdot p^{h_1+h_2+\cdots+h_{i-1}+\varkappa_i} \cdot \varphi(x)^{t-l_1-l_2-\cdots-l_{i-1}-\lambda_i},\\
&Q_{l_1+l_2+\cdots+l_{i-1}+2\lambda_i}(x) \cdot p^{h_1+h_2+\cdots h_{i-1}+2\varkappa_i} \cdot \varphi(x)^{t-l_1-l_2-\cdots-l_{i-1}-2\lambda_i},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&Q_{l_1+l_2+\cdots+l_{i-1}+l_i}(x) \cdot p^{h_1+h_2+\cdots+h_{i-1}+h_i} \cdot \varphi(x)^{t-l_1-l_2-\cdots-l_{i-1}-l_i}.
\end{aligned}\right\} \tag{9}$$

Sei jetzt $\psi_i(x)$ die Summe der Glieder (9), also

$$\psi_i(x) = p^{h_1+h_2+\cdots+h_{i-1}} \cdot \varphi(x)^{t-l_1-l_2-\cdots-l_i}(Q_{l_1+l_2+\cdots+l_{i-1}}(x) \cdot \varphi(x)^{l_i} +$$
$$+ Q_{l_1+\cdots+l_{i-1}+\lambda_i}(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{l_i-\lambda_i} + Q_{l_1+\cdots+l_{i-1}+2\lambda_i}(x) \cdot p^{2\varkappa_i} \cdot \varphi(x)^{l_i-2\lambda_i} + \cdots +$$
$$+ Q_{l_1+\cdots+l_{i-1}+l_i}(x) \cdot p^{h_i}).$$

Zur Abkürzung soll jetzt

$$Q_{l_1+l_2+\cdots+l_{i-1}+s\cdot\lambda_i}(x) = R_{i,s}(x)$$

gesetzt werden, wo also $R_{i,s}(x)$ entweder Null ist oder alle Koeffizienten nicht durch p teilbar sind. Dann kommt

$$\psi_i(x) = p^{h_1+h_2+\cdots+h_{i-1}} \cdot \varphi(x)^{t-l_1-l_2-\cdots-l_i} \cdot \varphi_i(x),$$

wo

$$\varphi_i(x) = R_{i,0}(x) \cdot \varphi(x)^{l_i} + R_{i,1}(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{l_i-\lambda_i} + R_{i,2}(x) \cdot p^{2\varkappa_i} \cdot \varphi(x)^{l_i-2\lambda_i} +$$
$$+ \cdots + R_{i,e_i}(x) \cdot p^{h_i}.$$

Nun ist allgemein

$$R_{i,e_i}(x) = R_{i+1,0}(x) \not\equiv 0 \pmod{p, \varphi(x)}.$$

Man kann daher immer solche Polynome $A_i(x)$ und $B_i(x)$ finden, dass

$$R_{i,0}(x) \cdot A_i(x) + \varphi(x) \cdot B_i(x) = 1 + C_i \cdot p \tag{10}$$

ist, wo C_i eine Constante, $A_i(x)$ von höchstens $(m-1)^{\text{ten}}$ Grade, $B_i(x)$ höchstens vom $(m-2)^{\text{ten}}$ Grade ist. Die Gleichung (10) kann auch

$$R_{i,0}(x) \cdot A_i(x) \equiv 1 \pmod{p, \varphi(x)}$$

geschrieben werden.

Wenn jetzt

$$f_i(x) = \varphi(x)^{l_i} + S_{i,1}(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{l_i - \lambda_i} + S_{i,2}(x) \cdot p^{2\varkappa_i} \cdot \varphi(x)^{l_i - 2\lambda_i} + \cdots + S_{i,e_i}(x) \cdot p^{h_i}$$

gesetzt wird, wo $S_{i,j}(x)$ Polynome von höchstens $(m-1)^{\text{ten}}$ Grade sind und ausserdem

$$S_{i,j}(x) \equiv A_i(x) \cdot R_{i,j}(x) \pmod{p, \varphi(x)} \tag{11}$$

ist, so kann man den folgenden wichtigen Satz beweisen:

Satz 5. Es ist

$$f(x) \equiv \prod_{i=1}^{r} f_i(x) \pmod{S}. \tag{12}$$

Ein Polynom soll *primär* genannt werden, wenn der Koeffizient für die höchste Potenz von $\varphi(x)$ in der Entwickelung $(p, \varphi(x))$ gleich 1 ist.

Nach (10) und (11) ist

$$S_{i,e_i}(x) \not\equiv 0 \pmod{p} \quad (i = 1, 2, \ldots r),$$

und das Polygon von $f_i(x)$ ist daher eine Gerade von derselben Neigung und Länge wie S_i. Folglich wird auch nach Satz 3 das Polygon von

$$\prod_{i=1}^{r} f_i(x)$$

gleich S. *Der Satz 5 besagt daher, dass man $f(x)$ (mod S) in solche primare Faktoren zerlegen kann, dass das Polygon eines Faktors $f_i(x)$ gleich einer Seite S_i von S ist.*

Da die beiden Seiten von (12) dasselbe Polygon S besitzen, kommt es, um die Richtigkeit dieser Kongruenz zu beweisen, nur darauf an zu zeigen dass die entsprechenden Glieder auf dem Polygone einander (modd $p, \varphi(x)$) gleich sind.

Der Satz soll jetzt durch vollständige Induktion bewiesen werden. Es wird daher erstens $r = 2$ angenommen, und man soll zeigen

$$\begin{aligned} f(x) \equiv f_1(x) \cdot f_2(x) = (&\varphi(x)^{l_1} + S_{1,1}(x) \cdot p^{\varkappa_1} \varphi(x)^{l_1 - \lambda_1} + \cdots + S_{1,e_1}(x) \cdot p^{h_1}) \cdot \\ &(\varphi(x)^{l_2} + S_{2,1}(x) \cdot p^{\varkappa_2} \varphi(x)^{l_2 - \lambda_2} + \cdots + S_{2,e_2}(x) \cdot p^{h_2}) \pmod{S}. \end{aligned} \tag{13}$$

Hier ist aber immer nach (11)

$$S_{1,i}(x) = Q_{i\lambda_1}(x),$$

so dass, wenn man in (13) die Multiplikation derart ausführt, dass man erstens $f_1(x)$ mit $\varphi(x)^{l_2}$ multipliziert, man alle Glieder von $f(x)$ erhält, deren repräsentierende Punkte auf der ersten Seite S_1 liegen.

Ein Glied

$$S_{1,i}(x) \,.\, p^{i\varkappa_1} \,.\, \varphi(x)^{l_1 - i\lambda_1}$$

in $f_1(x)$ wird durch einen Punkt $A_1 = (i\lambda_1, i\varkappa_1)$ abgebildet und ebenso ein Glied

$$S_{2,j}(x) \,.\, p^{j\varkappa_2} \,.\, \varphi(x)^{l_2 - j\,.\,\lambda_2}$$

in $f_2(x)$ durch einen Punkt $A_2 = (j\lambda_2, j\varkappa_2)$. Das Produkt dieser Glieder

$$S_{1,i}(x)\, S_{2,j}(x) \,.\, p^{i\varkappa_1 + j\varkappa_2} \,.\, \varphi(x)^{l_1 + l_2 - i\lambda_1 - j\lambda_2} \tag{14}$$

wird durch den Punkt

$$A = (i\lambda_1 + j\,.\,\lambda_2,\ i\varkappa_1 + j\,.\,\varkappa_2)$$

und noch dazu den Punkt

$$A' = (i\lambda_1 + j\lambda_2 - 1,\ i\varkappa_1 + j\varkappa_2)$$

abgebildet, wenn der Grad von

$$S_{1,i}(x) \,.\, S_{2,j}(x)$$

grösser als $m-1$ ist. Wenn aber A auf oder über dem Polygone von $f(x)$ liegt, so wird sicher A' oberhalb dieses Polygones liegen. Man braucht daher nur das Glied zu untersuchen, dem A entspricht. Man kann aber A in der Weise aus A_1 und A_2 erhalten, dass man die Vektoren OA_1 und OA_2 addiert, und diese Regel ist für das Produkt zweier Glieder allgemein gültig.[1]

Ein Produkt (14) wird daher immer Glieder geben, deren repräsentierende Punkte über dem Polygone S von $f(x)$ liegen, ausser in dem Falle, dass $i = e_i$ ist. Die Glieder, welche auf der zweiten Seite S_2 liegen, werden also durch

$$S_{1,e_1}(x) \,.\, p^{h_1} \,.\, f_2(x)$$

erschöpft, da ja das Glied

$$S_{1,e_1}(x) \,.\, p^{h_1} \,.\, \varphi(x)^{l_2},$$

[1] Die genauere Ausführung dieser Bemerkungen findet man in meiner oben zitierten Abhandlung S. 25.

welchem der Eckpunkt des Polygones entspricht, schon einmal früher mitgerechnet worden ist. Es ist aber nach (11)

$$S_{1,e_1}(x) \,.\, S_{2,i}(x) \equiv A_2(x) \,.\, R_{2,i}(x) \,.\, S_{1,e_1}(x) \pmod{p,\, \varphi(x)},$$

und daraus folgt

$$R_{2,i}(x) - S_{1,e_1}(x)\, S_{2,i}'(x) \equiv R_{2,i}(x)\,(1 - A_2(x) \,.\, S_{1,e_1}(x)) \pmod{p,\, \varphi(x)},$$

also nach (10) unter Berücksichtigung dessen, dass $S_{1,e_1}(x) = S_{2,0}(x)$,

$$R_{2,i}(x) \equiv S_{1,e_1}(x) \,.\, S_{2,i}(x) \pmod{p,\, \varphi(x)},$$

wodurch der Beweis erledigt ist.

Um jetzt den Induktionsbeweis zu vollenden, muss man annehmen, es sei schon bewiesen worden, dass $f(x)$ und das Produkt

$$\prod_{i=1}^{r-1} f_i(x)$$

für die ersten $r-1$ Seiten S_i dieselben repräsentierenden Glieder besitzen. Man muss dann das Produkt

$$f_r(x) \,.\, \prod_{i=1}^{r-1} f_i(x)$$

untersuchen. In dem Produkte

$$\varphi(x)^{l_r} \,.\, \prod_{i=1}^{r-1} f_i(x)$$

kommen alle Glieder von $f(x)$ vor, welche auf den $r-1$ ersten Seiten liegen. Die Glieder, welche auf der r^{ten} Seite liegen, können nur durch die Glieder von

$$f_r(x) \,.\, p^{h_1+h_2+\cdots+h_{r-1}} \,.\, S_{r-1,e_{r-1}}(x)$$

geliefert werden, wo der letzte Eckpunkt schon früher mitgerechnet worden ist. Alle anderen Glieder des Produktes werden nach den früheren Bemerkungen sicher oberhalb S liegen.

Nach (11) ist aber

$$S_{r-1,e_{r-1}}(x) \,.\, S_{r,j}(x) \equiv A_r(x) \,.\, R_{r,j}(x) \,.\, S_{r-1,e_{r-1}}(x) \pmod{p,\, \varphi(x)},$$

folglich

$$R_{r,j}(x) - S_{r-1,e_{r-1}}(x) \cdot S_{r,j}(x) \equiv R_{r,j}(x)\,(1 - A_r(x) \cdot S_{r-1,e_{r-1}}(x)) \pmod{p, \varphi(x)},$$

woraus nach (10) folgt

$$R_{r,j}(x) \equiv S_{r-1,e_{r-1}}(x) \cdot S_{r,j}(x) \pmod{p, \varphi(x)}.$$

Dadurch ist der Beweis des Satzes 5 vollständig geliefert worden.

Ohne Schwierigkeiten sieht man auch die Richtigkeit der folgenden, wichtigen Bemerkung ein:

Wenn man $f(x)$ nach Satz 5 in primäre Faktoren derart zerlegt, dass das Polygon eines Faktors gleich einer Seite des Polygones S ist, so sind die Koeffizienten der Faktoren (modd $p, \varphi(x)$) eindeutig bestimmt.

§ 5. Geradlinige Polygone.

Es soll jetzt der Fall behandelt werden, dass das Polygon $(p, \varphi(x))$ eine Gerade L ist. $f(x)$ kann dann immer in der Form

$$f(x) = \varphi(x)^l + A_1(x) \cdot p^{\frac{\overline{h}}{l}} \cdot \varphi(x)^{l-1} + A_2(x) \cdot p^{\frac{\overline{2h}}{l}} \cdot \varphi(x)^{l-2} + \cdots + A_l(x) \cdot p^h \qquad (15)$$

angenommen werden, wo die $A_i(x)$ Polynome von höchstens $(m-1)^{\text{tem}}$ Grade sind und

$$A_l(x) \not\equiv 0 \pmod{p, \varphi(x)}. \qquad (16)$$

Dabei bedeutet das Symbol $\underline{\overline{s}}$ für eine positive reelle Zahl s immer die kleinste positive Zahl, welche gleich oder grösser als s ist. Man kann auch Polynome mit mehrseitigem Polygone in der Form (15) schreiben, indem man nur für das Verhältnis $\frac{h}{l}$ die Neigungszahl $\frac{h_1}{l_1}$ der ersten Seite wählt. Dann braucht aber die Bedingung (16) nicht erfüllt zu sein. In (15) ist wie früher

$$h = e \cdot \varkappa$$
$$l = e \cdot \lambda$$

und daher

$$f(x) \equiv \varphi(x)^l + B_1(x) \cdot p^{\varkappa} \cdot \varphi(x)^{l-\lambda} + \cdots + B_l(x) \cdot p^h \pmod{L}, \qquad (17)$$

wenn

$$A_{i,\lambda}(x) = B_i(x)$$

gesetzt wird.

$f(x)$ wird *reduzibel* (mod L) genannt, wenn eine Zerlegung

$$f(x) \equiv g(x) \cdot h(x) \pmod{L}$$

möglich ist. Hier müssen nach Satz 3 $g(x)$ und $h(x)$ von der Form

$$\begin{aligned} g(x) &\equiv \varphi(x)^{r\cdot\lambda} + C_1(x) \cdot p^{\varkappa} \cdot \varphi(x)^{\lambda(r-1)} + \cdots + C_r(x) \cdot p^{r\cdot\varkappa} \\ h(x) &\equiv \varphi(x)^{s\cdot\lambda} + D_1(x) \cdot p^{\varkappa} \cdot \varphi(x)^{\lambda(s-1)} + \cdots + D_r(x) \cdot p^{s\cdot\varkappa} \end{aligned} \pmod{L} \qquad (18)$$

sein, wo $r+s=e$ ist.

Eine primäre Funktion, die ein geradliniges Polygon besitzt und noch dazu für dieses Polygon irreduzibel ist, soll eine *Primfunktion* (mod L) genannt werden. So ist z. B. $f(x)$ selbst immer eine Primfunktion (mod L), wenn $e=1$, also l zu h relativ prim ist. Allgemein kann $f(x)$ (mod L) nicht durch mehr als e Primfunktionen teilbar sein. Für eine Funktion mit geradlinigem Polygone hat man also immer eine Darstellung von der Form

$$f(x) \equiv \prod_{i=1}^{s} \varphi_i(x) \pmod{L},$$

wo die Polygone der Polynome $\varphi_i(x)$ Geraden sind, die aus Stücken von L bestehen, und diese Polynome sind für ihre geradlinigen Polygone Primfunktionen.

Dies gibt mit Satz 5:

Satz 6. Ein Polynom $f(x)$ mit einem beliebigen Polygone S kann in der Form

$$f(x) \equiv \prod_{i=1}^{r} \prod_{j=1}^{s_i} \varphi_{i,j}(x) \pmod{S}$$

geschrieben werden, wo die Polynome $\varphi_{i,j}(x)$ für ihre geradlinigen Polygone Primfunktionen sind, und diese Polygone bilden zusammen das Polygon S.

Es soll jetzt die Eindeutigkeit dieser Zerlegung bewiesen werden, und dazu sollen die Untersuchungen des Kap. 1 angewandt werden.

Es seien wie in (18) $g(x)$ und $h(x)$ zwei beliebige Polynome mit einem geradlinigen Polygone von der Neigung $\frac{\varkappa}{\lambda}$. Wenn man dann

$$\frac{\varphi(x)^{\lambda}}{p^{\varkappa}} = z$$

setzt, geht (18) in

$$\begin{aligned} g(x) &\equiv p^{r\cdot\varkappa}(z^r + C_1(x)\,.\,z^{r-1} + \cdots + C_r(x)) \\ h(x) &\equiv p^{s\cdot\varkappa}(z^s + D_1(x)\,.\,z^{s-1} + \cdots + D_s(x)) \end{aligned} \pmod{L}$$

über. Nun soll hier

$$\begin{aligned} G(z, x) &= z^r + C_1(x)\,.\,z^{r-1} + \cdots + C_r(x) \\ H(z, x) &= z^s + D_1(x)\,.\,z^{s-1} + \cdots + D_s(x) \end{aligned}$$

eingeführt werden; dann sieht man ein, dass eine Kongruenz

$$g(x) \equiv h(x) \pmod{L}$$

nichts anders als

$$G(z, x) \equiv H(z, x) \pmod{p, \varphi(x)}$$

bedeutet, indem z als eine unabhängige Variable betrachtet wird. Die Theorie der Polynome mit geradlinigen Polygonen kann daher ganz analog wie die der Kongruenzen (modd $p, \varphi(x)$) entwickelt und ausserdem aus dieser abgeleitet werden. So folgt z. B.: Wenn $g(x)$ (mod L) in Primfunktionen zerlegt ist, entspringt daraus eine entsprechende Zerlegung (modd $p, \varphi(x)$) von $G(z, x)$. Daraus folgt aus Kap. 1 auch die Eindeutigkeit der Zerlegung eines Polynoms für ein geradliniges Polygon.

Weiter kann man in dieser Weise die Sätze des Kap. 1 auf Kongruenzen (mod L) übertragen. So hat man z. B.

Satz 7. Wenn zwei primäre Polynome $g(x)$ und $h(x)$ mit demselben geradlinigen Polygone L gegeben sind, die von den Graden $r\,.\,\lambda$ und $s\,.\,\lambda$ in $\varphi(x)$ und (mod L) zu einander relativ prim sind, kann man immer solche Polynome $A(x)$ und $B(x)$ mit dem Polygone L bestimmen, dass

$$g(x)\,.\,A(x) + h(x)\,.\,B(x) \equiv p^{(r+a)\varkappa} \pmod{L},$$

wo $a\,.\,\lambda$ und $b\,.\,\lambda$ die Grade von $A(x)$ und $B(x)$ in $\varphi(x)$ bedeuten.

Hier ist natürlich $a + r = b + s$, und man kann ausserdem a und b derart wählen, dass $a < s$ und $b < r$. Wenn in diesem Satze gesagt wird, dass zwei Polynome dasselbe geradlinige Polygon L besitzen, so bedeutet dies hier wie im Folgenden, dass die Neigungen der beiden Polygone dieselben sind, aber die Längen brauchen nicht gleich zu sein, d. h. die Polynome brauchen nicht von gleichen Graden in $\varphi(x)$ zu sein.

Aus Satz 7 folgt weiter: Wenn ein Polynom $j(x)$ mit dem Polygone L und vom Grade $i\,.\,\lambda$ in $\varphi(x)$ gegeben ist, so kann man, wenn wie früher $g(x)$

zu $h(x)$ (mod L) relativ prim ist, zwei Polynome $A(x)$ und $B(x)$ derart bestimmen, dass

$$g(x) \cdot A(x) + h(x) \cdot B(x) \equiv p^{(r+a-i)\varkappa} \cdot j(x) \pmod{L}$$

ist. Hier kann man den Grad $a \cdot \lambda$ von $A(x)$ kleiner als $s \cdot \lambda$ wählen, und wenn daher der Grad von $j(x)$ in $\varphi(x)$ kleiner als $(r+s)\lambda$ ist, so wird auch $b \cdot \lambda < r \cdot \lambda$.

Weiter kann man den Satz 2 in dieser Sprache folgendermassen formulieren:

Satz 8. Es ist

$$\varphi(x)^{\lambda \cdot p^{n \cdot m}} - p^{\varkappa(p^{n \cdot m}-1)} \cdot \varphi(x)^{\lambda}$$

(mod L) kongruent dem Produkt aller Primfunktionen (mod L), deren Grade in $\varphi(x)^{\lambda}$ Teiler von n sind.

Zuletzt soll die folgende Erweiterung des Satzes 4 erwähnt werden, die sofort aus der Einführung der Primfunktionen mit Hilfe des Satzes 6 folgt. Es sollen für alle Primfunktionen $\varphi_i(x)$ (mod p), welche in $f(x)$ aufgehen, die zugehörigen Polygone S_i gezeichnet und es soll $f(x)$ (mod S_i) in Primfaktoren zerlegt werden. Seien

$$\lambda_i^{(j)} \cdot n_{i,k}^{(j)} \quad (k = 1, 2, \ldots t_i^{(j)})$$

die Grade in $\varphi(x)$ der irreduziblen Faktoren für eine beliebige Seite $S_i^{(j)}$ von S_i mit der Neigung

$$\frac{h_i^{(j)}}{l_i^{(j)}} = \frac{e_i^{(j)} \cdot \varkappa_i^{(j)}}{e_i^{(j)} \cdot \lambda_i^{(j)}} = \frac{\varkappa_i^{(j)}}{\lambda_i^{(j)}}.$$

$t_i^{(j)}$ bedeutet die Anzahl der irreduziblen Faktoren für diese Seite, also die Anzahl der Zahlen $n_{i,k}^{(j)}$, indem man, wenn (mod $S_i^{(j)}$) gleiche Faktoren vorkommen, die entsprechenden Grade $n_{i,k}^{(j)}$ so oft vorkommen lässt, wie die Multiplizität angibt.

Dann folgt die Richtigkeit des Satzes:

Satz 9. Ist für ein beliebiges Polynom

$$f(x) \equiv \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \ldots \varphi_s(x)^{e_s} \pmod{p}$$

die Zerlegung in Primfaktoren, wo der Grad der Primfunktion $\varphi_i(x)$ gleich m_i ist, so kann $f(x)$ im rationalen Bereiche nur dann einen Faktor vom Grade m haben, wenn m von der Form

$$m = \sum m_i \cdot \lambda_i^{(j)} \cdot n_{i,k}^{(j)}$$

ist, wo in dieser Summe eine beliebige Anzahl von Glieder mitgerechnet werden darf.

Wenn daher ein oder mehrere Diskriminantenteiler oder allgemeiner die Diskriminante des Polynoms bekannt ist, kann man nach diesem Satze in vielen Fällen die Untersuchung der Reduzibilität des Polynoms sehr vereinfachen.

§ 6. Reduzibilität für Polygonmoduln.

Den Primfunktionen für Polygonmoduln, welche in § 5 definiert worden sind, entsprechen genau die Primfunktionen für einen Primzahlmodul p. Es sollen jetzt einige Untersuchungen über Polygonmoduln ausgeführt werden, welche für die späteren Untersuchungen über Primideale in algebraischen Körper notwendig sind und gleichzeitig sehr interessante Sätze über höhere Kongruenzen ergeben.

Es soll erstens angenommen werden, dass $f(x)$ ein geradliniges Polygon L besitzt und daher die Form (15) hat. Nennen wir in (17) die rechte Seite $\psi(x)$, so wird die Differenz $f(x) - \psi(x)$ nur solche Glieder enthalten, wofür die repräsentierenden Punkte oberhalb L liegen. Es soll jetzt untersucht werden, wie solche Glieder oberhalb L überhaupt verteilt sein können.

Ein Glied

$$A_i(x) \cdot p^{\left\lfloor \frac{ih}{l} \right\rfloor} \cdot \varphi(x)^{l-i}$$

in (15) wird durch den Punkt

$$\left(i, \left\lfloor \frac{ih}{l} \right\rfloor\right) \quad (i = 0, 1, \ldots l)$$

abgebildet, und es sollen nun die Abstände dieser Punkte von L oder die damit proportionalen Grössen

$$d_i = \left\lfloor \frac{ih}{l} \right\rfloor - i \cdot \frac{h}{l} = \left\lfloor \frac{i\varkappa}{\lambda} \right\rfloor - i\frac{\varkappa}{\lambda} \quad (i = 1, 2, \ldots l). \tag{19}$$

untersucht werden.

Für diese Grössen soll jetzt gezeigt werden, dass immer

$$d_i = d_{i+\lambda} = d_{i+2\lambda} = \cdots$$

ist. Man hat nämlich

$$d_i - d_{i+\lambda} = \left\lfloor \frac{i\varkappa}{\lambda} \right\rfloor - \left\lfloor \frac{(i+\lambda)\varkappa}{\lambda} \right\rfloor - \frac{i\varkappa}{\lambda} + (i+\lambda)\frac{\varkappa}{\lambda}$$

oder

$$d_i - d_{i+\lambda} = \left\lfloor \frac{i\varkappa}{\lambda} \right\rfloor - \left\lfloor \frac{i\varkappa}{\lambda} + \varkappa \right\rfloor + \varkappa = 0.$$

Um daher die Zahlen (19) zu untersuchen, braucht man nur die Zahlen

$$d_0 = 0,\ d_1, d_2, \ldots d_{\lambda-1},\ d_\lambda = 0$$

zu bestimmen. Diese Zahlen sind nach (19) sicher kleiner als 1. Bei der Bestimmung ihrer Grösse braucht man daher nur auf die darin vorkommenden Brüche Rücksicht zu nehmen. Wenn aber in (19) i die Zahlen $1, 2, \ldots \lambda$ durchläuft, werden auch die Zahlen $i \cdot \varkappa$ ein vollständiges Restsystem (mod λ) bilden. Die echten Brüche, welche sich als Reste ergeben, wenn man $i \cdot \varkappa$ durch λ dividiert, sind daher alle verschieden, und folglich ist bewiesen:

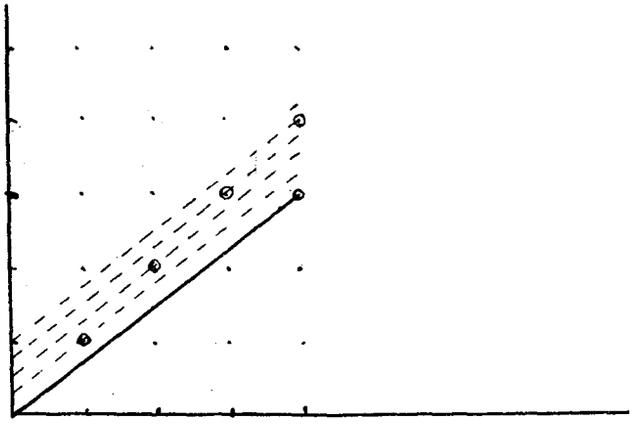

Fig. 2.

Die Zahlen $d_1, d_2, \ldots d_{\lambda-1}$ stimmen mit den Zahlen

$$\frac{1}{\lambda}, \frac{2}{\lambda}, \cdots \frac{\lambda-1}{\lambda}$$

in irgendeiner Reihenfolge überein.

Durch die Punkte der Y-achse

$$\left(0, \frac{1}{\lambda}\right), \left(0, \frac{2}{\lambda}\right), \cdots \left(0, \frac{\lambda-1}{\lambda}\right), (0, 1), \left(0, 1+\frac{1}{\lambda}\right), \cdots$$

werden jetzt Parallellen zu der Geraden L gezogen; diese Geraden sollen bzw. mit

$$L_1, L_2, L_3, \ldots\ldots L_{\lambda-1}, L_\lambda, L_{\lambda+1}, \ldots\ldots$$

bezeichnet werden, und wegen der Vollständigkeit werde $L = L_0$ gesetzt. Alle Gitterpunkte, welche oberhalb L liegen, werden auf irgendeine dieser Geraden fallen, und ein Glied

$$A(x) \cdot p^a \cdot \varphi(x)^i$$

wird daher durch einen Punkt repräsentiert, welcher auf einer bestimmten der Geraden L_k liegt. Umgekehrt liegen auf allen L_k Gitterpunkte. Die Glieder, welche durch Punkte auf L_0 abgebildet werden, sind schon in (17) aufgestellt. Es sollen jetzt allgemein die Glieder bestimmt werden, welche auf einer Seite L_k liegen, indem zunächst vorausgesetzt wird, dass $0 < k < \lambda$. Für ein Glied

$$A_i(x) \cdot p^{\left[\frac{i\varkappa}{\lambda}\right]} \cdot \varphi(x)^{l-i}$$

muss man

$$d_i = \frac{\left[i\varkappa\right]}{\left[\lambda\right]} - i\frac{\varkappa}{\lambda} = \frac{k}{\lambda}$$

haben, woraus durch Multiplikation mit λ folgt

$$i\varkappa + k \equiv 0 \pmod{\lambda}$$

Die kleinste positive Lösung dieser Kongruenz soll i_k genannt werden, dann ist die allgemeinste Lösung

$$i = i_k + \lambda \cdot s \quad (s = 0, 1, \ldots),$$

indem nur positive Werte von i berücksichtigt werden.

Ein Glied, das auf L_k liegt, wird daher von der Form

$$A_s(x) \cdot p^{\left[\frac{(i_k+\lambda \cdot s)\varkappa}{\lambda}\right]} \cdot \varphi(x)^{l-i_k-s\cdot\lambda}. \tag{20}$$

Es wurde hier vorausgesetzt dass $k < \lambda$ ist. Wenn man aber (20) mit p multipliziert, bekommt man, wie einfach einzusehen ist, ein Glied, das auf $L_{k+\lambda}$ liegt, und allgemeiner, wenn man (20) mit p^t multipliziert, erhält man Glieder, welche auf $L_{k+t.\lambda}$ liegen. Umgekehrt, wenn ein Glied G gegeben ist, welches auf $L_{k+t.\lambda}$ liegt, so ist G durch p^t teilbar, und man erhält durch Division durch p^t ein Glied auf L_k.

Es soll im Folgenden gesagt werden, dass *ein Polynom $f_1(x)$ zu L_k gehört*, wenn $j = k$ die kleinste Zahl ist, wofür ein Glied von $f_1(x)$ auf L_j liegt. Allgemeiner soll auch oft gesagt werden, wenn Missverständnisse nicht zu befürchten sind, dass $f_1(x)$ zu L_k gehört, wenn nur festgestellt ist, dass auf den Geraden $L_0, L_1, \ldots L_{k-1}$ keine Glieder von $f(x)$ liegen, aber nicht, dass es auf L_k wirklich Glieder von $f_1(x)$ gibt.

Durch (17) ist die allgemeine Form eines Polynoms gegeben, wofür alle Glieder auf L_0 liegen. Im Allgemeinen soll jetzt die Form eines Polynoms be-

stimmt werden, wofür alle Glieder auf L_k liegen, und man nehme erstens $k < \lambda$ an. Das gesuchte Polynom muss dann eine Summe der Glieder (20) sein, also

$$f_1(x) = \sum_{s=0}^{t} A_s(x) \cdot p^{\overline{\frac{(i_k+\lambda s)\cdot x}{\lambda}}} \cdot \varphi(x)^{l-i_k-s\cdot\lambda},$$

was man auch

$$f_1(x) = \frac{p^{\overline{\frac{i_k\cdot x}{\lambda}}}}{\varphi(x)^{i_k}} \cdot \sum_{s=0}^{t} A_s(x) \cdot p^{s\cdot x} \cdot \varphi(x)^{l-s\cdot\lambda}$$

schreiben kann oder

$$f_1(x) = \frac{p^{\overline{\frac{i_k\cdot x}{\lambda}}}}{\varphi(x)^{i_k}} \cdot \varphi_1(x),$$

wo $\varphi_1(x)$ ein Polynom ist, wofür alle Glieder auf L_0 liegen. Man bemerkt aber, dass $\varphi_1(x)$ immer durch $\varphi(x)^\lambda$ teilbar sein muss, woraus folgt:

$$f_1(x) = p^{\overline{\frac{i_k\cdot x}{\lambda}}} \cdot \varphi(x)^{\lambda-i_k} \cdot \psi_1(x), \tag{21}$$

wo $\psi_1(x)$ wieder ein Polynom ist, worin alle Glieder auf L_0 liegen.

Es war hier $k < \lambda$ vorausgesetzt. Soll man aber die Polynome bestimmen, wofür alle Glieder auf $L_{k'}$ liegen, wo $k' = t \cdot \lambda + k$, so kann man nur das eben gefundene $f_1(x)$ mit p^t multiplizieren.

Aus (21) folgt daher:

$f_1(x)$ sei ein Polynom, wofür alle Glieder auf L_k liegen. Dann kann man zwei positive, ganzzahlige Exponenten α und β derart finden, dass

$$f_1(x) = p^\alpha \cdot \varphi(x)^\beta \cdot \varphi_1(x),$$

wo in $\varphi_1(x)$ alle Glieder auf L_0 liegen. β kann hier immer kleiner als λ vorausgesetzt werden.

Und umgekehrt:

Wenn ein $\varphi_1(x)$ gegeben ist, wofür alle Glieder auf L_0 liegen, kann man immer solche α und $\beta < \lambda$ bestimmen, dass in

$$f_1(x) = p^\alpha \cdot \varphi(x)^\beta \cdot \varphi_1(x)$$

alle Glieder auf L_k liegen.

Es ist früher definiert worden, dass ein Polynom $F_1(x)$ zu L_k gehört, wenn alle Glieder in $F_1(x)$ oberhalb L_k liegen. Daraus folgt, dass, wenn $F_1(x)$ und $F_2(x)$ bzw. zu L_k und L_l gehören, $F_1(x) \cdot F_2(x)$ zu L_{k+l} gehört.

Die Kongruenz

$$f_1(x) \equiv f_2(x) \pmod{L_\gamma}$$

soll nun bezeichnen, dass in der Differenz $f_1(x) - f_2(x)$ alle repräsentierenden Punkte oberhalb L_γ liegen. Diese Kongruenzen (mod L_γ) werden in diesen Untersuchungen eine ähnliche Rolle wie in der gewöhnlichen Zahlentheorie die Kongruenzen für einen Primzahlpotenzmodul p^α spielen.

Es sei jetzt $f_1(x)$ ein gegebenes Polynom, das zu L_γ gehört, und es seien $g(x)$ und $h(x)$ zwei Polynome mit dem geradlinigen Polygone L_0 und ausserdem (mod L_0) relativ prim. Man kann dann immer solche Polynome $A_1(x)$ und $B_1(x)$ bestimmen, welche zu L_γ gehören, dass

$$g(x) \,.\, A_1(x) + h(x) \,.\, B_1(x) \equiv p^{j \cdot \varkappa} f_1(x) \pmod{L_\gamma}, \tag{22}$$

wo j eine ganze Zahl ist.

Dafür, dass diese Kongruenz erfüllt sein soll, spielen die Glieder in $f_1(x)$, welche oberhalb L_γ liegen, keine Rolle, und man kann daher voraussetzen, dass $f_1(x)$ ein Polynom ist, wofür alle Glieder auf L_γ liegen. Ebenso mit $A_1(x)$ und $B_1(x)$.

Dann kann

$$f_1(x) = p^\alpha \,.\, \varphi(x)^\beta \,.\, \varphi_1(x)$$

gesetzt werden, wo $\varphi_1(x)$ ein Polynom ist, wofür alle Glieder auf L_0 liegen. Nach § 5 ist es nun möglich, $A(x)$ und $B(x)$ mit Gliedern auf L_0 derart zu bestimmen, dass

$$g(x) \,.\, A(x) + h(x) \,.\, B(x) \equiv p^{(r+\alpha-i)\varkappa} \varphi_1(x) \pmod{L_0}.$$

Wenn diese Kongruenz mit $p^\alpha \,.\, \varphi(x)^\beta$ multipliziert und

$$A_1(x) = p^\alpha \,.\, \varphi(x)^\beta \,.\, A(x)$$

$$B_1(x) = p^\alpha \,.\, \varphi(x)^\beta \,.\, B(x)$$

gesetzt wird, folgt sofort die Richtigkeit von (22).[1]

Mittels dieser Bemerkung folgt jetzt der wichtige Satz:

Satz 10. Wenn $f(x) \equiv g(x) \,.\, h(x)$ (mod L) und $g(x)$ zu $h(x)$ (mod L) relativ prim ist, so ist $f(x)$ auch für alle Geraden L_γ reduzibel und zwar

$$f(x) \equiv g_\gamma(x) \,.\, h_\gamma(x) \pmod{L_\gamma}, \tag{23}$$

wo

$$g_\gamma(x) \equiv g(x), \quad h_\gamma(x) \equiv h(x) \pmod{L}.$$

[1] Man sieht ein: Wenn das Produkt $g(x) \,.\, h(x)$ das Polygon L_0 mit der Projektion $e \,.\, \lambda$ besitzt, und in $f_1(x)$, das von einem Grade in $\varphi(x)$ sein soll, der $\leqq e \,.\, \lambda$, alle Glieder auf dem entsprechenden L_γ liegen, so kann man die Kongruenz

$$g(x) \,.\, A_1(x) + h(x) \,.\, B_1(x) \equiv f_1(x) \pmod{L_\gamma}$$

erfüllen.

Dieser Satz soll durch vollständige Induktion bewiesen werden, indem man beachtet, dass $f(x)$ für $\gamma = 0$ reduzibel ist. Es kann daher angenommen werden, dass

$$f(x) \equiv g_{\gamma-1}(x) \cdot h_{\gamma-1}(x) \pmod{L_{\gamma-1}} \tag{24}$$

ist, wo

$$g_{\gamma-1}(x) \equiv g(x), \; h_{\gamma-1}(x) \equiv h(x) \pmod{L}.$$

Es soll jetzt

$$\left.\begin{aligned} g_\gamma(x) &= g_{\gamma-1}(x) + G(x) \\ h_\gamma(x) &= h_{\gamma-1}(x) + H(x) \end{aligned}\right\} \tag{25}$$

gesetzt werden, wo $G(x)$ und $H(x)$ nur Glieder auf L_γ haben sollen. Es kommt nun darauf an, die Zusatzpolynome $G(x)$ und $H(x)$ in (25) so zu wählen, dass, wenn (24) erfüllt ist, auch die Kongruenz (23) richtig wird.

Nach (24) ist

$$\psi(x) = f(x) - g_{\gamma-1}(x) \cdot h_{\gamma-1}(x) \equiv 0 \pmod{L_{\gamma-1}},$$

und $\psi(x)$ gehört daher zu L_γ. Wenn man daher (25) in (23) einsetzt, so folgt

$$\psi(x) \equiv G(x) \cdot h_{\gamma-1}(x) + H(x) \cdot g_{\gamma-1}(x) + H(x) \cdot G(x) \pmod{L_\gamma}.$$

Da das Produkt $H(x) \cdot G(x)$ nach den früheren Bemerkungen zu $L_{2\gamma}$ gehört, ist es hier ohne Bedeutung, und man hat daher nur die Bedingung

$$\psi(x) \equiv G(x) \cdot h_{\gamma-1}(x) + H(x) \cdot g_{\gamma-1}(x) \pmod{L_\gamma}. \tag{26}$$

Setzt man nun nach den Voraussetzungen

$$g_{\gamma-1}(x) = g(x) + \bar{g}(x), \; h_{\gamma-1}(x) = h(x) + \bar{h}(x),$$

wo

$$\bar{g}(x) \equiv \bar{h}(x) \equiv 0 \pmod{L}$$

ist, so folgt aus (26)

$$\psi(x) \equiv G(x) \cdot h(x) + H(x) \cdot g(x) \pmod{L_\gamma},$$

indem

$$G(x) \cdot \bar{h}(x) \equiv H(x) \cdot \bar{g}(x) \equiv 0 \pmod{L_\gamma}$$

wird. Diese letzte Kongruenz kann aber nach (22) (Fussnote) immer erfüllt werden, wodurch der Satz bewiesen ist. Es ist auch möglich, worauf ich hier nicht eingehe, die Eindeutigkeit der Zerlegung des Satzes 10 zu beweisen.

Aus Satz 10 folgt sofort, dass $f(x)$ für jede Primzahlpotenz p^a reduzibel wird, und zwar

$$f(x) \equiv g^{(a)}(x) \cdot h^{(a)}(x) \pmod{p^a},$$

wo

$$g^{(a)}(x) \equiv \varphi(x)^{r \cdot \lambda}, \quad h^{(a)}(x) \equiv \varphi(x)^{s \cdot \lambda} \pmod{p},$$

wenn $g(x)$ und $h(x)$ von der Form (18) sind.

Weiter folgt, wenn

$$f(x) \equiv \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \ldots \varphi_s(x)^{e_s} \pmod{L}$$

die Primfaktorenzerlegung (mod L) von $f(x)$ ist, dass auch

$$f(x) \equiv \Phi_1^{(\gamma)}(x) \cdot \Phi_2^{(\gamma)}(x) \ldots \Phi_s^{(\gamma)}(x) \pmod{L_\gamma}$$

für alle γ, wo

$$\Phi_i^{(\gamma)}(x) \equiv \varphi_i(x)^{e_i} \pmod{L}.$$

Wenn

$$e_1 = e_2 = \cdots = e_s = 1$$

ist, so sind die Funktionen $\Phi_i^{(\gamma)}(x)$ (mod L_γ) irreduzibel, aber wenn einige der Exponenten $e_i > 1$ sind, können auch die entsprechenden Faktoren $\Phi_i^{(\gamma)}(x)$ reduzibel sein.

Aus diesen Bemerkungen folgt auch, dass $f(x)$ für alle Primzahlpotenzmoduln p^a reduzibel wird und

$$f(x) \equiv \psi_1^{(a)}(x) \cdot \psi_2^{(a)}(x) \ldots \psi_s^{(a)}(x) \pmod{p^a},$$

wo

$$\psi_i^{(a)}(x) \equiv \varphi_i(x)^{e_i \cdot} \pmod{p}.$$

Nachdem so der Fall behandelt worden ist, dass das Polygon von $f(x)$ eine Gerade ist, soll nun der allgemeine Fall behandelt werden, dass das Polygon eine beliebige Anzahl von Seiten besitzt. Man kann dann den wichtigen Satz beweisen:

Satz 11. $f(x)$ ist für jeden Primzahlpotenzmodul p^a reduzibel, und zwar können die Faktoren derart gewählt werden, dass das Polygon eines Faktors gleich einer Seite des Polygones zu $f(x)$ ist, und die geradlinigen Polygone der Faktoren bilden zusammen das Polygon zu $f(x)$.

Um diesen Satz zu beweisen, kann man zunächst annehmen, was gestattet ist, dass das Polygon S ein Hauptpolygon ist. Sei $L = L_0$ die erste Seite dieses

Polygons, so soll gezeigt werden, dass $f(x)$ für alle zu L_0 parallelen Geraden L_γ reduzibel ist und zwar in der Weise, dass der eine Faktor das Polygon L_0 besitzt und der andere ein Polygon, das oberhalb L_0 liegt. Dadurch folgt nämlich, dass $f(x)$ auch für jeden Modul p^a reduzibel wird, und für genügend grosse α wird das Polygon des einen Faktors aus der Seite L und folglich nach dem Multiplikationssatze das Polygon des anderen Faktors aus dem anderen Teile von S bestehen. Den zweiten Faktor kann man aber dann in entsprechender Weise behandeln, und dadurch folgt einfach der Satz.

Es sei

$$f(x) \equiv (\varphi(x)^l + B_1(x) \cdot p^\varkappa \cdot \varphi(x)^{l-\lambda} + \cdots + B_e(x) \cdot p^h)\, \varphi(x)^j \pmod{L}$$

die Zerlegung von $f(x)$ (mod L), wo

$$B_e(x) \not\equiv 0 \text{ (modd } p, \varphi(x)).$$

Wenn hier j ein Multiplum von λ ist, so folgt wie im Satz 10, dass $f(x)$ für alle L_γ in der gewünschten Weise reduzibel wird. Im Allgemeinen ist aber j kein Multiplum von λ, und man kann dann $j = t \cdot \lambda - \varepsilon$ setzen, wo $0 \leqq \varepsilon < \lambda$. In diesem Falle wird der Satz wie der Satz 10 durch vollständige Induktion bewiesen, indem man folgendermassen vorgeht:

Es wird angenommen, es sei bereits bewiesen worden, dass

$$f(x) \equiv g^{(\gamma-1)}(x) \cdot h^{(\gamma-1)}(x) \pmod{L_{\gamma-1}}$$

ist, wo

$$\left.\begin{aligned} g^{(\gamma-1)}(x) &\equiv \varphi(x)^l + \cdots + B_e(x) \cdot p^h = f_1(x) \\ h^{(\gamma-1)}(x) &\equiv \varphi(x)^j \end{aligned}\right\} \pmod{L}.$$

Es soll dann gezeigt werden, dass man die Zusatzfunktionen $G(x)$ und $H(x)$ nur mit Gliedern auf L_γ, also

$$G(x) \equiv H(x) \equiv 0 \pmod{L_{\gamma-1}}$$

bestimmen kann, so dass, wenn

$$\begin{aligned} g^{(\gamma)}(x) &= g^{(\gamma-1)}(x) + G(x) \\ h^{(\gamma)}(x) &= h^{(\gamma-1)}(x) + H(x) \end{aligned}$$

gesetzt wird, die Kongruenz

$$f(x) \equiv g^{(\gamma)}(x) \cdot h^{(\gamma)}(x) \pmod{L_\gamma} \tag{27}$$

erfüllt ist.

Der Beweis wird jetzt ganz analog wie für Satz 10 geführt. Es ist

$$\psi(x) = f(x) - g^{(\gamma-1)}(x) \,.\, h^{(\gamma-1)}(x) \equiv 0 \pmod{L_{\gamma-1}},$$

und da (27) erfüllt sein soll, muss man

$$\psi(x) \equiv G(x) \,.\, h^{(\gamma-1)}(x) + H(x) \,.\, g^{(\gamma-1)}(x) + H(x) \,.\, G(x) \pmod{L_\gamma}.$$

haben. Nach den Voraussetzungen ist aber

$$H(x) \,.\, G(x) \equiv 0 \pmod{L_\gamma},$$

und die zu lösende Aufgabe reduziert sich daher dazu, zu zeigen, dass man die Polynome $G(x)$ und $H(x)$ mit Gliedern auf L_γ finden kann derart, dass

$$G(x) \,.\, h^{(\gamma-1)}(x) + H(x) \,.\, g^{(\gamma-1)}(x) \equiv \psi(x) \pmod{L_\gamma}.$$

Hier können aber in $\psi(x)$ alle Glieder weggelassen werden, welche oberhalb L_γ liegen, man kann also voraussetzen, dass $\psi(x)$ nur Glieder auf L_γ enthält. Ebenso kann man in $h^{(\gamma-1)}(x)$ und $g^{(\gamma-1)}(x)$ alle Glieder weglassen, welche oberhalb L_0 liegen. Die Kongruenz geht dann über in

$$G(x) \,.\, \varphi(x)^j + H(x) \,.\, f_1(x) \equiv \psi(x) \pmod{L_\gamma}. \tag{28}$$

Dies ist aber keine Kongruenz von der Form (22), ausser wenn j ein Multiplum von λ ist. Denn es war z. B.

$$f(x) \equiv \varphi(x)^{l+j} + B_1(x) \,.\, p^\varkappa \,.\, \varphi(x)^{l+j-1} + \cdots + B_e(x) \,.\, \varphi(x)^j \pmod{L_0},$$

und hier sind nicht die Exponenten der Potenzen von $\varphi(x)$ Multipla von λ wie früher. Durch Multiplikation mit $\varphi(x)^\varepsilon$ $(j = t \,.\, \lambda - \varepsilon)$ geht diese Kongruenz in eine Kongruenz der gewöhnlichen Art über. Um die Möglichkeit der Kongruenz (28) zu untersuchen, multipliziere man diese mit $\varphi(x)^\varepsilon$ und erhält

$$G(x) \,.\, \varphi(x)^{t \,.\, \lambda} + H(x) \,.\, \varphi(x)^\varepsilon \,.\, f_1(x) \equiv \psi(x) \,.\, \varphi(x)^\varepsilon \pmod{L_\gamma}.$$

Hier ist, wie eine einfache Überlegung zeigt, $\psi(x) \,.\, \varphi(x)^\varepsilon$ ein Polynom, das im gewöhnlichen Sinne wie in (22) zu L_γ gehört, und man kann daher solche Polynome $G(x)$ und $H_1(x)$ mit Gliedern auf L_γ bestimmen, dass

$$G(x) \,.\, \varphi(x)^{t \,.\, \lambda} + H_1(x) \,.\, f_1(x) \equiv \psi(x) \,.\, \varphi(x)^\varepsilon \pmod{L_\gamma}. \tag{29}$$

Wenn diese Kongruenz erfüllt sein soll, muss aber sicher $H_1(x)$ durch $\varphi(x)^\varepsilon$ teilbar sein, und man kann darum

$$H_1(x) = \varphi(x)^\varepsilon \cdot H(x)$$

setzen. Man dividiert dann die Kongruenz (29) durch $\varphi(x)^\varepsilon$, und die Kongruenz (28) ist in der gewünschten Weise erfüllt. Nach den ersten Durchführungen folgt daraus die Richtigkeit des Satzes 11.

Nach Satz 11 folgt die Zerlegung eines Polynoms (mod p^a), wenn das Polygon aus mehreren Seiten besteht, und aus Satz 10 folgt dann die Zerlegung der Faktoren mit geradlinigen Polygonen.

§ 7. Der Spezialfall $\varphi(x) = x$.

Es soll jetzt der Spezialfall $\varphi(x) = x$ eingehender untersucht werden. Dann ist einfach

$$f(x) = x^n + p^{a_1} \cdot A_1 \cdot x^{n-1} + \cdots + p^{a_n} \cdot A_n \tag{30}$$

die Entwickelung $(p, \varphi(x))$, wo die Koeffizienten A_i nicht durch p teilbar sind. Das Polygon $S(p, x)$ von $f(x)$ besteht aus dem Newtonschen Polygone zu den Punkten (i, α_i) und für dieses Polygon soll die gewöhnliche Bezeichnung angewandt werden, die in § 2 eingeführt wurde.

Wenn nun das Polygon (p, x) bestimmt worden ist, liefert der Satz 4: *$f(x)$ kann im rationalen Bereiche nur Faktoren von den Graden*

$$m = \sum_{i=1}^{r} \varepsilon_i \cdot \lambda_i \tag{31}$$

haben, wo ε_i eine der Zahlen 0, 1, ... *e_i ist.*

Dies ist der früher erwähnte Satz von Dumas.[1]

Aus diesem Satze soll nun ein weiterer Satz bewiesen werden, der für verschiedene Untersuchungen nützlich ist. Sei ϑ eine beliebige, algebraische Zahl und $P(\vartheta)$ der daraus abgeleitete Körper. Sei weiter

$$p = \mathfrak{p}^u \cdot \mathfrak{p}_1$$

eine Idealzerlegung von p in $P(\vartheta)$, wo $\mathfrak{p}$ ein Primideal und $\mathfrak{p}_1$ nicht durch $\mathfrak{p}$ teilbar ist. Aus dem Polygone S für $f(x)(p, x)$ soll nun das Polygon $S'(\mathfrak{p}, x)$ für

[1] Dumas, loc. cit. S. 237.

$f(x)$ bestimmt werden. Die Entwickelung $(\mathfrak{p}, x)$ ist wie früher durch (30) angegeben, indem man bemerkt, dass p^{a_i} genau durch $\mathfrak{p}^{u \cdot a_i}$ teilbar ist. Man hat daher das Polygon zu den Punkten $(i, u \,.\, a_i)$ zu konstruieren. Die Seitenzahl der beiden Polygone wird daher dieselbe, die Projektionen der Seiten auf die X-achse bleiben ungeändert gleich l_i, während für S' die Projektionen auf die Y-achse gleich $u \,.\, h_i$ sind.

Der Satz von Dumas bleibt aber nach § 3 auch in $P(\vartheta)$ richtig, und aus (31) folgt, dass $f(x)$ in diesem Körper nur Faktoren von den Graden

$$m = \sum_{i=1}^{r} \varepsilon_i \,.\, \frac{l_i}{f_i}$$

haben kann, wo f_i der grösste gemeinsame Faktor von l_i und $u \,.\, h_i$ ist und ε_i eine der Zahlen $0, 1, \ldots f_i$ bedeutet. Da aber e_i der grösste gemeinsame Faktor von l_i und h_i ist, so hat man

$$f_i = e_i \,.\, g_i,$$

wo g_i der grösste gemeinsame Faktor von λ_i und u ist. Folglich ist bewiesen:

Satz 12. $p = \mathfrak{p}^u \,.\, \mathfrak{p}_1$ sei eine Zerlegung von p im Körper $P(\vartheta)$. $f(x)$ kann dann in diesem Körper nur Faktoren von den Graden

$$m = \sum_{i=1}^{r} \varepsilon_i \,.\, \frac{\lambda_i}{g_i} \tag{32}$$

haben, wo ε_i eine der Zahlen $0, 1, \ldots, e_i \,.\, g_i$ und g_i der grösste gemeinsame Faktor von λ_i und u ist.

Mittels des Satzes 12 kann man viele interessante Sätze über Gleichungen ableiten, wie ich in der Arbeit: »Gleichungen mit primitiven Gruppen.»[1] gezeigt habe. Aus diesen Untersuchungen folgt z. B. als Spezialfall ein Satz von FURTWÄNGLER.[2]

Man kann hier noch eine andere wichtige Bemerkung machen: Wenn $u = 1$ ist, wird $g_i = 1$, und (32) geht in (31) über. Da nach DEDEKIND u nur dann grösser als 1 sein kann, wenn p ein Teiler der Körperdiskriminante ist, sieht man ein:

Die möglichen Gradzahlen der Faktoren können nur dann geändert werden, wenn p ein Teiler der Körperdiskriminante von $P(\vartheta)$ ist.

---

[1] Zeitschrift für Math. 1923.

[2] FURTWÄNGLER, Math. Ann. 85, S. 37.

Speziell folgt daraus:

Ein Polynom, das nach den Sätzen von Eisenstein oder Königsberger im rationalen Bereiche irreduzibel ist, bleibt auch in jedem Körper irreduzibel, dessen Diskriminante nicht durch p teilbar ist.

In einer anderen Arbeit[1] habe ich gezeigt, wie man aus dieser Bemerkung ganz einfach die Sätze von KRONECKER[2] über die Reduzibilität von Kreisteilungsgleichungen in algebraischen Körpern ableiten und noch allgemeinere Sätze aufstellen kann.

§ 8. Höhere Kongruenzen. Die Sätze von Hensel.

Die Satze des § 6 gestatten eine einfache Untersuchung der Eigenschaften von höheren Kongruenzen für Primzahlpotenzmoduln p^a. $x = x_0$ sei eine Wurzel der Kongruenz

$$f(x) \equiv 0 \pmod{p}. \tag{33}$$

Nun kann man die Frage aufwerfen, wann man aus x_0 eine Wurzel $x_0^{(a)}$ der Kongruenz

$$f(x) \equiv 0 \pmod{p^a} \tag{34}$$

ableiten kann derart, dass

$$x_0^{(a)} \equiv x_0 \pmod{p}.$$

Man soll also die Lösbarkeit der Kongruenz für beliebig grosse α untersuchen oder nach HENSEL, wann die Gleichung $f(x) = 0$ im p-adischen Bereiche lösbar ist.

Wenn x_0 eine einfache Wurzel von (33) ist, so hat man

$$f'(x_0) \not\equiv 0 \pmod{p},$$

und in diesem Falle bestimmt man einfach eine und nur eine Wurzel $x_0^{(a)}$ von (34) von der gewünschten Art.[3]

Wenn aber x_0 eine mehrfache Wurzel ist, wird

$$f'(x_0) \equiv 0 \pmod{p},$$

und p ist in diesem Falle ein Teiler der Diskriminante von $f(x)$. In diesem Falle kann es sehr wohl eintreffen, dass, wenn α genügend gross wird, kein

---

[1] »Irreduzibilität in algebraischen Körpern». Norsk matematisk Forenings skrifter. I, no. 9. Kristiania 1922.

[2] KRONECKER, Journal de math. Sér. I, t. 19, S. 177.

[3] Man sehe z. B. CAHEN: Théorie des nombres. § 168.

solches $x_0^{(\alpha)}$ existiert, wie im Folgenden gezeigt werden soll. Über diese Kongruenzen hat nun HENSEL[1] ein paar wichtige Sätze bewiesen und darin Bedingungen aufgestellt, unter welchen eine p-adische Wurzel existiert, also wann man immer ein $x_0^{(\alpha)}$ bestimmen kann.

Sei allgemein

$$\frac{f^{(i)}(x_0)}{i!}$$

genau durch p^{ϱ_i} teilbar, $f(x_0)$ genau durch p^{ϱ_0}, dann lauten die Sätze von Hensel:

Wenn $\varrho_0 - 2\varrho_1 > 0$ *ist, wird die Kongruenz* (34) *für alle* α *derart lösbar, dass* $x_0^{(\alpha)} \equiv x_0 \pmod{p}$.

Und allgemeiner:

Wenn x_0 *eine derartige Wurzel von* (33) *ist, dass*

$$\varrho_0 > \operatorname{Max}\left(\frac{i\varrho_1 - \varrho_i}{i-1}\right) \quad (i = 2, 3, \ldots \nu)$$

ist, so wird die Kongruenz (34) *für alle* α *in der gewünschten Art lösbar, vorausgesetzt, dass für alle* $x_0^{(\alpha)}$ *die Zahlen* $\varrho_1, \varrho_2, \ldots \varrho_\nu$ *ungeändert bleiben.*

Dabei bedeutet ν die erste Zahl, wofür $\varrho_\nu = 0$ ist.

Es sollen jetzt diese Sätze als Spezialfälle von allgemeineren Sätzen abgeleitet werden. Wenn $f(x) \pmod{p^\alpha}$ die Wurzel $x_0^{(\alpha)}$ haben soll, so ist

$$f(x) - f(x_0^{(\alpha)}) = (x - x_0^{(\alpha)}) f_1(x)$$

oder

$$f(x) \equiv (x - x_0^{(\alpha)}) f_1(x) \pmod{p^\alpha},$$

d. h. $f(x)$ muss $(\text{mod } p^\alpha)$ einen Linearfaktor $x - x_0^{(\alpha)}$ besitzen und umgekehrt, wenn dies der Fall ist, so hat man eine Lösung der Kongruenz (34). Um die Lösbarkeit der Kongruenz (34) zu untersuchen, braucht man daher nur die Faktorenzerlegung $(\text{mod } p^\alpha)$ von $f(x)$ zu bestimmen. Zu diesem Zwecke wird die Entwickelung $(p, x - x_0)$ von $f(x)$ bestimmt, und man hat

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}(x - x_0) + \cdots + (x - x_0)^n.$$

Das zugehörige Polygon S wird dann aus dem Newtonschen Polygone zu den Punkten

$$(0, 0),\ (1, \varrho_{n-1}),\ \ldots\ldots (n-1, \varrho_1),\ (n, \varrho_0)$$

bestehen.

---

[1] HENSEL: Theorie der algebraischen Zahlen. Kap. IV. § 4.

Wenn jetzt $f(x)$ für einen beliebig hohen Modul p^a einen Linearfaktor haben soll, muss es in diesem Polygone wenigstens eine Seite L_i geben, wofür $\lambda_i = 1$ ist. Denn Seiten, wofür $\lambda_i > 1$ ist, können nach § 6 nur Faktoren liefern, in denen höhere Potenzen von $x - x_0$ vorkommen. Weiter müssen die zugehörigen Polynome dieser Seite L_i in der Zerlegung von $f(x)$ (mod S) (§ 4) einen oder mehrere Linearfaktoren (mod L_i) enthalten. Wenn diese Faktoren verschieden sind, ergibt es sich entsprechend viele lineare Faktoren von $f(x)$ (mod p^a) für alle α (§ 6). Wenn mehrere von diesen Linearfaktoren (mod L_i) einander gleich sind, steht die Frage noch dahin.

Es ist also bewiesen:

Damit die Kongruenz (34) *für alle* α *erfüllt sein soll, ist notwendig, dass es in dem Polygone* $(p, x - x_0)$ *mindestens eine Seite* L_i *gibt, wofür* $\lambda_i = 1$ *ist, und der zu dieser Seite gehörige Faktor* $f_i(x)$ *in der Zerlegung (mod S) muss mindestens einen Linearfaktor (mod* L_i*) besitzen. Wenn es einen solchen Linearfaktor gibt, der auch in* $f_i(x)$ *(mod* L_i*) einfach vorkommt, so ist diese Bedingung auch hinreichend.*

Wenn aber alle Linearfaktoren für alle solche Seiten L_i mehrfach vorkommen, steht die Frage noch dahin. Wenn für eine Seite $l_i = \lambda_i = 1$ ist, so sind alle Bedingungen des eben bewiesenen Satzes erfüllt, und man hat:

Satz 13. Wenn es in dem Polygone von $f(x)$ $(p, x - x_0)$ *eine Seite gibt, wofür* $l_i = 1$ *ist, so ist die Kongruenz* (34) *für alle* α *lösbar.*

Um jetzt zu den Henselschen Sätzen zu kommen, braucht man nur diesen Satz umzuformen. Die Bedingung, dass das Polygon eine Seite, haben soll, wofür $l_i = 1$ ist, kann auch folgendermassen ausgedrückt werden. Seien nämlich

$$(n - r, \varrho_r), \ (n - r + 1, \varrho_{r-1})$$

die beiden Punkte des Polygons, wodurch diese Seite geht, dann wird die Gleichung der Seite

$$y - \varrho_r = (\varrho_{r-1} - \varrho_r)(x - n + r)$$

oder

$$y - \varrho_r - (\varrho_{r-1} - \varrho_r)(x - n + r) = 0. \tag{35}$$

Da alle Punkte $(n - i, \varrho_i)$ auf derselben Seite dieser Geraden liegen, so müssen sie alle, in die linke Seite von (35) eingesetzt, Werte von gleichen Vorzeichen ergeben. Da aber für den Punkt (0, 0) dieser Wert positiv ist, wie eine einfache Rechnung zeigt, so ist immer

$$\varrho_i - \varrho_r - (\varrho_{r-1} - \varrho_r)(r - i) > 0$$

und daher

$$\varrho_r < \varrho_i - (\varrho_{r-1} - \varrho_r)(r - i) \quad (i = 0, 1, 2, \ldots r - 2, r + 1, \ldots n).$$

Umgekehrt sieht man leicht ein, dass dies eine hinreichende Bedingung dafür ist, dass das Polygon eine Seite besitzt, wofür die Projektion $l_s = 1$ ist.

Man kann daher Satz 13 so aussprechen:

Satz 14. Wenn für ein r

$$\varrho_r < \text{Max}\,(\varrho_i - (\varrho_{r-1} - \varrho_r)(r-i)) \quad (i = 0, 1, 2, \ldots r-2, r+1, \ldots n)$$

ist, so wird die Kongruenz (34) *für alle α lösbar.*

Für $r = 1$ folgt

$$\varrho_1 < \varrho_i + (\varrho_0 - \varrho_1)(i-1)$$

oder

$$\varrho_i > \frac{i\varrho_1 - \varrho_i}{i-1} \quad (i = 2, 3, \ldots n).$$

Daraus folgt der Satz von Hensel.

Kap. 3. Verallgemeinerung der Dedekindschen Sätze.

§ 1. Die Untersuchungen von Dedekind.

Ich werde in diesem Kapitel die Bestimmung der Primideale eines algebraischen Körpers behandeln. Dabei soll der Einfachkeit wegen der rationale Bereich zu Grunde gelegt werden. Diese Einschränkung ist aber nicht notwendig, und man hätte durch diese Methoden auch ganz allgemein die Primideale eines Relativkörpers bestimmen können.

Es sei wie früher

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

eine ganze, rationale Funktion mit ganzen, rationalen Koeffizienten. Von jetzt an soll aber immer vorausgesetzt werden, dass $f(x)$ im rationalen Bereiche irreduzibel ist und folglich durch die Gleichung

$$f(\vartheta) = 0 \tag{1}$$

ein algebraischer Körper $P(\vartheta)$ n^{ten} Grades definiert wird. Sei D die Diskriminante von $f(x)$ und d die Diskriminante des Zahlenkörpers, dann ist

$$D = k^2 \cdot d,$$

wo der Index k eine ganze, rationale Zahl ist. Im Folgenden soll jede Primzahl p, die in k aufgeht, ein *Indexteiler* heissen.

Weiter sei

$$f(x) \equiv \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \ldots \varphi_r(x)^{e_r} \pmod{p} \tag{2}$$

die Primfunktionzerlegung von $f(x) \pmod{p}$, wo die Primfunktionen $\varphi_i(x)$ von den Graden m_i alle verschieden sind.

Wenn nun in (2)

$$e_1 = e_2 = \cdots = e_r = 1$$

ist, wird p bekanntlich kein Teiler von D, und die Primidealzerlegung von p ist in diesem Falle nach DEDEKIND[1]

$$p = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_r,$$

wo

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

und der Grad von $\mathfrak{p}_i$ ist gleich m_i, also $N\mathfrak{p}_i = p^{m_i}$.

Wenn aber allgemeiner in (2) einige der Exponenten e_i grösser als 1 sind, p aber kein Indexteiler ist, so ist auch

$$p = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_r^{e_r}$$

die Zerlegung von p, wo

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

und $N\mathfrak{p}_i = p^{m_i}$.

Für die Anwendung dieser Untersuchungen muss man natürlich entscheiden können, wann eine gegebene Primzahl ein Teiler des Index ist, und dies liefert das Kriterium von DEDEKIND.[2]

Sei

$$f(x) = \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \ldots \varphi_r(x)^{e_r} + p \cdot M(x)$$

und seien z. B. $e_\alpha, e_\beta, \ldots$ die Exponenten, welche grösser als 1 sind, so ist die Primzahl p dann und nur dann ein Teiler des Index, wenn das Polynom $M(x)$ (mod p) durch eine der Primfunktionen $\varphi_\alpha(x), \varphi_\beta(x), \ldots$ teilbar ist.

---

[1] DEDEKIND: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Göttinger Abhandlungen 1878. § 2. Diese Abhandlung wird im Folgenden mit A bezeichnet.

[2] DEDEKIND A § 3.

§ 2. Anwendung der Newtonschen Polygone auf die Bestimmung der Primideale.

Die Untersuchungen von Dedekind enthalten also die Lücke, dass sie für den Fall eines Indexteilers unanwendbar sind. Um diese Schwierigkeit zu umgehen, könnte man versuchen, anstatt der Gleichung (1) die Gleichung irgend einer anderen Zahl des Körpers zur Bestimmung der Primidealzerlegung von p zu verwenden. Leider aber gibt es, wie DEDEKIND[1] gezeigt hat, Körper, wofür alle Indices k der Zahlen des Körpers einen gemeinsamen Teiler $\Delta > 1$ haben, und für Primzahlen, welche in Δ aufgehen, wird die Dedekindsche Methode ohne Bedeutung. Hensel[2] hat sogar gezeigt »dass das Auftreten solcher gemeinsamen ausserwesentlichen Diskriminantenteiler eigentlich keine Ausnahme, sondern die Regel ist».

Es soll hier gezeigt werden, dass man mit Hilfe der Newtonschen Polygone auch in dem Falle, dass p ein Indexteiler ist, die Primidealzerlegung bestimmen kann.

Für jede der Primfunktionen $\varphi_i(x)$ in (2) soll die zugehörige Entwickelung $(p, \varphi(x))$ von $f(x)$ bestimmt und das zugehörige Polygon gezeichnet werden. Da

$$f(x) \equiv 0 \pmod{p, \varphi(x)},$$

so müssen also diese Polygone auch Seiten besitzen, die über die X-achse fallen, d. h. Hauptpolygone besitzen, und für die späteren Untersuchungen spielen nur diese eine Rolle.

Man sieht jetzt einfach ein:

Die notwendige und hinreichende Bedingung dafür, dass die Primzahl p kein Teiler der Diskriminante D ist, besteht darin, dass alle Hauptpolygone für die Entwickelungen $(p, \varphi(x))$ aus einer Geraden bestehen, wofür $l_1 = 1$ ist.

Denn in diesem Falle ist $f(x) \pmod{p}$ nicht durch das Quadrat einer Primfunktion teilbar. Weiter sieht man mittels des Dedekindschen Kriteriums ein:

Satz 15. Die notwendige und hinreichende Bedingung dafür, dass die Primzahl p kein Teiler des Index k ist, wird dadurch ausgedrückt, dass alle Hauptpolygone für die Entwickelungen $(p, \varphi(x))$ aus Geraden bestehen, wofür entweder $l_1 = 1$ oder $h_1 = 1$ ist.

Die Untersuchungen von Dedekind behandeln daher nur den Fall, dass die Polygone geradlinig sind und ausserdem entweder die X-achsenprojektionen oder

[1] DEDEKIND A § 5.

[2] HENSEL, loc. cit. S. 273.

die Y-achsenprojektionen gleich 1 sind. In diesem Kapitel werde ich diese Untersuchungen in der Weise verallgemeinern, dass ich zunächst allgemein den Fall behandle, dass sämtliche Polygone geradlinig sind. Im nächsten Kapitel soll dann der Fall eines beliebigen Polygones behandelt werden.

§ 3. Bestimmung der möglichen Exponenten.

Den Zusammenhang zwischen der Theorie der Ideale und den Newtonschen Polygonen $(p, \varphi(x))$ sieht man deutlich durch den hier zu beweisenden Satz ein.

Es soll eine Beziehung zwischen den gemeinsamen Primidealfaktoren von p und $\varphi(\vartheta)$ bestimmt werden.

Es seien

$$\left.\begin{aligned} p &= \mathfrak{p}_1^{s_1} \cdot \mathfrak{p}_2^{s_2} \cdots \mathfrak{p}_k^{s_k} \cdot P \\ \varphi(\vartheta) &= \mathfrak{p}_1^{t_1} \cdot \mathfrak{p}_2^{t_2} \cdots \mathfrak{p}_k^{t_k} \cdot \Phi \end{aligned}\right\} \tag{3}$$

die Primidealzerlegungen von p und $\varphi(\vartheta)$, wo die Ideale P und Φ zu einander relativ prim sind. Es sollen nun die Verhältnisse

$$\frac{s_i}{t_i} \quad (i = 1, 2, \ldots k)$$

untersucht und ihre möglichen Werte bestimmt werden. Zu diesem Zwecke wird ein Primideal $\mathfrak{p}$ ausgewählt, und man setzt

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

wo $\mathfrak{p}_1$ und $\mathfrak{p}_2$ nicht durch $\mathfrak{p}$ teilbar sind. Die Kongruenz (2) soll nun in der Form

$$f(x) \equiv \pi(x) \cdot \varphi(x)^e \pmod{p}$$

geschrieben werden, wo $\pi(x) \pmod{p}$ nicht durch $\varphi(x)$ teilbar ist. Daraus leitet man für alle α eine Kongruenz

$$f(x) \equiv \Pi(x) \cdot \Phi(x) \pmod{p^\alpha}$$

ab, wo

$$\left.\begin{aligned} \Pi(x) &\equiv \pi(x) \\ \Phi(x) &\equiv \varphi(x)^e \end{aligned}\right\} \pmod{p}.$$

Wenn hier α genügend gross gewählt wird, so besteht das Polygon $(p, \varphi(x))$ von $\Phi(x)$ aus dem Hauptpolygone von $f(x)(p, \varphi(x))$.

Die ganze Zahl $\Pi(\vartheta)$ kann nicht durch $\mathfrak{p}$ teilbar sein, denn man kann immer solche Polynome $A(x)$ und $B(x)$ bestimmen, dass

$$A(x) \,.\, \Pi(x) + B(x) \,.\, \varphi(x) \equiv 1 \pmod{p},$$

woraus für $x = \vartheta$ folgt:

$$A(\vartheta) \,.\, \Pi(\vartheta) \equiv 1 \pmod{\mathfrak{p}}.$$

Es soll nun die Zahl $\Phi(\vartheta)$ untersucht werden; man bestimmt die zugehörige Entwickelung $(p, \varphi(x))$ für $\Phi(x)$ und konstruiert das daraus bestimmte Polygon. Es sollen für dieses Polygon die Bezeichnungen des Kap. II angewandt werden.

Ein Glied

$$Q_i(x) \,.\, p^{a_i} \,.\, \varphi(x)^i$$

in dieser Entwickelung wird dann genau durch

$$\mathfrak{p}^{s \,.\, a_i + t \,.\, i}$$

teilbar, wenn $x = \vartheta$ gesetzt wird. $Q_i(\vartheta)$ kann nämlich nicht durch $\mathfrak{p}$ teilbar sein, denn da $Q_i(x)$ zu $\varphi(x) \pmod{p}$ relativ prim ist, kann man solche Polynome $A(x)$ und $B(x)$ bestimmen, dass

$$A(x) \,.\, Q(x) + B(x) \,.\, \varphi(x) \equiv 1 \pmod{p}$$

ist und folglich

$$A(\vartheta) \,.\, Q(\vartheta) \equiv 1 \pmod{\mathfrak{p}}.$$

Zu jedem Gliede gibt es also einen zugehörigen Exponenten $s \,.\, a_i + t \,.\, i$. Da $f(\vartheta) = 0$ ist, kann es kein einziges Glied geben, wofür dieser Exponent absolut am kleinsten ist, sondern es muss mindestens zwei oder mehrere Glieder geben, wofür der zugehörige Exponent diesen Minimalwert erreicht. Die repräsentierenden Punkte für diese Glieder müssen nun alle auf derselben Geraden liegen. Denn aus

$$s \,.\, a_i + t \,.\, i = s \,.\, a_j + t \,.\, j$$

folgt sofort

$$\frac{i - j}{a_j - a_i} = \frac{s}{t}. \tag{4}$$

und dieses Verhältnis wird für alle solche Punkte (i, a_i) dasselbe. Nach bekannten Eigenschaften der Newtonschen Polygone wird aber für alle Punkte, welche unterhalb dieser Geraden liegen, die Summe $s \,.\, a_i + t \,.\, i$ kleiner als die entsprechenden Summen für Glieder, welche auf oder oberhalb dieser Geraden

liegen. Da aber der Wert der Summe der kleinste mögliche sein soll, bleibt nur die Möglichkeit übrig, dass diese Gerade mit einer der Seiten des Polygones zusammenfällt.

Es sei nun wie in § 4. II

$$\left.\begin{aligned}\psi_i(x) = p^k \cdot \varphi(x)^l (R_{s,0}(x) \cdot \varphi(x)^{l_s} + R_{s,1}(x) \cdot p^{\varkappa_s} \cdot \varphi(x)^{l_s-\lambda_s} + \\ + R_{s,2}(x) \cdot p^{2\varkappa_s} \cdot \varphi(x)^{l_s-2\lambda_s} + \cdots + R_{s,e_s}(x)\, p^{h_s})\end{aligned}\right\} \quad (5)$$

die Summe der Glieder, deren entsprechende Punkte auf der s^{ten} Seite liegen. Zur Abkürzung ist

$$k = h_1 + h_2 + \cdots + h_{s-1}$$
$$l = e - l_1 - l_2 - \cdots - l_{s-1}$$

gesetzt worden. Für die Glieder von (5) ist aber das Verhältniss (4) konstant, nämlich

$$\frac{s}{t} = \frac{j-i}{\alpha_i - \alpha_j} = \frac{l + l_s - i_1 \cdot \lambda_s - (l + l_s - i_2 \cdot \lambda_s)}{k + i_2 \cdot \varkappa_s - (k + i_1 \cdot \varkappa_s)} = \frac{\lambda_s}{\varkappa_s},$$

und daher ist bewiesen:

Satz 16. Wenn die Primidealzerlegungen von p und $\varphi(\vartheta)$ durch (3) gegeben sind, werden nur solche Exponenten möglich, wofür das Verhältniss $\frac{t_i}{s_i}$ gleich einer der Neigungszahlen $\frac{\varkappa_s}{\lambda_s}$ des Polygones $(p, \varphi(x))$ ist.

Da nun (5) alle Glieder enthält, wofür der Exponent von $\mathfrak{p}$ den kleinsten Wert erreicht, so werden alle anderen Glieder in der Entwickelung $(p, \varphi(x))$ durch höhere Potenzen von $\mathfrak{p}$ teilbar. Da aber $f(\vartheta) = 0$ ist, folgt daraus, dass die Summe

$$R_{s,0}(\vartheta) \cdot \varphi(\vartheta)^{l_s} + R_{s,1}(\vartheta) \cdot p^{\varkappa_s} \cdot \varphi(\vartheta)^{l_s-\lambda_s} + \cdots + R_{s,e_s}(\vartheta) \cdot p^{h_s}$$

sicher durch die Potenz $\mathfrak{p}^{h_s s+1} = \mathfrak{p}^{l_s \cdot t+1}$ teilbar wird. Bestimmt man nun ein Polynom $A_s(x)$ derart, dass

$$A_s(x) \cdot R_{s,0}(x) \equiv 1 \pmod{p, \varphi(x)},$$

so ist $A_s(\vartheta)$ sicher nicht durch $\mathfrak{p}$ teilbar. Die Summe

$$A_s(x)\,(R_{s,0}(x) \cdot \varphi(x)^{l_s} + \cdots + R_{s,e_s}(x)\, p^{h_s})$$

wird dann sicher für $x = \vartheta$ durch $\mathfrak{p}^{h_s \cdot s+1}$ teilbar. Daraus folgt aber nach § 4. II:

Satz 17. Sei $\mathfrak{p}$ *ein Primideal, wofür* $\frac{s}{t} = \frac{\varkappa_i}{\lambda_i}$ *ist. Wenn dann*

$$f_i(x) = \varphi(x)^{l_i} + S_{i,1}(x) \,.\, p^{\varkappa_i} \,.\, \varphi(x)^{l_i - \lambda_i} + \cdots + S_{i,e_i}(x) \,.\, p^{h_i}$$

der Faktor der i^{ten} *Seite in der Zerlegung für das Polygon ist* (§ 4. II), *so ist* $f_i(\vartheta)$ *durch*

$$\mathfrak{p}^{h_i \cdot s+1} = \mathfrak{p}^{l_i \cdot t+1}$$

teilbar.

§ 4. Hilfssätze über algebraische Zahlen.

Sei

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

eine Basis von $P(\vartheta)$; dann kann jede ganze Zahl des Körpers in der Form

$$\alpha = A_1 \,.\, \omega_1 + A_2 \,.\, \omega_2 + \cdots + A_n \,.\, \omega_n$$

geschrieben werden, wo die A_i ganze rationale Zahlen sind. Daher hat man auch

$$\left.\begin{aligned} 1 &= a_1^{(1)} \,.\, \omega_1 + a_2^{(1)} \,.\, \omega_2 + \cdots + a_n^{(1)} \,.\, \omega_n \\ \vartheta &= a_1^{(2)} \,.\, \omega_1 + a_2^{(2)} \,.\, \omega_2 + \cdots + a_n^{(2)} \,.\, \omega_n \\ \vartheta^2 &= a_1^{(3)} \,.\, \omega_1 + a_2^{(3)} \,.\, \omega_2 + \cdots + a_n^{(3)} \,.\, \omega_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \vartheta^{n-1} &= a_1^{(n)} \,.\, \omega_1 + a_2^{(n)} \,.\, \omega_2 + \cdots + a_n^{(n)} \,.\, \omega_n, \end{aligned}\right\} \tag{6}$$

wo alle $a_j^{(i)}$ ganze rationale Zahlen sind und bekanntlich

$$k = \left|a_j^{(i)}\right| \tag{7}$$

ist. Aus (6) leitet man mittels (7) ab:

$$k \,.\, \omega_i = b_0^{(i)} + b_1^{(i)} \,.\, \vartheta + \cdots + b_{n-1}^{(i)} \,.\, \vartheta^{n-1}, \tag{8}$$

wo alle $b_j^{(i)}$ auch ganze rationale Zahlen sind.

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

$$k \,.\, l \equiv 1 \pmod{p},$$

und daher folgt aus (8)

$$\omega_i \equiv l\,(b_0^{(i)} + b_1^{(i)} \,.\, \vartheta + \cdots + b_{n-1}^{(i)} \,.\, \vartheta^{n-1}) \pmod{p},$$

und dies zeigt:

Wenn p kein Indexteiler ist, so wird jede ganze Zahl α des Körpers (mod p) kongruent einer Zahl

$$a_0 + a_1 . \vartheta + \cdots + a_{n-1} . \vartheta^{n-1}, \tag{9}$$

wo alle a_i ganz rational sind.

Weiter folgt einfach, dass in diesem Falle zwei Zahlen $F_1(\vartheta)$ und $F_2(\vartheta)$ mit ganzen rationalen Koeffizienten einander nur dann (mod p) kongruent sein können, wenn

$$F_1(x) \equiv F_2(x) \text{ (modd } p, f(x)),$$

Daraus folgt z. B., dass eine Zahl von der Form (9) nur dann durch p teilbar sein kann, wenn

$$a_0 \equiv a_1 \equiv a_2 \equiv \cdots \equiv a_{n-1} \equiv 0 \text{ (mod } p). \tag{10}$$

Unter den Zahlen (9) gibt es daher (mod p) p^n inkongruente Zahlen.[1]

Wenn aber k durch p teilbar ist, kann man nach der Theorie der linearen Kongruenzen eine solche ganze Zahl β von der Form (9) bestimmen, dass $\beta \equiv 0$ (mod p) ist, ohne dass (10) erfüllt ist. Umgekehrt ist dies auch eine hinreichende Bedingung dafür, dass p ein Indexteiler ist. Unter den Zahlen (9) gibt es daher in diesem Falle weniger als p^n inkongruente für den Modul p. Im nächsten Paragraphen soll aber eine untere Grenze für die Anzahl der inkongruenten Zahlen gegeben werden.

Sei allgemein k durch genau p^ϱ teilbar, also $k = p^\varrho . k_1$, wo k_1 nicht durch p teilbar ist; dann kann man ein l derart bestimmen, dass

$$k_1 . l \equiv 1 \text{ (mod } p^{\varrho+1})$$

und folglich nach (8)

$$\omega_i . p^\varrho \equiv l (b_0^{(i)} + b_1^{(i)} . \vartheta + \cdots + b_{n-1}^{(i)} . \vartheta^{n-1}) \text{ (mod } p^{\varrho+1}).$$

Daraus folgt:

Jede ganze Zahl des Körpers ist einer ganzen Zahl von der Form

$$\frac{1}{p^\varrho} (d_0 + d_1 \vartheta + \cdots + d_{n-1} . \vartheta^{n-1})$$

kongruent.

Dabei ist natürlich nicht gesagt, dass diese Zahlen alle ganz sind.

---

[1] Man sehe auch A, § 1.

Für die späteren Anwendungen soll nun der folgende wichtige Satz bewiesen werden:

Satz 18. Sei α eine ganze Zahl des Körpers, die durch alle verschiedenen Primidealteiler der Primzahl p teilbar ist. Wenn dann α der Gleichung

$$x^n + e_1 . x^{n-1} + \cdots + e_n = 0 \tag{11}$$

genügt, so ist

$$e_1 \equiv e_2 \equiv \cdots \equiv e_n \equiv 0 \pmod{p}.$$

Falls α durch p teilbar ist, wird der Satz beinahe selbstverständlich, wenn man erstens die Gleichung für die ganze Zahl $\frac{\alpha}{p}$ bildet und dann diese Gleichung mit p^n multipliziert. Wenn aber α nicht durch p teilbar ist, gibt es, da α durch alle Primidealfaktoren von p teilbar ist, einen solchen Exponenten a, dass

$$\alpha^a \equiv 0 \pmod{p}.$$

Nach einem bekannten Satze ist nun, wenn man die Gleichung

$$x^n + e_1^{(1)} . x^{n-1} + \cdots + e_n^{(1)} = 0$$

bildet, deren Wurzeln die p^{ten} Potenzen der Wurzeln von (11) sind,

$$e_1 \equiv e_1^{(1)}, \; e_2 \equiv e_2^{(1)}, \; \ldots \; e_n \equiv e_n^{(1)} \pmod{p}.$$

Daraus folgt aber allgemein, dass, wenn man die Gleichung

$$x^n + e_1^{(m)} . x^{n-1} + \cdots + e_n^{(m)} = 0 \tag{12}$$

bildet, deren Wurzeln die $p^{m\text{ten}}$ Potenzen der Wurzeln von (11) sind,

$$e_1 \equiv e_1^{(m)}, \; e_2 \equiv e_2^{(m)}, \; \ldots \; e_n \equiv e_n^{(m)} \pmod{p} \tag{13}$$

ist. Wenn nun m so gross gewählt wird, dass $p^m > a$ ist, so muss a^{p^m} durch p teilbar sein, und folglich werden in (12) alle Koeffizienten durch p teilbar. Aus (13) folgt dann, dass auch in (11) alle Koeffizienten durch p teilbar werden, wodurch der Satz bewiesen ist.

§ 5. Über die Idealteiler der Primzahl p.

Es ist nun möglich, auch im allgemeinsten Falle verschiedene Eigenschaften der Idealteiler von p direkt aus der Primfunktionzerlegung (2) zu bestimmen.

Es soll zunächst untersucht werden, unter welchen Bedingungen eine Zahl α von der Form (9) durch p teilbar sein kann, oder allgemeiner, wann eine solche Zahl α durch alle verschiedenen Primidealteiler von p teilbar ist.

Sei $\alpha = A(\vartheta)$, wo

$$A(x) = a_0 + a_1 x + \cdots + a_{n-1} \cdot x^{n-1}.$$

und $\mathfrak{p}$ ein beliebiges Primideal, das in p und daher auch in $A(\vartheta)$ aufgeht, indem vorausgesetzt wird, dass α durch alle Primidealteiler von p teilbar ist. Sei weiter $B(x)$ der grösste gemeinsame Faktor von $A(x)$ und $f(x)$ (mod p). Dann kann man solche Polynome $C(x)$ und $D(x)$ bestimmen, dass

$$C(x) \cdot f(x) + D(x) \cdot A(x) \equiv B(x) \pmod{p},$$

und daraus folgt, wenn $x = \vartheta$ gesetzt wird,

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

für alle Primidealteiler von p.

Man bildet jetzt die Gleichung

$$B(\vartheta)^n + e_1 \cdot B(\vartheta)^{n-1} + \cdots + e_n = 0 \tag{14}$$

welcher $B(x)$ genügt; dann sind hier nach Satz 17 alle Koeffizienten durch p teilbar. Die Gleichung (14) zeigt wegen der Irreduzibilität von $f(x)$, dass eine Identität

$$B(x)^n + e_1 B(x)^{n-1} + \cdots + e_n = f(x) \cdot F(x)$$

besteht, wo $F(x)$ ein Polynom ist. Daraus folgt aber

$$B(x)^n \equiv 0 \text{ (modd } p, f(x)),$$

und weil $B(x)$ ein Teiler von $f(x)$ (mod p) ist, folgt daraus, dass $B(x)$ (mod p) durch alle Primfunktionen teilbar ist, welche in $f(x)$ aufgehen. Man sieht daher ein, dass eine Zahl $A(\vartheta)$ nur dann durch alle verschiedenen Primidealteiler von p teilbar sein kann, wenn

$$A(x) \equiv 0 \text{ (modd } p, \varphi_1(x) \cdot \varphi_2(x) \ldots \varphi_r(x)).$$

Es folgt leicht, dass diese Bedingung eine hinreichende ist. Speziell ergibt sich aus diesen Untersuchungen das Resultat, dass es unter den Zahlen (9) mindestens

$$p^{m_1+m_2+\cdots+m_r}$$

inkongruente (mod p) gibt.

Es sollen nun ein paar Bemerkungen über die Zerlegung von p gemacht werden. Nach (1) und (2) ist

$$\varphi_1(\vartheta)^{e_1} \cdot \varphi_2(\vartheta)^{e_2} \dots \varphi_r(\vartheta)^{e_r} \equiv 0 \pmod{p}.$$

Hier können zwei Zahlen

$$\varphi_i(\vartheta),\ \varphi_j(\vartheta) \qquad i \neq j$$

keinen gemeinsamen Idealfaktor besitzen, der gleichzeitig in p aufgeht. Denn da $\varphi_i(x)$ zu $\varphi_j(x)$ relativ prim ist, kann man solche Polynome $A(x)$ und $B(x)$ bestimmen, dass

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

und wenn hier $x = \vartheta$ gesetzt wird, folgt leicht die Behauptung. Es ist daher bewiesen:

Wenn die Zerlegung von $f(x)$ (mod p) von der Form (2) ist, so wird

$$p = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \dots \mathfrak{a}_r$$

eine Idealzerlegung von p, wo alle Ideale $\mathfrak{a}_i$ zu einander relativ prim sind und

$$\mathfrak{a}_i = (p, \varphi_i(\vartheta)^{e_i}).$$

Diese Ideale $\mathfrak{a}_i$ können nicht Einheitsideale sein, denn wäre z. B. $\varphi_1(\vartheta)$ zu p relativ prim, so wäre schon das Produkt

$$\varphi_2(\vartheta) \dots \varphi_r(\vartheta)$$

durch alle Primidealteiler von p teilbar, was nach dem eben Bewiesenen unmöglich ist.

Sei nun $\mathfrak{p}_i$ ein Primideal, das gleichzeitig in p und $\varphi_i(\vartheta)$ aufgeht. Wenn dann eine Zahl $\alpha = A(\vartheta)$ von der Form (9) durch $\mathfrak{p}_i$ teilbar sein soll, so muss

$$A(x) \equiv 0 \pmod{p, \varphi_i(x)}$$

sein. Denn wenn dies nicht der Fall wäre, könnte man solche Polynome $B(x)$ und $C(x)$ bestimmen, dass

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

woraus sich für $x = \vartheta$ ergibt

$$A(\vartheta) \cdot B(\vartheta) \equiv 1 \pmod{\mathfrak{p}_i},$$

was nicht möglich ist. Auf Grund dieser Bemerkung folgt, dass es mindestens p^{m_i} inkongruente Zahlen (mod $\mathfrak{p}_i$) gibt, und der Grad von $\mathfrak{p}_i$ kann daher nicht kleiner als m_i sein.

Man kann nun zeigen, dass der Grad von $\mathfrak{p}_i$ immer durch m_i teilbar sein muss. Es sei nämlich $\varphi(x)$ eine Primfunktion, welche (mod p) in $f(x)$ aufgeht, und $\mathfrak{p}$ ein Primideal, wofür

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

Wenn dann f den Grad von $\mathfrak{p}$ bezeichnet, so ist

$$N\mathfrak{p} = p^f,$$

und alle ganzen Zahlen ω des Körpers genügen der Kongruenz

$$\omega^{p^f} - \omega \equiv 0 \pmod{\mathfrak{p}}. \tag{15}$$

Sei jetzt $\Pi(x)$ das Produkt aller Primfunktionen $F(x)$ (mod p), deren Grade Teiler von f sind; dann ist bekanntlich

$$\Pi(x) \equiv x^{p^f} - x \pmod{p}.$$

Nach (15) ist aber auch

$$\vartheta^{p^f} - \vartheta \equiv 0 \pmod{p},$$

folglich gibt es unter den Primfunktionen $F(x)$ eine derart, dass

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

und nach den früheren Bemerkungen muss man dann notwendigerweise

$$F(x) \equiv 0 \pmod{p, \varphi(x)}$$

haben. Da aber $F(x)$ selbst eine Primfunktion ist, folgt

$$F(x) \equiv \varphi(x) \pmod{p},$$

und daher ist der Grad m von $\varphi(x)$ ein Teiler von f, also auch

$$N\mathfrak{p} = p^{e \cdot m},$$

wo e eine ganze Zahl ist.

§ 6. Erste Verallgemeinerung der Dedekindschen Untersuchungen.

Die letzten Untersuchungen gestatten schon unter Anwendung des Satzes 16 die Bestimmung der Primideale von p in allgemeineren Fällen als die Dedekindschen Untersuchungen.

Es sei

$$f(x) \equiv \varphi_1(x)^{l_1} \cdot \varphi_2(x)^{l_2} \ldots \varphi_r(x)^{l_r} \pmod{p} \tag{16}$$

die Primfunktionzerlegung (mod p) von $f(x)$, und es werde vorausgesetzt, dass die Hauptpolygone L_i der Entwickelungen $(p, \varphi_i(x))$ sämtlich geradlinig sind. Die Projektion von L_i auf die X-achse wird dann l_i, und die Projektion auf die Y-achse soll h_i sein, wo weiter vorausgesetzt werden soll, dass h_i zu l_i relativ prim ist. Nach Satz 15 ist offenbar der Fall von Dedekind in diesem allgemeineren enthalten.

Nach § 4 gibt es nun immer mindestens einen gemeinsamen Primidealfaktor $\mathfrak{p}_i$ für p und $\varphi_i(\vartheta)$, und nach Satz 16 muss dieser in einer Potenz in p aufgehen, wo der Exponent ein Multiplum von l_i ist, also etwa in der Potenz $\alpha_i \cdot l_i$. Weiter ist aber nach § 4

$$N\mathfrak{p}_i = p^{\beta_i \cdot m_i},$$

wo β_i eine ganze Zahl ist. Es soll nun gezeigt werden, dass es nur ein einziges solches Primideal $\mathfrak{p}_i$ für alle i gibt. Man hat nämlich

$$p = \mathfrak{p}_1^{\alpha_1 \cdot l_1} \cdot \mathfrak{p}_2^{\alpha_2 \cdot l_2} \ldots\ldots \mathfrak{p}_r^{\alpha_r \cdot l_r} \cdot P, \tag{17}$$

wo das Ideal P durch alle Primideale von p teilbar ist, welche von $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$ verschieden sind. Es soll aber nun gezeigt werden, dass P in der Tat das Einheitsideal ist, also $NP = 1$. Denn nimmt man auf den beiden Seiten von (17) die Norm, so kommt

$$p^n = p^{\Sigma \gamma_i \cdot m_i \cdot l_i} \cdot NP, \tag{18}$$

wo der Kürze wegen

$$\gamma_i = \alpha_i \cdot \beta_i \geqq 1$$

gesetzt worden ist. Dies zeigt aber, dass man immer $\gamma_i = 1$ haben muss, denn es ist doch

$$n = \sum_{i=1}^{r} m_i \cdot l_i,$$

und wenn daher einige der γ_i grösser als 1 wären, so würde in (18) die rechte Seite durch eine höhere Potenz von p als die linke teilbar. Weiter folgt aus (18), dass $NP = 1$ ist.

Es ist folglich bewiesen, dass

$$p = \mathfrak{p}_1^{l_1} \cdot \mathfrak{p}_2^{l_2} \cdots \mathfrak{p}_r^{l_r}, \tag{19}$$

die Primidealzerlegung von p ist. Es bleibt also nur übrig, die Primideale $\mathfrak{p}_i$ als grösste gemeinsame Faktoren von Hauptidealen darzustellen. Nach Satz 16 folgt aus (19)

$$\varphi_i(\vartheta) = \mathfrak{p}_i^{h_i} \cdot \Phi,$$

wo Φ zu p relativ prim ist. Es soll nun die Bezeichnung

$$\Pi_i(x) = \varphi_1(x)^{h_1} \cdots \varphi_{i-1}(x)^{l_{i-1}} \cdot \varphi_{i+1}(x)^{l_{i+1}} \cdots \varphi_r(x)^{l_r}$$

eingeführt werden. Weiter kann man, da l_i zu h_i relativ prim ist, solche ganze rationale positive Zahlen x_i und y_i bestimmen, dass

$$h_i \cdot x_i - l_i \cdot y_i = 1. \tag{20}$$

Dann ist

$$T = \Pi_i(\vartheta)^{y_i} \cdot \frac{\varphi_i(\vartheta)^{x_i}}{p^{y_i}}$$

eine ganze Zahl. Denn $\Pi_i(\vartheta)$ ist nach § 4 durch alle Idealteiler von p teilbar, welche zu $\varphi_i(\vartheta)$ relativ prim sind. Das Primideal $\mathfrak{p}_i$ dagegen geht in p^{y_i} in der Potenz $\mathfrak{p}_i^{l_i \cdot y_i}$ auf, während $\varphi_i(\vartheta)^{x_i}$ genau durch $\mathfrak{p}_i^{h_i \cdot x_i}$ teilbar ist. T ist daher nach (20) eine ganze Zahl, welche genau durch $\mathfrak{p}_i$ in der ersten Potenz teilbar ist.

Man hat daher

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

und kann den Satz aussprechen:

Satz 19. Es sei

$$f(x) \equiv \varphi_1(x)^{h_1} \cdots\cdots \varphi_r(x)^{l_r} \pmod{p}$$

und die Hauptpolygone der Entwickelungen $(p, \varphi_i(x))$ seien sämtlich Geraden mit den Neigungen $\frac{h_i}{l_i}$, wo h_i zu l_i relativ prim ist. Man bestimme x_i und y_i derart, dass

$$x_i \cdot h_i - y_i \cdot l_i = 1,$$

und setze

$$H_i(x) = \varphi_1^{l_1} \dots \varphi_{i-1}^{l_{i-1}} \cdot \varphi_{i+1}^{l_{i+1}} \dots \varphi_r^{l_r}.$$

Dann ist

$$p = \mathfrak{p}_1^{l_1} \cdot \mathfrak{p}_2^{l_2} \dots \mathfrak{p}_r^{l_r},$$

wo das Primideal $\mathfrak{p}_i$ *den Grad* m_i *hat und*

$$\mathfrak{p}_i = \left(p, \varphi_i(\vartheta), H_i(\vartheta)^{y_i} \cdot \frac{\varphi_i(\vartheta)^{x_i}}{p^{y_i}}\right)$$

ist.

Wenn hier für alle i entweder $l_i = 1$ oder $h_i = 1$ ist, kommt man zu dem Falle von Dedekind, und man leitet aus Satz 18 ohne Schwierigkeiten die Dedekindschen Ergebnisse ab. Denn wenn in diesem Falle $\mathfrak{p}_i$ ein gemeinsamer Primidealteiler von p und $\varphi_i(\vartheta)$ ist, so geht dieser entweder in p oder in $\varphi_i(\vartheta)$ in genau der ersten Potenz auf, und man hat daher

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

§ 7. Ein geradliniges Polygon.

Es soll nun allgemein der Fall behandelt werden, dass alle Hauptpolygone in den Entwickelungen $(p, \varphi_i(x))$ Geraden sind. Um aber diese Verhältnisse ganz klar zu machen, werde ich zunächst den einfachsten Fall behandeln, dass $f(x)$ (mod p) nur durch eine einzige Primfunktion $\varphi(x)$ teilbar ist, also

$$f(x) \equiv \varphi(x)^l \pmod{p} \tag{21}$$

und das Polygon $(p, \varphi(x))$ eine Gerade L ist.

Sei

$$\frac{h}{l} = \frac{e \cdot \varkappa}{e \cdot \lambda} = \frac{\varkappa}{\lambda}$$

die Neigungszahl für L. Nach § 5. II kann man

$$f(x) = \varphi(x)^l + A_1(x) \cdot p^{\frac{h}{l}} \cdot \varphi(x)^{l-1} + A_2(x) \cdot p^{\frac{2h}{l}} \cdot \varphi(x)^{l-2} + \dots + A_l(x) \cdot p^h$$

annehmen, und man hat dann mit den früheren Bezeichnungen

$$f(x) \equiv \varphi(x)^l + B_1(x) \cdot p^{\varkappa} \cdot \varphi(x)^{l-\lambda} + \dots + B_e(x)\, p^h \pmod{L}$$

$$B_i(x) = A_{i\lambda}(x) \qquad B_e(x) \not\equiv 0 \ (\text{modd } p, \varphi(x)).$$

Weiter sei

$$f(x) \equiv f_1(x) \cdot f_2(x) \ldots f_s(x) \pmod{L} \tag{22}$$

die Primfunktionzerlegung von $f(x)$ (mod L), wo

$$f_i(x) = \varphi(x)^{\varepsilon_i \cdot \lambda} + C_1^{(i)}(x) \cdot p^{\varkappa} \cdot \varphi(x)^{(\varepsilon_i - 1)\lambda} + \cdots + C_{\varepsilon_i}^{(i)}(x) \cdot p^{\varepsilon_i \cdot \varkappa} \tag{23}$$

und daher

$$n = m \cdot \lambda (\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_s).$$

Es soll nun die Voraussetzung gemacht werden, dass in (22) alle Primfunktionen (mod L) verschieden sind.

Nach (21) ist

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

und alle Primidealteiler von p gehen also in $\varphi(\vartheta)$ auf. Sei $\mathfrak{p}$ ein Primidealteiler von p, so ist

$$\left.\begin{aligned} p &= \mathfrak{p}^s \cdot \mathfrak{p}_1 \\ \varphi(\vartheta) &= \mathfrak{p}^t \cdot \mathfrak{p}_2 \end{aligned}\right\}, \tag{24}$$

wo die Ideale $\mathfrak{p}_1$ und $\mathfrak{p}_2$ nicht durch $\mathfrak{p}$ teilbar sind. Nach Satz 16 ist dann

$$\frac{s}{t} = \frac{\lambda}{\varkappa}$$

oder

$$s \cdot \varkappa = t \cdot \lambda.$$

Aus dieser Gleichheit folgt, dass die Zahlen $p^{\varkappa}$ und $\varphi(\vartheta)^{\lambda}$ durch dieselbe Potenz von $\mathfrak{p}$ teilbar sind. Daher ist, weil dies für alle Primidealteiler von p richtig ist,

$$\theta(\vartheta) = \frac{\varphi(\vartheta)^{\lambda}}{p^{\varkappa}}, \quad \theta(\vartheta)^{\varrho} = \frac{\varphi(\vartheta)^{l}}{p^{h}}$$

eine ganze Zahl des Körpers, und diese Zahl ist ausserdem zu p relativ prim.

Wenn man (24) in die Gleichung $f(\vartheta) = 0$ einsetzt, so sieht man ein, dass alle Glieder in $f(x)$, deren repräsentierende Punkte auf L liegen, genau durch

$$\mathfrak{p}^{s \cdot h} = \mathfrak{p}^{t \cdot l}$$

teilbar werden müssen. Alle übrigen Glieder in $f(x)$ werden gewiss durch höhere Potenzen von $\mathfrak{p}$ teilbar.

Es soll nun $f(\vartheta)$ durch p^h dividiert werden, und man erhält

$$\frac{f(\vartheta)}{p^h} = \psi_1(\vartheta, \theta(\vartheta)) \cdot \psi_2(\vartheta, \theta(\vartheta)) \ldots \psi_s(\vartheta, \theta(\vartheta)) + M(\vartheta), \tag{25}$$

wo

$$\psi_i(x, y) = y^{\varepsilon_i} + C_1^{(i)}(x) \cdot y^{\varepsilon_i - 1} + \cdots + C_{\varepsilon_i}^{(i)}(x)$$

und daher

$$\psi_i(\vartheta, \theta(\vartheta)) = \frac{f_i(\vartheta)}{p^{\varepsilon_i \cdot \varkappa}} = \theta(\vartheta)^{\varepsilon_i} + C_1^{(i)}(\vartheta) \quad \theta(\vartheta)^{\varepsilon_i - 1} + \cdots + C_{\varepsilon_i}^{(i)}(\vartheta). \tag{26}$$

In (25) ist weiter

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

für alle Primidealteiler von p und daraus folgt weiter aus (25), dass das Produkt

$$F(\vartheta, \theta(\vartheta)) = \psi_1(\vartheta, \theta(\vartheta)) \ldots \psi_s(\vartheta, \theta(\vartheta))$$

durch alle Primidealteiler von p teilbar sein muss, eine Tatsache, die man auch einfach aus dem Satze 17 ableitet. Der Kürze wegen ist hier

$$F(x, y) = \psi_1(x, y) \ldots \psi_s(x, y)$$

gesetzt worden.

Es soll nun das Ideal

$$\mathfrak{a}_i = [p, \psi_i(\vartheta, \theta(\vartheta))]$$

untersucht werden und zwar erstens gezeigt werden, dass $\mathfrak{a}_i$ kein Einheitsideal ist.

Anstatt der natürlichen Ordnung

$$[1, \vartheta, \ldots \vartheta^{n-1}],$$

welche in § 4 untersucht worden ist, sollen hier alle ganzen Zahlen von der Form

$$A(\vartheta, \theta(\vartheta)) = A_1(\vartheta) \cdot \theta(\vartheta)^{e-1} + A_2(\vartheta) \cdot \theta(\vartheta)^{e-2} + \cdots + A_e(\vartheta), \tag{27}$$

untersucht werden, wo die $A_i(\vartheta)$ beliebige Polynome in ϑ sind.

Es soll nun erstens untersucht werden, wann eine solche Zahl durch alle Primidealteiler von p teilbar sein kann. Es sei jetzt $A(\vartheta, \theta(\vartheta))$ eine gegebene Zahl von dieser Eigenschaft. Man kann dann den grössten gemeinsamen Faktor

$B(x, y)$ von $A(x, y)$ und $F(x, y)$ (modd $p, \varphi(x)$) bilden und nach § 1. I ist es immer möglich solche Funktionen $C(x, y)$ und $D(x, y)$ zu bestimmen, dass

$$C(x, y) \cdot F(x, y) + D(x, y) \cdot A(x, y) \equiv B(x, y) \text{ (modd } p, \varphi(x)).$$

Daraus folgt sofort, wenn $x = \vartheta, y = \theta(\vartheta)$ gesetzt wird, dass auch $B(\vartheta, \theta(\vartheta))$ durch alle Primidealfaktoren von p teilbar sein muss. Ohne der Allgemeinheit zu schaden, kann man nun annehmen, dass in $B(\vartheta, \theta(\vartheta))$ der höchste Koeffizient für $\theta(\vartheta)$ gleich 1 ist. Denn wäre er etwa $B_0(\vartheta)$, so kann man immer ein $C_0(x)$ derart finden, dass

$$C_0(x) \cdot B_0(x) \equiv 1 \text{ (modd } p, \varphi(x))$$

ist, und die obige Kongruenz mit $C_0(x)$ multiplizieren. Man kann also

$$B(x, y) = y^\varepsilon + C_1(x) \cdot y^{\varepsilon-1} + \cdots + C_\varepsilon(x)$$

annehmen, und daher ist

$$p^{\varepsilon \cdot \varkappa} \cdot B(x, \theta(x)) = B'(x) = \varphi(x)^{\varepsilon \cdot \lambda} + C_1(x) \cdot p^\varkappa \varphi(x)^{(\varepsilon-1)\lambda} + \cdots + C_\varepsilon(x) \cdot p^{\varepsilon \cdot \varkappa}.$$

Es wird jetzt die Gleichung

$$B^n + e_1 \cdot B^{n-1} + \cdots + e_n = 0$$

gebildet, welcher die Zahl $B(\vartheta, \theta(\vartheta))$ genügt, wo nach Satz 18 alle e_i durch p teilbar sind. Diese Gleichung zeigt aber wegen der Irreduzibilität von $f(x)$, dass eine Identität

$$B(x, \theta(x))^n + e_1 \cdot B(x, \theta(x))^{n-1} + \cdots + e_n = f(x) \cdot g(x) \tag{28}$$

besteht. Wenn diese Identität mit $p^{\varepsilon \cdot \varkappa \cdot n}$ multipliziert wird, geht sie in die ganzzahlige Gleichheit

$$B'(x)^n + e_1 \cdot p^{\varepsilon \cdot \varkappa} \cdot B'(x)^{n-1} + \cdots + e_n \cdot e^{\varepsilon \cdot \varkappa \cdot n} = f(x) \cdot g_1(x)$$

über, und hier hat die linke Seite $(p, \varphi(x))$ das Polygon L und ist (mod L) kongruent

$$B'(x)^n.$$

Daher hat auch die rechte Seite das Polygon L, und wegen der Eindeutigkeit der Zerlegung (mod L) sieht man ein, dass $B'(x)$ (mod L) durch $f(x)$ teilbar ist. Daraus folgt aber weiter, dass $B(x, y)$ (modd $p, \varphi(x)$) durch $F(x, y)$ teilbar sein

muss, und da $A(x, y)$ nach (27) höchstens vom Grade $e-1$ in y ist, muss man

$$A_1(x) \equiv A_2(x) \equiv \cdots \equiv A_e(x) \equiv 0 \pmod{p, \varphi(x)} \tag{29}$$

haben.

Daraus folgt leicht, dass ein Ideal $\mathfrak{a}_i$ nicht das Einheitsideal sein kann. Denn wenn $\mathfrak{a}_i$ ein Einheitsideal wäre, müsste schon das Produkt

$$\psi_1(\vartheta, \theta(\vartheta)) \ldots \psi_{i-1}(\vartheta, \theta(\vartheta)) \psi_{i+1}(\vartheta, \theta(\vartheta)) \ldots \psi_s(\vartheta, \theta(\vartheta))$$

durch alle Primidealteiler von p teilbar sein, was nach dem eben Bewiesenen nicht möglich ist.

Es sei daher $\mathfrak{p}_i$ ein Primideal, das in $\mathfrak{a}_i$ aufgeht. Wenn eine Zahl von der Form (27) durch $\mathfrak{p}_i$ teilbar sein soll, muss die Funktion $A(x, y) \pmod{p, \varphi(x)}$ durch $\psi_i(x, y)$ teilbar sein. Denn wenn dies nicht der Fall wäre, könnte man solche Funktionen $B(x, y)$ und $C(x, y)$ bestimmen, dass

$$A(x, y) \cdot B(x, y) + \psi_i(x, y) \cdot C(x, y) \equiv 1 \pmod{p, \varphi(x)}$$

und folglich

$$A(\vartheta, \theta(\vartheta)) \cdot B(\vartheta, \theta(\vartheta)) \equiv 1 \pmod{\mathfrak{p}_i}$$

wäre, was offenbar nicht möglich ist.

Dies zeigt, dass es unter den Zahlen (27) immer mindestens $p^{\varepsilon_i \cdot m}$ inkongruente für das Ideal $\mathfrak{p}_i$ gibt, und daher ist der Grad f_i von $\mathfrak{p}_i$ sicher nicht kleiner als $\varepsilon_i \cdot m$.

f_i ist nach § 4 immer durch m teilbar, also etwa $f_i = e_i \cdot m$. Man kann aber weiter zeigen, dass e_i immer durch ε_i teilbar sein muss. Denn da jede ganze Zahl des Körpers der Kongruenz

$$\omega^{p^{e_i \cdot m}} - \omega \equiv 0 \pmod{\mathfrak{p}_i}$$

genügt, so ist auch

$$\theta(\vartheta)^{p^{e_i \cdot m}} - \theta(\vartheta) \equiv 0 \pmod{\mathfrak{p}_i}.$$

Nach Satz 2. I ist aber

$$y^{p^{e_i \cdot m}} - y$$

kongruent dem Produkt aller Primfunktionen $H(x, y) \pmod{p, \varphi(x)}$, deren Grade Teiler von e_i sind. Es muss daher eine solche Primfunktion $H(x, y)$ geben, dass

$$H(\vartheta, \theta(\vartheta)) \equiv 0 \pmod{\mathfrak{p}_i},$$

und daraus folgt nach den, früheren Bemerkungen, dass $H(x, y)$ (modd $p, \varphi(x)$) durch $\psi_i(x, y)$ teilbar und, da diese Funktionen beide Primfunktionen sind,

$$H(x, y) \equiv \psi_i(x, y) \text{ (modd } p, \varphi(x))$$

sein muss, also beide von demselben Grade sein müssen, und daraus folgt sofort, dass ε_i ein Teiler von e_i ist.

Man hat daher

$$N\mathfrak{p}_i = p^{a_i \cdot \varepsilon_i \cdot m},$$

wo α_i eine ganze Zahl ≥ 1 ist. Weiter geht $\mathfrak{p}_i$ in p in einer Potenz auf, deren Exponent ein Multiplum von λ ist, und folglich wird das Ideal

$$p' = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_s)^\lambda$$

sicher ein Teiler von p. Hier ist

$$Np' = p^{m \cdot \lambda \cdot \sum_1^s a_i \cdot \varepsilon_i}, \quad Np = p^n,$$

und es muss

$$n \geq m \cdot \lambda \cdot (\alpha_1 \cdot \varepsilon_1 + \alpha_2 \cdot \varepsilon_2 + \cdots + \alpha_s \cdot \varepsilon_s)$$

sein. Da aber

$$n = m \cdot \lambda (\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_s)$$

ist, muss notwendigerweise

$$\alpha_1 = \alpha_2 = \cdots = \alpha_s = 1$$

sein, und da dann $Np' = p^n$ wird, muss auch

$$p = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_s)^\lambda$$

die Primidealzerlegung von p sein.

Daraus folgt nach Satz 16, dass auch

$$\varphi(\vartheta) = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_s)^\varkappa \cdot \Phi,$$

wo das Ideal Φ zu p relativ prim ist.

Es soll nun das Primideal $\mathfrak{p}_i$ bestimmt werden. $\mathfrak{p}_i$ war ein Teiler des Ideals $\mathfrak{a}_i$; dieses Ideal kann aber nicht durch andere Primideale teilbar sein, denn sonst würde man nach den obigen Schlüssen $Np > p^n$ erhalten, was offenbar nicht möglich ist. Es muss daher $\mathfrak{a}_i$ eine Potenz von $\mathfrak{p}_i$ sein.

Man bestimme nun die positiven Zahlen x und y derart, dass

$$x \,.\, \varkappa - y \,.\, \lambda = 1$$

ist, was immer möglich ist, da $\varkappa$ zu λ relativ prim ist. Dann wird die Zahl

$$\frac{\varphi(\vartheta)^x}{p^y}$$

ganz und durch jedes Primideal $\mathfrak{p}_i$ genau in der ersten Potenz teilbar. Denn $\mathfrak{p}_i$ geht im Zähler genau in der Potenz $x \,.\, \varkappa$ und im Nenner in der Potenz $y \,.\, \lambda$ auf, und da $x \,.\, \varkappa > y \,.\, \lambda$, ist die Zahl ganz und, wie man leicht sieht, durch $\mathfrak{p}_i$ genau in der ersten Potenz teilbar. Man erhält daher für $\mathfrak{p}_i$ die Darstellung:

$$\mathfrak{p}_i = \left(p, \frac{\varphi(\vartheta)^x}{p^y}, \psi_i(\vartheta, \theta(\vartheta))\right).$$

Man kann die Resultate folgendermassen in einem Satze zusammenfassen:

Satz 20. Sei

$$f(x) \equiv \varphi(x)^l \pmod{p}$$

und das Polygon $(p, \varphi(x))$ *eine Gerade* L *von der Neigung* $\frac{\varkappa}{\lambda}$ *und*

$$f(x) \equiv f_1(x) \,.\, f_2(x) \ldots f_s(x) \pmod{L},$$

wo alle Primfunktionen $f_i(x)$ *verschieden sind und* $f_i(x)$ *vom Grade* $\varepsilon_i \,.\, m$ *in* x *ist. Dann hat man für* p *die Primidealzerlegung*

$$p = (\mathfrak{p}_1 \,.\, \mathfrak{p}_2 \ldots \mathfrak{p}_s)^\lambda .$$

Das Primideal $\mathfrak{p}_i$ *ist vom Grade* $\varepsilon_i \,.\, m$ *und durch*

$$\mathfrak{p}_i = \left(p, \frac{\varphi(\vartheta)^x}{p^y}, \frac{f_i(\vartheta)}{p^{\varepsilon_i \,.\, x}}\right)$$

bestimmt, wo die positiven, ganzen rationalen Zahlen x *und* y *die Gleichung* $x \,.\, \varkappa - y \,.\, \lambda = 1$ *erfüllen.*

Dadurch ist der einfachste Fall erledigt, und man sieht ein, dass es für diese Seite gewisse Primideale gibt, deren Produkt in der λ^{ten} Potenz in p aufgeht. Ein ganz analoges Verhältnis hat man, wenn das betrachtete Polygon mehrere Seiten besitzt und wenn gleichzeitig mehrere Polygone vorkommen. Die Untersuchungen in diesem Paragraphen beruhen hauptsächlich darauf, dass die Zahlen $\theta(\vartheta)^i$ ganz sind. Bei allgemeineren Polygonen kommt die Schwierigkeit hinzu,

dass die für jede Seite entsprechend gebildeten Zahlen nicht mehr ganz werden und daher das hier angewandte Schlussverfahren modifiziert werden muss. Unter den Voraussetzungen des nächsten Paragraphen kann diese Schwierigkeit ziemlich einfach überwunden werden, erst im nächsten Kapitel wird gezeigt, wie man unter den allgemeinsten Voraussetzungen vorgehen kann.

§ 8. Geradlinige Polygone im Allgemeinen.

Nachdem der Fall behandelt worden ist, dass $f(x)$ (mod p) nur durch eine Primfunktion teilbar und das Polygon $(p, \varphi(x))$ eine Gerade ist, überführt man dieses Resultat ziemlich analog auf den Fall, dass

$$f(x) \equiv \varphi_1(x)^{l_1} \cdot \varphi_2(x)^{l_2} \dots \varphi_s(x)^{l_s} \pmod{p}$$

und das Hauptpolygon $(p, \varphi_i(x))$ für alle i eine Gerade L_i ist. $\frac{\varkappa_i}{\lambda_i} = \frac{h_i}{l_i}$ sei die Neigungszahl für L_i. Man bestimmt die Primfunktionzerlegung von $f(x)$ (mod L_i), und es soll angenommen werden, dass die Primfunktionen

$$f_1^{(i)}(x),\ f_2^{(i)}(x),\ \dots f_{t_i}^{(i)}(x)$$

alle (mod L_i) verschieden sind und der Grad von $f_j^{(i)}(x)$ in $\varphi_i(x)^{\lambda_i}$ gleich $\varepsilon_j^{(i)}$ ist.

Es sei nun der Kürze wegen $\varphi_i(x) = \varphi(x)$ gesetzt und

$$f(x) \equiv \pi(x) \cdot \varphi(x)^l \pmod{p}, \tag{30}$$

wo $\pi(x)$ zu $\varphi(x)$ (mod p) relativ prim und das Hauptpolygon L zu $f(x)$ $(p, \varphi(x))$ geradlinig und von der Neigungszahl $\frac{h}{l}$ ist. Aus (30) folgt

$$f(x) \equiv \Pi(x) \cdot \Phi(x) \pmod{p^{h+1}}, \tag{31}$$

wo $\Phi(x) \equiv \varphi(x)^l \pmod{p}$. Die Zahl $\Pi(\vartheta)$ ist daher durch alle Idealteiler von p^{h+1} teilbar, welche zu $\varphi(\vartheta)$ relativ prim sind. Es soll nun

$$\theta(\vartheta) = \frac{\varphi(\vartheta)^\lambda}{p^\varkappa}$$

gesetzt werden, aber diese Zahl ist nicht wie in § 7 ganz. Die Zahlen

$$\Pi(\vartheta) \cdot \theta(\vartheta)^\varepsilon = \Pi(\vartheta) \cdot \left(\frac{\varphi(\vartheta)^\lambda}{p^\varkappa}\right)^\varepsilon \quad (\varepsilon = 1, 2, \dots e) \tag{32}$$

sind dagegen alle ganz. Denn wenn $\mathfrak{p}$ ein Primideal ist, wofür

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

so ist $\frac{s}{t} = \frac{\lambda}{\varkappa}$, und daraus folgt, dass die Zahlen (32) alle ganz und nicht durch $\mathfrak{p}$ teilbar sind.

Sei nun

$$\Phi(x) \equiv f_1(x) \ldots f_t(x) \pmod{L},$$

wo

$$f_j(x) = \varphi(x)^{e_j \cdot \lambda} + C_1^{(j)}(x) \cdot p^{\varkappa} \cdot \varphi(x)^{(e_j-1)\lambda} + \cdots + C_{e_j}^{(j)}(x) \cdot p^{e_j \cdot \varkappa}.$$

Wenn man dann die Kongruenz (31) durch p^h dividiert, erhält man

$$\frac{f(\vartheta)}{p^h} = \psi_1(\vartheta, \theta(\vartheta)) \ldots \psi_t(\vartheta, \theta(\vartheta)) \cdot \Pi(\vartheta) + M(\vartheta),$$

wo $M(\vartheta)$ durch alle Primidealteiler von p teilbar wird, und daher hat auch die Zahl

$$\Pi(\vartheta)\, \psi_1(\vartheta, \theta(\vartheta)) \ldots \psi_t(\vartheta, \theta(\vartheta))$$

diese Eigenschaft. Dabei bedeutet

$$\psi_j(x, y) = y^{e_j} + C_1^{(j)}(x) \cdot y^{e_j - 1} + \cdots + C_{e_j}^{(j)}(x),$$

und weiter soll

$$F(x, y) = \psi_1(x, y) \ldots \psi_t(x, y)$$

gesetzt werden.

Es sollen nun alle Zahlen von der Form

$$\Pi(\vartheta) \cdot A(\vartheta, \theta(\vartheta)) = \Pi(\vartheta)\,(A_0(\vartheta) + A_1(\vartheta) \cdot \theta(\vartheta) + \cdots + A_{e-1}(\vartheta) \cdot \theta(\vartheta)^{e-1}) \qquad (33)$$

untersucht werden, wo die $A_i(\vartheta)$ Polynome in ϑ bedeuten. Diese Zahlen spielen für diese Untersuchungen eine ganz analoge Rolle wie früher die Zahlen (27). Speziell soll untersucht werden, wann eine Zahl $\Pi(\vartheta) A(\vartheta, \theta(\vartheta))$ durch alle Primidealteiler von p teilbar sein kann, und da diese Zahl immer durch alle Primideale von p teilbar ist, welche nicht in $\varphi(\vartheta)$ aufgehen, bleibt nur übrig zu untersuchen, wann eine solche Zahl durch alle Primidealteiler von $(p, \varphi(\vartheta))$ teilbar ist.

Die Zahl (33) sei nun durch alle Primidealfaktoren von p teilbar. Man bildet dann den grössten gemeinsamen Faktor $B(x, y)$ (modd $p, \varphi(x)$) von $A(x, y)$ und $F(x, y)$ und hat

$$A(x, y) \cdot C(x, y) + F(x, y) \cdot D(x, y) \equiv B(x, y) \pmod{p, \varphi(x)},$$

wo die Funktionen $C(x, y)$ und $D(x, y)$ immer bestimmt werden können. Wenn diese Kongruenz mit $\Pi(x)^2$ multipliziert und $x = \vartheta$ gesetzt wird, folgt, dass auch

$$\Pi^2(\vartheta) \,.\, B(\vartheta, \theta(\vartheta))$$

durch alle Primideale von p teilbar ist, und daraus folgt ohne Weiteres, dass

$$b = \Pi(\vartheta) \,.\, B(\vartheta, \theta(\vartheta))$$

diese Eigenschaft besitzt. Man kann hier wie früher annehmen, dass $B(x, y)$ von der Form

$$B(x, y) = y^\varepsilon + C_1(x) \,.\, y^{\varepsilon-1} + \cdots + C_\varepsilon(x)$$

und daher

$$p^{\varepsilon \cdot \varkappa} \,.\, B(x, \theta(x)) = B'(x) = \varphi(x)^{\varepsilon \cdot \lambda} + C_1(x) \,.\, p^\varkappa \,.\, \varphi(x)^{(\varepsilon-1)\lambda} + \cdots + C_\varepsilon(x) \,.\, p^{\varepsilon \cdot \varkappa}$$

ein Polynom mit dem Polygone $L(p, \varphi(x))$ ist.

Man bildet nun die Gleichung

$$b^n + b^{n-1} \,.\, e_1 + \cdots + e_n = 0,$$

welcher b genügt und welche besagt, dass eine Identität

$$\Pi(x)^n \,.\, B(x, \theta(x))^n + \cdots + e_n = f(x) \,.\, g(x)$$

besteht, wo nach Satz 18 alle e_i durch p teilbar sind. Wenn diese Identität mit $p^{\varepsilon \cdot \varkappa \cdot n}$ multipliziert wird, geht sie in

$$\Pi(x)^n \,.\, B'(x)^n + e_1 \,.\, p^{\varepsilon \cdot \varkappa} \,.\, \Pi(x)^{n-1} \,.\, B'(x)^{n-1} + \cdots + p^{\varepsilon \cdot \varkappa \cdot n} = f(x) \,.\, g_1(x)$$

über, und wie man leicht einsieht, hat hier die linke Seite das geradlinige Hauptpolygon L und ist kongruent $B'(x)^n$ (mod L). Für die rechte Seite muss das Hauptpolygon $(p, \varphi(x))$ daher auch gleich L sein, und es folgt, dass $B'(x)$ (mod L) durch das Produkt $f_1(x) \,.\, f_2(x) \ldots f_t(x)$ teilbar sein muss. Dies ist aber nur möglich, wenn $B(x, y)$ (modd p, $\varphi(x)$) durch $F(x, y)$ teilbar ist, und dies zeigt natürlich, dass in $A(x, y)$ alle Koeffizienten kongruent Null (modd p, $\varphi(x)$) sind. Eine Zahl von der Form (33) kann also nicht durch alle Primidealfaktoren von p teilbar sein, ausser wenn

$$A_0(x) \equiv A_1(x) \equiv \cdots \equiv A_{e-1}(x) \equiv 0 \text{ (modd } p, \varphi(x)).$$

Es sollen nun die Ideale

$$\mathfrak{a}_j = (p, \varphi(\vartheta), \ \Pi(\vartheta) \, . \, \psi_j(\vartheta, \theta(\vartheta))$$

untersucht werden und zwar soll erstens gezeigt werden, dass $\mathfrak{a}_j$ nicht das Einheitsideal sein kann. Denn wäre $\psi_j(\vartheta, \theta(\vartheta)) \, . \, \Pi(\vartheta)$ zu $(p, \varphi(\vartheta))$ relativ prim, so wäre schon

$$\Pi(\vartheta) \, \psi_1 \ldots \psi_{j-1} \, . \, \psi_{j+1} \ldots \psi_t$$

durch alle Primideale von p teilbar, was nach dem Bewiesenen nicht möglich ist.

Es sei daher $\mathfrak{p}_j$ ein Primideal, das in $\mathfrak{a}_j$ aufgeht. Eine Zahl

$$\Pi(\vartheta) \, . \, A(\vartheta, \theta(\vartheta))$$

kann dann nicht durch $\mathfrak{p}_j$ teilbar sein, ausser wenn $A(x, y)$ (modd $p, \varphi(x)$) durch $\psi_j(x, y)$ teilbar ist. Denn wenn dies nicht der Fall wäre, könnte man solche Funktionen $C(x, y)$ und $D(x, y)$ bestimmen, dass

$$A(x, y) \, . \, C(x, y) + \psi_j(x, y) \, . \, D(x, y) \equiv 1 \ (\text{modd } p, \varphi(x)),$$

woraus durch Multiplikation mit $\Pi(x)^2$ und für $x = \vartheta, \ y = \theta(\vartheta)$ folgt:

$$\Pi(\vartheta) \, . \, A(\vartheta, \theta(\vartheta)) \, . \, \Pi(\vartheta) \, . \, C(\vartheta, \theta(\vartheta)) \equiv \Pi(\vartheta)^2 \ (\text{mod } \mathfrak{p}_i),$$

was offenbar nicht möglich ist, da $\Pi(\vartheta)$ nicht durch $\mathfrak{p}_j$ teilbar ist. Dies zeigt, dass es (mod $\mathfrak{p}_j$) mindestens $p^{\varepsilon_j \cdot m}$ verschiedene inkongruente Zahlen gibt und dass daher der Grad von $\mathfrak{p}_j$ nicht kleiner als $\varepsilon_j \, . \, m$ sein kann, also etwa $f_j = \varepsilon_j \, . \, m + \varrho_j$ ist, wo $\varrho_j \geq 0$ ist.

Nun geht $\mathfrak{p}_j$ in p in mindestens einer Potenz λ auf, und daher ist das Ideal

$$P = \mathfrak{p}_1^{\lambda} \, . \, \mathfrak{p}_2^{\lambda} \ldots \mathfrak{p}_t^{\lambda}$$

gewiss ein Teiler von p. Hier ist

$$N P = p^{\lambda \Sigma(\varepsilon_j \, . \, m + \varrho_j)} = p^{n'},$$

und da

$$m \, . \, \lambda \, . \sum_{j=1}^{t} \varepsilon_j = m \, . \, l$$

ist, muss man $n' \geq m \, . \, l$ haben, wo das Gleichheitszeichen nur dann vorkommen kann, wenn alle ϱ_j verschwinden.

Wenn nun diese Untersuchungen für alle Primfunktionen $\varphi_i(x)$ richtig sind, kann man für alle i solche Ideale P_i bestimmen, die Teiler von p sind, und da diese P_i alle zu einander relativ prim sind, so ist auch

$$p' = P_1 . P_2 \ldots P_s$$

ein Teiler von p, und es ist

$$Np' = p^{\Sigma n'_i}.$$

Da aber für alle i $n'_i \geqq m_i . l_i$, so wird auch

$$\sum_{i=1}^{s} n'_i \geqq \sum_{i=1}^{s} m_i . l_i = n,$$

während man doch immer, weil p' ein Idealteiler von p ist,

$$\sum_{i=1}^{s} n'_i \geqq n$$

haben muss. Es bleibt daher nur die Möglichkeit übrig, dass

$$\sum_{i=1}^{s} n'_i = n \tag{34}$$

ist, und daraus folgt, dass die Ideale p und p' gleich sein müssen, und folglich ist die Primidealzerlegung von p durch

$$\left.\begin{aligned} p &= P_1 . P_2 \ldots P_s \\ P_i &= \left(\mathfrak{p}_1^{(i)} . \mathfrak{p}_2^{(i)} \ldots \mathfrak{p}_{l_i}^{(i)}\right)^{\lambda_i} \end{aligned}\right\} \tag{35}$$

bestimmt.

Die Gleichung (34) kann nur dann erfüllt sein, wenn immer $n' = m . l$ für alle Primfunktionen $\varphi_i(x)$ ist, und daraus folgt, dass alle ϱ_j verschwinden müssen, und es ist folglich

$$N\mathfrak{p}_j^{(i)} = p^{\varepsilon_j^{(i)} . m_i},$$

wodurch der Grad von $\mathfrak{p}_j^{(i)}$ bestimmt ist.

Man kommt jetzt zu der Aufgabe, das Primideal $\mathfrak{p}_j^{(i)}$ zu bestimmen. Das Ideal

$$\mathfrak{a}_j^{(i)} = [p, \varphi_i(\vartheta), \Pi_i(\vartheta) . \psi_j^{(i)}(\vartheta, \theta_i(\vartheta))]$$

war durch $\mathfrak{p}_j^{(i)}$ teilbar, und aus den obigen Schlüssen folgt, dass $\mathfrak{a}_j^{(i)}$ nicht durch andere Primidealteiler von p teilbar sein kann. $\mathfrak{a}_j^{(i)}$ muss daher eine Potenz von $\mathfrak{p}_j^{(i)}$ sein.

Man kann den Ausdruck dieses Ideals etwas umformen, indem man berücksichtigt, dass in dem Ausdrucke

$$\Pi_i(\vartheta) \,.\, \psi_j^{(i)}(\vartheta, \theta_i(\vartheta)) = \Pi_i(\vartheta) \,.\, \frac{f_j^{(i)}(\vartheta)}{p^{\varepsilon_j^{(i)} \cdot \varkappa_i}}$$

der Faktor $\Pi_i(\vartheta)$ nur zugesetzt worden ist, um eine ganze Zahl zu erhalten. Man kann daher anstatt $\Pi_i(\vartheta)$ jede andere ganze Zahl α anwenden, wenn nur α zu $\varphi_i(\vartheta)$ relativ prim und durch alle Idealteiler von $p^{\varepsilon_j^{(i)} \cdot \varkappa_i}$ teilbar ist, welche zu $\varphi_i(\vartheta)$ relativ prim sind. Wenn daher wie in (30)

$$f(x) \equiv \pi_i(x) \,.\, \varphi_i(x)^{l_i} \pmod{p}$$

ist, wird die Zahl $\pi_i(\vartheta)$ zu $\varphi_i(\vartheta)$ relativ prim und durch alle Idealteiler von p teilbar, welche zu $\varphi_i(\vartheta)$ relativ prim sind. Mann kann daher die Zahl $\pi^i(\vartheta)^{\varepsilon_j^{(i)} \cdot \varkappa_i}$ als eine Zahl α anwenden und erhält für $\mathfrak{a}_j^{(i)}$ die Darstellung

$$\mathfrak{a}_j^{(i)} = \left(p, \varphi_i(\vartheta), \pi_i(\vartheta)^{\varepsilon_j^{(i)} \cdot \varkappa_i} \,.\, \psi_j^{(i)}(\vartheta, \theta_i(\vartheta))\right).$$

Es soll nun eine Zahl bestimmt werden, welche genau durch $\mathfrak{p}_j^{(i)}$ in der ersten Potenz teilbar ist. Aus der Primidealzerlegung von p folgt, dass man nach Satz 16 auch

$$\varphi_i(\vartheta) = \left(\mathfrak{p}_1^{(i)} \,.\, \mathfrak{p}_2^{(i)} \,.\, \ldots \,.\, \mathfrak{p}_{t_i}^{(i)}\right)^{\varkappa_i} \,.\, \Phi_i$$

hat, wo das Ideal Φ_i zu p relativ prim ist. Man kann nun immer zwei positive, ganze rationale Zahlen x_i und y_i derart bestimmen, dass

$$x_i \,.\, \varkappa_i - y_i \,.\, \lambda_i = 1$$

ist. Dann ist die Zahl

$$\pi_i(\vartheta)^{y_i} \,.\, \frac{\varphi_i(\vartheta)^{x_i}}{p^{y_i}}$$

eine ganze Zahl, welche genau durch $\mathfrak{p}_j^{(i)}$ in der ersten Potenz teilbar ist. Denn ein Primidealteiler von p, der nicht in $\varphi(\vartheta)$ aufgeht, wird sicher in $\pi_i(\vartheta)$ auf-

gehen. Ein Primidealteiler $\mathfrak{p}_j^{(i)}$ $(j = 1, 2, \ldots t_i)$ geht im Zähler genau in der Potenz $x_i \cdot \varkappa_i$ und im Nenner genau in der Potenz $x_i \cdot \varkappa_i$ auf, also in der Zahl überhaupt genau in der ersten Potenz. Daraus folgt, weil $\mathfrak{a}_j^{(i)}$ eine Potenz von $\mathfrak{p}_j^{(i)}$ ist, dass

$$\mathfrak{p}_j^{(i)} = \left(p,\ \varphi_i(\vartheta),\ \pi_i(\vartheta)^{y_i} \cdot \frac{\varphi_i(\vartheta)^{x_i}}{p^{y_i}},\ \pi_i(\vartheta)^{\varepsilon_j^{(i)} \cdot \varkappa_i} \cdot \psi_j(\vartheta, \theta_i(\vartheta))\right)$$

wird.

Man kann dann den folgenden Satz aussprechen:

Satz 21. Es sei

$$f(x) \equiv \varphi_1(x)^{l_1} \cdot \varphi_2(x)^{l_2} \ldots \varphi_s(x)^{l_s} \pmod{p}$$

und die Hauptpolygone $(p,\ \varphi_i(x))$ seien alle Geraden L_i mit den Neigungen $\frac{\varkappa_i}{\lambda_i}$. $f_1^{(i)}(x),\ f_2^{(i)}(x) \ldots f_{t_i}^{(i)}(x)$ seien die sämtlichen Primfunktionen von $f(x)$ $(\mathrm{mod}\ L_i)$; diese sollen alle verschieden vorausgesetzt werden und der Grad von $f_j^{(i)}(x)$ in $\varphi(x)^{\lambda_i}$ soll gleich $\varepsilon_j^{(i)}$ sein. Weiter soll

$$\pi_i(x) = \varphi_1(x)^{l_2} \ldots \varphi_{i-1}(x)^{l_{i-1}} \varphi_{i+1}^{l_i+1}(x) \ldots \varphi_s(x)^{l_s}$$

gesetzt werden. Dann ist

$$p = P_1 \cdot P_2 \ldots P_s,$$

wo das Ideal P_i die Primidealzerlegung

$$P_i = \left(\mathfrak{p}_1^{(i)}\, \mathfrak{p}_2^{(i)} \ldots \mathfrak{p}_{t_i}^{(i)}\right)^{\lambda_i}$$

hat. Das Primideal $\mathfrak{p}_j^{(i)}$ ist vom Grade $\varepsilon_j^{(i)} \cdot m_i$ und durch

$$\mathfrak{p}_j^{(i)} = \left(p,\ \varphi_i(\vartheta),\ \pi_i(\vartheta)^{y_i} \cdot \frac{\varphi_i(\vartheta)^{x_i}}{p^{y_i}},\ \pi_i(\vartheta)^{\varepsilon_j^{(i)} \cdot \varkappa_i} \cdot \frac{f_j(\vartheta)}{p^{\varepsilon_j^{(i)} \cdot \varkappa_i}}\right)$$

bestimmt, wo die positiven, ganzen rationalen Zahlen x_i und y_i durch $x_i \cdot \varkappa_i - y_i \cdot \lambda_i = 1$ bestimmt sind.

Durch diesen Satz ist allgemein der Fall erledigt, dass die Polygone Geraden sind. Man hätte natürlich diesen Satz aus den folgenden allgemeineren Sätzen ableiten können, aber ich habe hier den Satz besonders abgeleitet, weil er in so engem Zusammenhange mit den Dedekindschen Untersuchungen steht, und auch, um an diesem einfacheren Falle die folgenden Untersuchungen klarer zu machen.

Kap. 4. Willkürliche Polygone.

§ 1. Bezeichnungen und Hilfsgrössen.

Ich gehe jetzt dazu über, den allgemeinen Fall zu behandeln, dass alle Polygone $(p, \varphi(x))$ aus einer beliebigen Anzahl von Seiten bestehen. Es sei

$$f(x) \equiv \pi(x) \cdot \varphi(x)^l \pmod{p}, \tag{1}$$

und es sollen die gemeinsamen Idealteiler von p und $\varphi(\vartheta)$ untersucht werden. Für das Polygon S $(p, \varphi(x))$ sollen die Bezeichnungen des Kap. 2 angewandt werden. Die Neigungszahlen dieses Polygones sind dann

$$\frac{h_i}{l_i} = \frac{e_i \cdot \varkappa_i}{e_i \cdot \lambda_i} = \frac{\varkappa_i}{\lambda_i} \quad (i = 1, 2, \ldots k),$$

wo $\varkappa_i$ zu λ_i relativ prim ist und k die Anzahl der Seiten bedeutet. Hier ist

$$l_1 + l_2 + \cdots + l_k = l,$$

und für die Neigungszahlen hat man

$$\frac{\varkappa_1}{\lambda_1} < \frac{\varkappa_2}{\lambda_2} < \cdots < \frac{\varkappa_k}{\lambda_k}. \tag{2}$$

Es sollen nun die folgenden Bezeichnungen eingeführt werden:

$$f_i(x) = \varphi(x)^{l_i} + S_{i,1}(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{l_i - \lambda_i} + \cdots + S_{i,e_i}(x) \cdot p^{h_i} \quad (i = 1, 2, \ldots k) \tag{3}$$

sei der Faktor, welcher der i^{ten} Seite L_i in der Zerlegung von $f(x)$ (mod S) entspricht. Weiter sei

$$f_i(x) \equiv f_1^{(i)}(x)^{e_1^{(i)}} \cdot f_2^{(i)}(x)^{e_2^{(i)}} \cdots f_{t_i}^{(i)}(x)^{e_{t_i}^{(i)}} \pmod{L_i} \tag{4}$$

die Primfunktionzerlegung von $f_i(x)$ (mod L_i), wo

$$f_j^{(i)}(x) = \varphi(x)^{\varepsilon_j^{(i)} \cdot \lambda_i} + S_{j,1}^{(i)}(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{\left(\varepsilon_j^{(i)} - 1\right)\lambda_i} + \cdots + S_{j,\varepsilon_j^{(i)}}^{(i)}(x) \cdot p^{\varepsilon_j^{(i)} \cdot \varkappa_i} \tag{5}$$

ist und die Primfunktionen $f_j^{(i)}(x)$ alle verschieden sind. Weiter soll

$$F_i(x, y) = y^{e_i} + S_{i,1}(x) \cdot y^{e_i - 1} + \cdots + S_{i,e_i}(x) \tag{6}$$

gesetzt werden, und aus (4) folgt dann, dass man auch

$$F_i(x, y) \equiv \psi_1^{(i)}(x, y)^{e_1^{(i)}} \dots \psi_{t_i}^{(i)}(x, y)^{e_{t_i}^{(i)}} \pmod{p, \varphi(x)} \tag{7}$$

hat, wo

$$\psi_j^{(i)}(x, y) = y^{\varepsilon_j^{(i)}} + S_{j,1}(x) \cdot y^{\varepsilon_j^{(i)}-1} + \dots + S_{j,\varepsilon_j^{(i)}}^{(i)}(x) \tag{8}$$

ist.

Wird hier auch

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

eingeführt, dann leitet man aus (3) und (6) ab

$$\frac{f_i(x)}{p^{h_i}} = F_i(x, \theta_i(x)) = \theta_i(x)^{e_i} + S_{i,1}(x) \cdot \theta_i(x)^{e_i-1} + \dots + S_{i,e_i}(x)$$

und ebenso aus (5) und (8)

$$\frac{f_j^{(i)}(x)}{p^{\varepsilon_j^{(i)} \cdot \varkappa_i}} = \psi_j^{(i)}(x, \theta_i(x)) = \theta_i(x)^{\varepsilon_j^{(i)}} + S_{j,1}^{(i)}(x) \cdot \theta_i(x)^{\varepsilon_j^{(i)}-1} + \dots + S_{j,\varepsilon_j^{(i)}}^{(i)}(x).$$

Für die folgenden Untersuchungen sind nun verschiedene Hilfsgrössen wichtig, die hier bestimmt werden sollen. Nach (1) ist

$$\varphi(\vartheta)^l \cdot \pi(\vartheta) \equiv 0 \pmod{p},$$

und die Zahl $\pi(\vartheta)$ ist daher durch alle Idealteiler von p teilbar, welche zu $\varphi(\vartheta)$ relativ prim sind. Wenn aber $\mathfrak{p}$ ein gemeinsamer Primidealteiler von p und $\varphi(\vartheta)$ ist und p genau durch $\mathfrak{p}^s$, $\varphi(\vartheta)$ genau durch $\mathfrak{p}^t$ teilbar ist, so ist nach Satz 16

$$s \cdot \varkappa_i = t \cdot \lambda_i, \tag{9}$$

wo i eine der Zahlen $1, 2, \dots k$ ist. Wenn nun für $\mathfrak{p}$ die Gleichung (9) erfüllt ist, soll $\mathfrak{p}$ ein *Primideal der i^{ten} Seite des Polygones* $(p, \varphi(x))$ genannt werden.

Es soll jetzt gezeigt werden, dass die Zahlen

$$\pi(\vartheta)^{i \cdot \varkappa_1} \cdot \theta_1(\vartheta)^i = \pi(\vartheta)^{i \cdot \varkappa_1} \cdot \frac{\varphi(\vartheta)^{i \cdot \lambda_1}}{p^{i \cdot \varkappa_1}} \tag{10}$$

alle ganz sind. Dies folgt einfach indem man zeigt, dass alle Idealteiler des Nenners $p^{i \cdot \varkappa_1}$ auch im Zähler aufgehen. Nach der früheren Bemerkung geht ein

Primideal $\mathfrak{p}$, das gleichzeitig in p und $\pi(\vartheta)$ aufgeht, gewiss ebenso oft im Zähler wie im Nenner auf. Ist dagegen $\mathfrak{p}$ ein Primideal, das gleichzeitig in p und $\varphi(\vartheta)$ aufgeht und das zur ersten Seite gehört, wofür also

$$s \,.\, \varkappa_1 = t \,.\, \lambda_1$$

ist, dann wird ein solches Primideal genau so oft im Zähler wie im Nenner aufgehen, und wenn die Zahlen (10) ganz sind, können sie also nicht durch ein Primideal der ersten Seite teilbar sein. Ist zuletzt $\mathfrak{p}$ ein Primideal der i^{ten} Seite, $i \geqq 2$, so hat man nach (2)

$$t = s \cdot \frac{\varkappa_i}{\lambda_i} > s \cdot \frac{\varkappa_1}{\lambda_1}$$

oder

$$i \,.\, t \,.\, \lambda_1 > i \,.\, s \,.\, \varkappa_1 ,$$

d. h. $\mathfrak{p}$ geht im Zähler in einer höheren Potenz als im Nenner auf. Aus diesen Eigenschaften der Zahlen (10) leitet man einfach ab:

Die Zahlen

$$\pi(\vartheta)^{h_1+\varkappa_1+1} \,.\, \theta_1(\vartheta)^i \quad (i = 1, 2, \ldots e_1 + 1)$$

sind alle ganz und durch alle Primidealteiler von p teilbar ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zur ersten Seite gehören.

Daraus folgt weiter, dass die Zahl

$$\pi(\vartheta)^{h_1+\varkappa_1+1} \,.\, \frac{f_1(\vartheta)}{p^{h_1}} = \pi(\vartheta)^{h_1+\varkappa_1+1}(\theta_1(\vartheta)^{e_1} + S_{1,1}(\vartheta) \,.\, \theta_1(\vartheta)^{e_1-1} + \cdots + S_{1,e_1}(\vartheta)) \quad (11)$$

auch ganz ist, und nach Satz 17, dass diese Zahl durch alle Primidealteiler von p teilbar ist, welche in $\varphi(\vartheta)$ aufgehen und zur ersten Seite gehören. Wenn $\mathfrak{p}$ ein gemeinsames Primideal von p und $\varphi(\vartheta)$ ist, das zur i^{ten} Seite gehört, $i \geqq 2$, so kann diese Zahl (11) nicht durch ein solches Primideal teilbar sein, denn in (11) sind alle Glieder ausser dem letzten durch $\mathfrak{p}$ teilbar. Es ist daher bewiesen:

Die Zahl

$$T_1(\vartheta) = \pi(\vartheta)^{h_1+\varkappa_1+1} \,.\, \frac{f_1(\vartheta)}{p^{h_1}}$$

ist ganz und durch alle Primideale von p teilbar, welche nicht in $\varphi(\vartheta)$ aufgehen oder in $\varphi(\vartheta)$ aufgehen und zur ersten Seite gehören, aber durch keine anderen Primidealteiler von p.

Diese Untersuchungen sollen nun durch den folgenden Satz verallgemeinert werden:

Satz 22. Man kann eine solche Reihe von ganzen Zahlen des Körpers

$$T_0(\vartheta) = \pi(\vartheta),\ T_1(\vartheta),\ T_2(\vartheta), \ldots T_k(\vartheta)$$

von der Eigenschaft bestimmen, dass $T_i(\vartheta)$ durch alle Primideale von p teilbar ist ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zu den Seiten $S_{i+1}, S_{i+2}, \ldots S_k$ gehören.

Der Satz soll durch vollständige Induktion bewiesen werden, indem man beachtet, dass die Zahlen $T_0(\vartheta)$ und $T_1(\vartheta)$ von den gewünschten Eigenschaften schon bestimmt sind.

Es sei daher eine Zahl $T_{i-1}(\vartheta)$ derart bestimmt, dass sie erstens ganz und zweitens durch alle Primidealteiler von p, welche nicht in $\varphi(\vartheta)$ aufgehen, und durch alle Primidealteiler von $(p, \varphi(\vartheta))$, wofür

$$s \cdot \varkappa_j = t \cdot \lambda_j \quad (j = 1, 2, \ldots i-1),$$

aber durch keine anderen Primideale von p teilbar ist. Man kann dann die ganze rationale, positive Zahl x_{i-1} so bestimmen, dass die Zahlen

$$T_{i-1}(\vartheta)^{x_{i-1}} \cdot \theta_i(\vartheta)^u = T_{i-1}(\vartheta)^{x_{i-1}} \cdot \frac{\varphi(\vartheta)^{u \cdot \lambda_i}}{p^{u \cdot \varkappa_i}} \quad (u = 1, 2, \ldots e_i + 1) \tag{12}$$

alle ganz sind. Denn man kann x_{i-1} so gross wählen, dass alle Primideale, welche gleichzeitig in p und $T_{i-1}(\vartheta)$ aufgehen, in $T_{i-1}(\vartheta)^{x_{i-1}}$ in einer höheren Potenz als in $p^{u \cdot \varkappa_i}$ aufgehen. Ein Primideal, das in $\varphi(\vartheta)$ aufgeht und wofür $s \cdot \varkappa_i = t \cdot \lambda_i$ ist, geht genau ebenso oft im Zähler wie im Nenner auf, und wenn daher die Zahlen (12) ganz sind, können sie sicher nicht durch solche Primideale teilbar sein. Wenn zuletzt $\mathfrak{p}$ ein Primideal ist, das in $(p, \varphi(\vartheta))$ aufgeht und zur j^{ten} Seite gehört, $j > i$, so folgt aus (2)

$$t = s \cdot \frac{\varkappa_j}{\lambda_j} > s \cdot \frac{\varkappa_i}{\lambda_i}$$

oder

$$u \cdot t \cdot \lambda_i > s \cdot \varkappa_i \cdot u,$$

und $\mathfrak{p}$ geht daher im Zähler in einer höheren Potenz als im Nenner auf. Die Zahlen (12) sind also alle ganz und durch alle Primidealteiler von p teilbar, ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zur i^{ten} Seite gehören.

Daraus folgt, dass die Zahl

$$T_{i-1}(\vartheta)^{x_i-1} \cdot F_i(\vartheta, \theta_i(\vartheta)) = T_{i-1}(\vartheta)^{x_i-1}(\theta_i(\vartheta)^{e_i} + \\ + S_{i,1}(\vartheta) \cdot \theta_i(\vartheta)^{e_i-1} + \cdots + S_{i,e_i}(\vartheta)) \tag{13}$$

ganz sein muss, und diese Zahl ist durch alle Primideale von p teilbar, welche in $T_{i-1}(\vartheta)$ aufgehen, also solche, welche nicht in $\varphi(\vartheta)$ aufgehen oder in $\varphi(\vartheta)$ aufgehen und zu den Seiten $S_1, S_2, \ldots S_{i-1}$ gehören. Aus

$$F_i(\vartheta, \theta_i(\vartheta)) = \frac{f_i(\vartheta)}{p^{h_i}}$$

folgt nach Satz 17, dass die Zahl (13) auch durch solche Primideale teilbar wird, welche zur i^{ten} Seite gehören. Wenn zuletzt $\mathfrak{p}$ ein Primidealteiler von $(p, \varphi(\vartheta))$ ist, der zur j^{ten} Seite gehört, $j > i$, so geht dieser in allen Gliedern ausser dem letzten von (13) auf, und folglich ist diese Zahl nicht durch $\mathfrak{p}$ teilbar.

Man kann daher

$$T_i(\vartheta) = T_{i-1}(\vartheta)^{x_i-1} \cdot F_i(\vartheta, \theta_i(\vartheta))$$

setzen, womit der Beweis des Satzes 22 durchgeführt ist.

Aus dem Beweise sieht man auch die Richtigkeit des folgenden Satzes ein:

Satz 23. Die Zahlen

$$N_i(\vartheta) = T_{i-1}(\vartheta)^{x_i-1} \cdot \theta_i(\vartheta) \quad (i = 1, 2, \ldots k) \tag{14}$$

sind alle ganz, und $N_i(\vartheta)$ ist durch alle Primidealteiler von p teilbar ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zur i^{ten} Seite gehören.

Man kann leicht die Zahlen $T_i(\vartheta)$ explicite darstellen, denn es ist

$$T_0(\vartheta) = \pi(\vartheta),$$
$$T_1(\vartheta) = \pi(\vartheta)^{x_0} \cdot F_1(\vartheta, \theta_1(\vartheta)) \quad x_0 = h_1 + \varkappa_1 + 1,$$
$$T_2(\vartheta) = \pi(\vartheta)^{x_0 \cdot x_1} \cdot F_1(\vartheta, \theta_1(\vartheta))^{x_1} \cdot F_2(\vartheta, \theta_2(\vartheta)),$$

und daraus folgt im Allgemeinen

$$T_i(\vartheta) = \pi(\vartheta)^{x_0 \cdot x_1 \cdots x_i - 1} \cdot F_1(\vartheta, \theta_1(\vartheta))^{x_1 \cdots x_i - 1} F_2(\vartheta, \theta_2(\vartheta))^{x_2 \cdots x_i - 1} \ldots F_i(\vartheta, \theta_i(\vartheta)) \tag{15}$$

Dieser Formel zeigt, dass es eine solche Potenz p^a von p gibt, dass man, wenn man $T_i(x)$ mit p^a multipliziert, ein Polynom erhält, dessen Hauptpolygon

$(p, \varphi(x))$ aus i Seiten besteht, die zu den i ersten Seiten des Polygones S von $f(x)$ parallel sind, aber eine andere Länge besitzen. Aus (15) folgt, dass man

$$\alpha = x_1 \cdot x_2 \ldots x_{i-1} \cdot h_1 + x_2 \ldots x_{i-1} \cdot h_2 + \cdots + x_{i-1} \cdot h_{i-1} + h_i$$

setzen kann.

§ 2. Weitere Untersuchungen.

Es ist schon gezeigt worden, dass die Zahl

$$T_i(\vartheta) = T_{i-1}(\vartheta)^{x_i - 1} \cdot F_i(\vartheta, \theta_i(\vartheta)) = K_i(\vartheta) \cdot (\theta_i(\vartheta)^{e_i} + S_{i,1}(\vartheta) \cdot \theta_i(\vartheta)^{e_i - 1} + \cdots + S_{i,e_i}(\vartheta)), \quad (16)$$

wo

$$T_{i-1}(x)^{x_i - 1} = K_i(x), \quad (17)$$

ganz und durch alle Primideale von p teilbar ist, welche in $\pi(\vartheta)$ aufgehen oder in $\varphi(\vartheta)$ aufgehen und wofür gleichzeitig $s \cdot \varkappa_j = t \cdot \lambda_j$ ist, wo j eine der Zahlen $1, 2, \ldots i$ bedeutet. Ebenso folgt aus Satz 23, dass die Zahl

$$K_i(\vartheta) \cdot \theta_i(\vartheta)$$

ganz und durch alle Primidealteiler von p teilbar ist ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und wofür $s \cdot \varkappa_i = t \cdot \lambda_i$. Die Zahl

$$K_i(\vartheta)^2 \cdot \theta_i(\vartheta) \cdot F_i(\vartheta, \theta_i(\vartheta))$$

und folglich auch die Zahl

$$K_i(\vartheta) \cdot \theta_i(\vartheta) \cdot F_i(\vartheta, \theta_i(\vartheta)) \quad (18)$$

werden daher ebenfalls ganz und durch alle Primidealteiler von p teilbar. Hier ist zu bemerken, dass, wenn $i = k$ ist, schon die Zahl (16) durch alle Primidealteiler von p teilbar wird.

Von jetzt an soll vorausgesetzt werden, dass in (4) alle Exponenten $e_j^{(i)} = 1$ sind, also $f^{(i)}(x)$ für alle i nur verschiedene Primfaktoren (mod L_i) enthalten soll. Man hat dann

$$f_i(x) \equiv f_1^{(i)}(x) \cdot f_2^{(i)}(x) \ldots f_{t_i}^{(i)}(x) \pmod{L_i},$$

und durch Vergleichung der Gradzahlen erhält man die Relation

$$\lambda_i \cdot \sum_{j=1}^{t_i} \varepsilon_j^{(i)} = l_i \quad (19)$$

Es sollen nun alle Zahlen von der Form

$$K_i(\vartheta)\,.\,\theta_i(\vartheta)\,.\,A(\vartheta,\,\theta_i(\vartheta)) =$$

$$K_i(\vartheta)\,.\,\theta_i(\vartheta)\,(A_1(\vartheta)\,.\,\theta_i(\vartheta)^{e_i-1} + A_2(\vartheta)\,.\,\theta_i(\vartheta)^{e_i-2} + \cdots + A_{e_i}(\vartheta)) \quad (20)$$

untersucht werden, wo die Koeffizienten $A_i(\vartheta)$ Polynome in ϑ sind. Es wird hier $i \leqq k-1$ vorausgesetzt, der Fall $i = k$ soll später erwähnt werden.

Man soll nun erstens bestimmen, unter welchen Bedingungen eine Zahl von der Form (20) durch alle Primidealteiler von p teilbar sein kann. Aus § 1 folgt, dass eine Zahl (20) immer durch alle Primidealteiler von p teilbar sein muss ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zur i^{ten} Seite gehören.

Wenn in (20) alle Koeffizienten $A_i(x)$ (mod p) durch $\varphi(x)$ teilbar sind, also

$$A_1(x) \equiv A_2(x) \equiv \cdots \equiv A_{e_i}(x) \equiv 0 \ (\text{modd } p,\, \varphi(x)), \quad (21)$$

so ist diese Zahl sicher durch alle Primidealteiler von p teilbar. Man kann daher voraussetzen, dass in (20) der erste Koeffizient, der nicht durch $\varphi(x)$ (mod p) teilbar ist, gleich $A_{e_i-\varepsilon}(x)$ ist. Man kann dann ein Polynom $C(x)$ derart bestimmen, dass

$$C(x)\,.\,A_{e_i-\varepsilon}(x) \equiv 1 \ (\text{modd } p,\, \varphi(x)),$$

und wenn

$$C(x)\,.\,A_{e_i-\varepsilon+j}(x) \equiv B_i(x) \ (\text{modd } p,\, \varphi(x))$$

gesetzt wird, so folgt, dass auch die ganze Zahl

$$b = K_i(\vartheta)\,.\,\theta_i(\vartheta)\,.\,B(\vartheta,\,\theta_i(\vartheta)) = K_i(\vartheta)\,.\,\theta_i(\vartheta)\,(\theta_i(\vartheta)^{\varepsilon} + B_1(\vartheta)\,.\,\theta_i(\vartheta)^{\varepsilon-1} + \cdots + B_\varepsilon(\vartheta))$$

durch alle Primidealteiler von p teilbar sein muss. Hier kann offenbar auch

$$B_\varepsilon(x) \not\equiv 0 \ (\text{modd } p,\, \varphi(x))$$

vorausgesetzt werden.

Dabei bedeutet

$$B(x,\,y) = y^{\varepsilon} + B_1(x)\,.\,y^{\varepsilon-1} + \cdots + B_\varepsilon(x)\,.\,p^{\varepsilon\,.\,\varkappa_i},$$

und folglich ist

$$B'(x) = p^{\varepsilon\,.\,\lambda_i}\,.\,B(x,\,\theta_i(x)) = \varphi(x)^{\varepsilon\,.\,\lambda_i} + B_1(x)\,.\,p^{\varkappa_i}\,.\,\varphi(x)^{(\varepsilon-1)\,\lambda_i} + \cdots + B_\varepsilon(x)\,.\,p^{\varepsilon\,.\,\varkappa_i}$$

ein Polynom mit dem geradlinigen Polygone L_i $(p,\,\varphi(x))$. Möglicherweise könnte $B(x,\,y)$ sich auf die Einheit reduzieren, indem es dann keine Primideale der i^{ten} Seite gäbe.

Man kann jetzt immer eine solche Potenz p^β bestimmen, dass

$$p^\beta \,.\, K_i(x) \,.\, B(x, \theta_i(x)) = C(x) \tag{22}$$

ein Polynom wird mit einem Hauptpolygone $(p, \varphi(x))$, das aus i Seiten besteht, welche zu den i ersten Seiten des Polygones S von $f(x)$ $(p, \varphi(x))$ parallel sind. A priori ist es jedoch möglich, dass in $C(x)$ die i^{te} Seite fehlt.

Man bildet nun die Gleichung

$$b^n + e_1 \,.\, b^{n-1} + \cdots + e_n = 0,$$

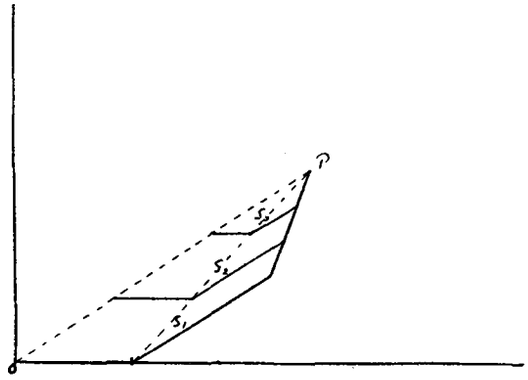

Fig. 3.

welcher die Zahl b genügt, und hier sind nach Satz 18 alle Koeffizienten e_i durch p teilbar. Diese Gleichung zeigt, dass eine Identität

$$K_i(x)^n \,.\, \theta_i(x)^n \,.\, B(x, \theta_i(x))^n + \\ + e_1 \,.\, K_i(x)^{n-1} \,.\, \theta_i(x)^{n-1} \,.\, B(x, \theta_i(x))^{n-1} + \cdots + e_n = f(x) \,.\, g(x)$$

besteht. Wenn diese Identität mit $p^{n\cdot\beta + n\cdot\varkappa_i}$ multipliziert wird, folgt nach (22)

$$C(x)^n \,.\, \varphi(x)^{\lambda_i \cdot n} + e_1 \,.\, C(x)^{n-1} \,.\, \varphi(x)^{\lambda_i(n-1)} \,.\, p^{\beta+\varkappa_i} + \cdots + e_n \,.\, p^{n(\beta+\varkappa_i)} = f(x) \,.\, g_1(x), \tag{23}$$

wo beide Seiten ganzzahlig sind. Das Hauptpolygon $(p, \varphi(x))$ der linken Seite von (23) soll jetzt bestimmt werden. Zu diesem Zwecke beachte man, dass die Polynome

$$C(x)^n,\ p^\beta \,.\, C(x)^{n-1},\ \ldots\ p^{(n-1)\beta} \,.\, C(x),\ p^{n\cdot\beta} \tag{24}$$

alle Polygone besitzen, die einander ähnlich sind, und nach (22) bestehen diese Polygone aus i Seiten, welche zu den i ersten Seiten des Hauptpolygones von

$f(x)$ parallel sind. Dazu kommt noch eine Seite, die zu der X-Achse parallel ist. Wenn man diese Polygone aufzeichnet, werden sie etwa so liegen, wie es in Fig. 3 abgebildet worden ist, wo das Ähnlichkeitszentrum der repräsentierende Punkt von $p^{n\cdot\beta}$ ist.

Nun kommen aber in (23) nicht die Polynome (24) vor, sondern die Glieder

$$C(x)^n \cdot \varphi(x)^{\lambda_i \cdot n},$$

$$p^{\beta+\varkappa_i} \cdot C(x)^{n-1} \cdot \varphi(x)^{\lambda_i(n-1)}, \ldots p^{(n-1)(\beta+\varkappa_i)} \cdot C(x) \cdot \varphi(x)^{\lambda_i},\ p^{n(\beta+\varkappa_i)}. \qquad (25)$$

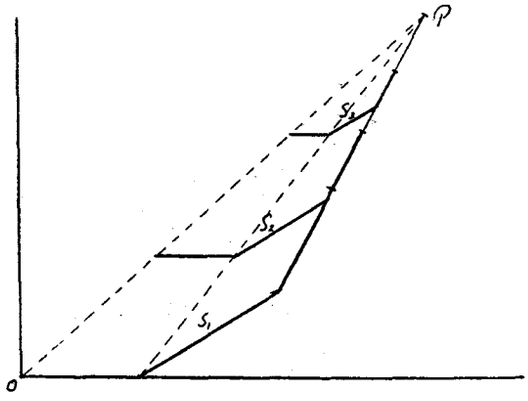

Fig. 4.

Die Lage der Polygone dieser Polynome erhält man aber leicht aus den Polygonen von (24) und aus Fig. 3, indem man beachtet, dass, wenn ein Glied mit $\varphi(x)^\alpha$ multipliziert wird, dies eine Verschiebung der repräsentierenden Punkte parallel der X-Achse nach links um eine Strecke α bedeutet. Ebenso bedeutet die Multiplikation mit p^γ eine Verschiebung parallel der Y-Achse um eine Strecke γ nach oben. Wenn daher $(t, n\beta)$ die Koordinaten des Ähnlichkeitszentrums in Fig. 3, also des gemeinsamen Endpunktes der Polygone von den Polynomen (24) sind, so wird der Endpunkt des Polygones von einem der Polynome (25)

$$p^{s(\beta+\varkappa_i)} \cdot C(x)^{n-s} \cdot \varphi(x)^{\lambda_i(n-s)}$$

in den Punkt P fallen, der die Koordinaten

$$(t + \lambda_i \cdot s,\ n\beta + s \cdot \varkappa_i))$$

besitzt, also auf eine Gerade von der Neigung $\frac{\varkappa_i}{\lambda_i}$, welche durch den Punkt $(t, n \cdot \beta)$

geht. Die Polygone von den Polynomen (25) müssen also wie in Fig. 4 liegen, wo das Ähnlichkeitszentrum die Koordinaten

$$(t + \lambda_i \,.\, n,\ n(\beta + \varkappa_i))$$

hat.

Man sieht daraus, dass ein Polynom, das aus einer Summe von den mit gewissen Zahlenkoeffizienten versehenen Gliedern (25) besteht, ein Hauptpolygon $(p, \varphi(x))$ besitzen wird, das erstens aus den i Seiten von $C(x)^n$ besteht und dann für den Rest entweder mit der Geraden von der Neigung $\frac{\varkappa_i}{\lambda_i}$ von dem Endpunkte dieses Polygones bis zum Punkte P ganz oder teilweise zusammenfällt oder oberhalb dieser Geraden fällt.

In diesem Falle, wo das Polygon der linken Seite von (23) bestimmt werden soll, sind aber alle Koeffizienten e_i durch p teilbar, und daraus folgt leicht, dass das Polygon $(p, \varphi(x))$ der linken Seite von (23) aus den i Seiten von $C(x)^n$ bestehen muss und dazu noch einigen Seiten, die gewiss von grösseren Neigungen sind. Weiter sieht man ein, dass von den Gliedern in (23) nur $C(x)^n$ solche Glieder in der Entwickelung $(p, \varphi(x))$ liefern kann, welche auf den i ersten Seiten dieses Polygones liegen. Durch diese Bemerkung folgt nach (22), dass der Faktor, welcher der i^{ten} Seite entspricht, gleich $B'(x)^n$ sein muss.

Da die rechte Seite von (23) $f(x)$ als Faktor enthält, muss diese Seite ein Polygon besitzen, worin das Polygon S von $f(x)$ in der Weise eingehen muss, dass jede Seite von S darin vorkommt. Es muss folglich auch in dem Polygone für die linke Seite von (23) eine Seite von der Neigung $\frac{\varkappa_i}{\lambda_i}$ vorkommen. Da weiter $f_i(x)$ ein Faktor der i^{ten} Seite in dem Polygone rechts ist, so folgt dass $B'(x)^n$ (mod L_i) durch $f_i(x)$ teilbar sein muss.

Da aber $f_i(x)$ nach den Voraussetzungen nur verschiedene Primfaktoren (mod L_i) besitzt, folgt, dass auch $B'(x)$ (mod L_i) durch $f_i(x)$ teilbar sein muss. Nun ist aber $f_i(x)$ von einem höheren Grade als $B'(x)$, und $B'(x)$ kann daher nicht (mod L_i) durch $f_i(x)$ teilbar sein.

Durch diesen Widerspruch ist bewiesen, *dass eine Zahl von der Form* (20) *nicht durch alle Primidealteiler von p teilbar sein kann, ausser wenn* (21) *erfüllt ist.*

Bei diesen Untersuchungen ist $i \leq k-1$ vorausgesetzt worden. Wenn $i = k$ ist, wird schon die Zahl

$$K_k(\vartheta) \,.\, F_k(\vartheta, \theta_k(\vartheta)) = K_k(\vartheta) \,.\, (\theta_k(\beta)^{e_k} + S_{k,1}(\vartheta) \,.\, \theta_k^{e_k-1} + \cdots + S_{k,e_k}(\vartheta))$$

durch alle Primidealteiler von p teilbar, und man untersucht in diesem Falle ganz analog, wann eine Zahl von der Form

$$K_k(\vartheta) \,.\, A(\vartheta, \theta_k(\vartheta)) = K_k(\vartheta)\,(A_1(\vartheta) \,.\, \theta_k(\vartheta)^{e_k-1} + \cdots + A_{e_k}(\vartheta)) \qquad (26)$$

durch alle Primidealteiler von p teilbar sein kann. Wenn eine Zahl (26) durch alle Primidealteiler von p teilbar ist, wird es wie früher möglich, eine Zahl von der Form

$$b = K_k(\vartheta)\,(B(\vartheta, \theta_k(\vartheta)) = K_k(\vartheta)\,(\theta_k(\vartheta)^{\varepsilon} + B_1(\vartheta) \,.\, \theta_k(\vartheta)^{\varepsilon-1} + \cdots + B_\varepsilon(\vartheta))$$

derart zu bestimmen, dass auch b durch alle Primidealteiler von p teilbar ist. Weiter kann man hier immer einen solchen Exponenten α von p bestimmen, dass

$$p^\alpha \,.\, K_k(x) \,.\, B(x, \theta_k(x)) = K'_k(x) \,.\, B'(x)$$

ein Polynom mit einem Hauptpolygone $(p, \varphi(x))$ wird, das aus k Seiten besteht, die zu den Seiten des Polygones $(p, \varphi(x))$ von $f(x)$ parallel sind, und der Faktor, welcher der k^{ten} Seite dieses Polygones entspricht, gleich $B'(x)$ wird.

Man bildet wie früher die Gleichung

$$b^n + e_1 \,.\, b^{n-1} + \cdots + e_n = 0,$$

welcher b genügt und wo alle Koeffizienten nach Satz 18 durch p teilbar werden. Daraus folgt weiter das Bestehen einer Identität

$$K'_k(x)^n \,.\, B'(x)^n + e_1 \,.\, p^\alpha \,.\, K'_k(x)^{n-1} \,.\, B'(x)^{n-1} + \cdots + e_n \,.\, p^{n\cdot\alpha} = f(x) \,.\, g(x). \qquad (27)$$

Die Polygone der Glieder

$$K'(x)^n \,.\, B'(x)^n,\ K'_k(x)^{n-1} \,.\, B'(x)^{n-1} \,.\, p^\alpha,\ \ldots\ K'_k(x) \,.\, B'(x) \,.\, p^{(n-1)\alpha},\ p^{n\cdot\alpha}$$

liegen alle so, wie es in Fig. 3 abgebildet worden ist, und daraus folgt leicht, dass die linke Seite von (27) ein Polygon besitzt, das mit dem Polygone von $K'_k(x)^n \,.\, B'(x)^n$ identisch ist, und dass alle anderen Polynome $e_i \,.\, p^{i\cdot\alpha} \,.\, K'_k(x)^{n-i} \,.\, B'(x)^{n-i}$ nur solche Glieder liefern können, welche oberhalb dieses Polygones liegen. Daraus folgt wie früher, dass $B'(x)^n \pmod{L_k}$ durch $f_k(x)$ und daher auch $B'(x) \pmod{L_k}$ durch $f_k(x)$ teilbar sein muss. Dies ist aber offenbar nicht möglich, und daraus folgt, dass eine Zahl von der Form (26) nur durch alle Primidealteiler von p teilbar sein kann, wenn

$$A_1(x) \equiv A_2(x) \equiv \cdots \equiv A_{e_k}(x) \equiv 0 \ (\text{modd } p, \varphi(x)).$$

§ 3. Die Primidealzerlegung von p.

Es folgt nun sofort aus § 2, dass es für jede Seite Primideale gibt. Denn wäre für eine Seite L_i, $i<k$, dies nicht der Fall, so müsste schon die Zahl

$$K_i(\vartheta)\,.\,\theta_i(\vartheta)$$

durch alle Primidealteiler von p teilbar sein, was nicht möglich ist. Wenn $i=k$ ist, würde schon die Zahl $K_k(\vartheta)$ durch alle Primidealteiler von p teilbar sein, was auch nicht möglich ist.

Um eine einheitliche Darstellung der folgenden Untersuchungen zu erhalten, soll die Bezeichnung

$$\left.\begin{aligned} K_i(\vartheta)\,.\,\theta_i(\vartheta) &= M_i(\vartheta) \quad (i=1,2,\dots k-1)\\ K_k(\vartheta) \qquad\quad &= M_k(\vartheta) \end{aligned}\right\} \tag{28}$$

eingeführt werden. Die ganze Zahl $M_i(\vartheta)$ ist dann nach § 1 durch alle Primideale von p teilbar ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zur i^{ten} Seite gehören.

Man kann daher die Resultate des § 2 folgendermassen zusammenfassen: *Eine Zahl*

$$M_i(\vartheta)\,.\,A(\vartheta,\theta_i(\vartheta)) = M_i(\vartheta)(A_1(\vartheta)\,.\,\theta_i(\vartheta)^{e_i-1}+\cdots+A_{e_i}(\vartheta)) \tag{29}$$

kann nur dann durch alle Primidealteiler von p teilbar sein, wenn

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

Es sollen nun die Primideale der i^{ten} Seite untersucht werden. Die ganze Zahl

$$M_i(\vartheta)\,.\,\psi_j^{(i)}(\vartheta,\theta_i(\vartheta)) \quad (j=1,2,\dots t_i) \tag{30}$$

muss für alle j durch ein Primideal der i^{ten} Seite teilbar sein, denn wäre dies nicht der Fall, müsste schon, da $M_i(\vartheta)\,.\,F_i(\vartheta,\theta_i(\vartheta))$ durch alle Primideale der i^{ten} Seite teilbar ist,

$$M_i(\vartheta)^{t_i-1}\,.\,\psi_1^{(i)}\dots\psi_{j-1}^{(i)}\,.\,\psi_{j+1}^{(i)}\dots\psi_{t_i}^{(i)}$$

$$[\psi_j^{(i)}=\psi_j^{(i)}(\vartheta,\theta_i(\vartheta))]$$

durch alle Primideale der i^{ten} Seite und folglich auch

$$M_i(\vartheta) \cdot \psi_1^{(i)} \ldots \psi_{j-1}^{(i)} \cdot \psi_{j+1}^{(i)} \ldots \psi_{t_i}^{(i)}$$

durch alle Primidealteiler von p teilbar sein, was nicht möglich ist.

Weiter können zwei von den Zahlen (30) nicht durch dasselbe Primideal der i^{ten} Seite teilbar sein, denn man kann immer solche Funktionen $C(x, y)$ und $D(x, y)$ bestimmen, dass

$$\psi_{j_1}^{(i)}(x, y) \cdot C(x, y) + \psi_{j_2}^{(i)}(x, y) \cdot D(x, y) \equiv 1 \pmod{p, \varphi(x)}$$

ist, und wenn diese Kongruenz mit $M_i(\vartheta)^2$ multipliziert und $x = \vartheta$, $y = \theta_i(\vartheta)$ gesetzt wird, folgt, dass auch $M_i(\vartheta)^2$ durch einen gemeinsamen Primidealteiler der i^{ten} Seite teilbar sein muss, was aber nach den Eigenschaften von $M_i(\vartheta)$ nicht möglich ist. Es gibt daher sicher mindestens t_i verschiedene Primideale der i^{ten} Seite.

Sei nun $\mathfrak{p}_j^{(i)}$ ein Primideal der i^{ten} Seite, das in einer Zahl (30) aufgeht. Wenn dann eine Zahl von der Form (29) durch $\mathfrak{p}_j^{(i)}$ teilbar sein soll, so muss $A(x, y) \pmod{p, \varphi(x)}$ durch $\psi_j^{(i)}(x, y)$ teilbar sein. Denn wäre dies nicht der Fall, könnte man solche Funktionen $C(x, y)$ und $D(x, y)$ bestimmen, dass

$$\psi_j^{(i)}(x, y) \cdot C(x, y) + A(x, y) \cdot D(x, y) \equiv 1 \pmod{p, \varphi(x)},$$

und durch Multiplikation mit $M_i(\vartheta)^2$ würde wie früher folgen, wenn $x = \vartheta$, $y = \theta_i(\vartheta)$ gesetzt wird, dass $M_i(\vartheta)$ durch $\mathfrak{p}_j^{(i)}$ teilbar wäre, was nicht möglich ist.

Aus dieser Bemerkung folgt, dass es unter den Zahlen (29) mindestens $p^{\varepsilon_j^{(i)} \cdot m}$ inkongruente Zahlen für den Modul $\mathfrak{p}_j^{(i)}$ gibt, und daher ist der Grad $f_j^{(i)}$ von $\mathfrak{p}_j^{(i)}$ sicher nicht kleiner als $\varepsilon_j^{(i)} \cdot m$. Indem man berücksichtigt, dass nach § 5. III $f_j^{(i)}$ immer durch m teilbar sein muss, kann man daher

$$f_j^{(i)} = (\varepsilon_j^{(i)} + \alpha_j^{(i)}) \cdot m$$

setzen, wo $\alpha_j^{(i)} \geq 0$ ist. Es soll gezeigt werden, dass in der Tat $\alpha_j^{(i)} = 0$ ist.

Das Primideal $\mathfrak{p}_j^{(i)}$ geht nach Satz 16 mindestens in einer Potenz λ_i in p auf, und daher ist gewiss $\mathfrak{p}_j^{(i)\lambda_i}$ ein Teiler von p. Das Ideal

$$P_i = \left(\mathfrak{p}_1^{(i)} \cdot \mathfrak{p}_2^{(i)} \ldots \mathfrak{p}_{t_i}^{(i)}\right)^{\lambda_i}$$

ist daher auch ein Teiler von p und enthält nur Primideale der i^{ten} Seite. Man hat hier

$$NP_i = p^{\lambda_i \sum_{j=1}^{t_i} f_j^{(i)}},$$

und setzt man

$$f_i = \lambda_i \sum_{j=1}^{t_i} f_j^{(i)} = m \,.\, \lambda_i \,.\, \sum_{j=1}^{t_i} (\varepsilon_j^{(i)} + \alpha_j^{(i)}),$$

so ergibt sich nach (19)

$$f_i = m \,.\, l_i + m \,.\, \sum_{j=1}^{t_i} \alpha_j^{(i)} = m \,.\, l_i + \beta_i.$$

Daher ist also

$$NP_i = p^{f_i},$$

wo $f_i \geqq m \,.\, l_i$, und es kann nur dann $f_i = m \,.\, l_i$ sein, wenn alle $\alpha_j^{(i)}$ verschwinden.

Für alle Seiten des Polygones $(p, \varphi(x))$ von $f(x)$ kann man nun entsprechende Idealfaktoren P_i von p bestimmen, und es wird dann auch

$$P = P_1 \,.\, P_2 \ldots P_k$$

ein Teiler von p und nach § 4. III auch ein Teiler des Ideals $\mathfrak{a} = (p, \varphi(\vartheta)^l)$. Hier wird

$$NP = p^{\Sigma f_i},$$

und da

$$\Sigma f_i = \Sigma m \,.\, l_i + \Sigma \beta_i = m \,.\, l + \Sigma \beta_i,$$

kann man

$$NP = p^{m \,.\, l + \beta},$$

setzen, wo $\beta \geqq 0$ ist.

Diese Untersuchungen beziehen sich alle auf die Bestimmung der gemeinsamen Primfaktoren von p und $\varphi(\vartheta)$. Wenn aber die Voraussetzung gilt, dass für alle Primfunktionenentwickelungen $(p, \varphi_s(x))$ von $f(x)$ die Faktoren in der Zerlegung für das Polygon $(p, \varphi_s(x))$ verschieden sind, so kann man für alle diese Primfunktionen $\varphi_s(x)$ die ähnlichen Untersuchungen über die Primideale vornehmen, und man erhält in dieser Weise für alle Primfunktionen $\varphi_s(x)$ die entsprechenden Ideale P, die alle zu einander relativ prim sind und auch alle in p aufgehen. Nennt man daher p' das Produkt dieser Ideale P, so ist p' auch ein Idealteiler von p. Es ist aber

$$Np' = p^{\Sigma(ml + \beta)},$$

wo die Summe über die Werte für alle verschiedenen Primfunktionen $\varphi_s(x)$ auszudehnen ist. Da aber

$$\Sigma(ml+\beta) = n + \Sigma\beta$$

und $Np = p^n$, folgt, dass $\Sigma\beta = 0$ sein muss, und es wird $p = p'$, wodurch also die Primidealzerlegung von p vollständig bestimmt ist.

Aus der Bedingung $\Sigma\beta = 0$ folgt, dass auch alle β verschwinden müssen, und da $\beta = \Sigma\beta_i$ war, wo alle β_i positiv oder Null waren, so müssen auch alle $\beta_i = 0$ sein, und folglich $f_i = m \cdot l_i$. Dies war aber nur dann möglich, wenn alle $\alpha_j^{(i)}$ verschwinden. Daher ist also

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

Man kann diese Resultate in dem folgenden Hauptsatze zusammenfassen:

Satz 24. Sei

$$f(x) \equiv \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \ldots \varphi_s(x)^{e_s} \pmod{p}$$

die Primfunktionzerlegung von $f(x)$. Dann ist

$$p = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \ldots \mathfrak{a}_s,$$

wo

$$\mathfrak{a}_t = (p, \varphi_t(\vartheta)^{e_t}).$$

Um die Primidealzerlegung eines Ideals

$$\mathfrak{a} = (p, \varphi(\vartheta)^e)$$

zu bestimmen, konstruiert man das Newtonsche Polygon $(p, \varphi(x))$ von $f(x)$ und bestimmt die Primfunktionen

$$f_1^{(i)}(x),\ f_2^{(i)}(x), \ldots f_{t_i}^{(i)}(x) \qquad (i = 1, 2, \ldots k)$$

für alle Seiten L_i des Polygones. Wenn bei dieser Zerlegung für die Seiten nur verschiedene Primfaktoren vorkommen und dies für alle Primfunktionen $\varphi(x)$ gilt, so ist

$$\mathfrak{a} = (\mathfrak{p}_1^{(1)} \cdot \mathfrak{p}_2^{(1)} \ldots \mathfrak{p}_{t_1}^{(1)})^{\lambda_1} \cdot (\mathfrak{p}_1^{(2)} \ldots \mathfrak{p}_{t_2}^{(2)})^{\lambda_2} \ldots (\mathfrak{p}_1^{(k)} \ldots \mathfrak{p}_{t_k}^{(k)})^{\lambda_k}.$$

Hier ist das Primideal $\mathfrak{p}_j^{(i)}$ vom Grade $\varepsilon_j^{(i)} \cdot m$, wenn $\varepsilon_j^{(i)} \cdot m$ den Grad von $f_j^{(i)}(x)$ bedeutet.

Es bleibt nun nur übrig, die Primideale $\mathfrak{p}_j^{(i)}$ zu bestimmen.

§ 4. Bestimmung der Primideale.

Um ein Primideal $\mathfrak{p}_j^{(i)}$ als grösste gemeinsame Faktor von Hauptidealen zu bestimmen, beachte man, dass $\mathfrak{p}_j^{(i)}$ immer in

$$M_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta)) \tag{31}$$

aufgeht. Diese Zahl kann aber durch keine anderen Primideale der i^{ten} Seite teilbar sein, denn sonst würde man nach der Schlussweise in § 3 folgern können, dass $Np > p^n$ wäre. Daher ist (31) durch eine Potenz von $\mathfrak{p}_j^{(i)}$ und übrigens durch keine anderen Primideale der i^{ten} Seite teilbar.

Wenn $i = k$ ist, hat man nach (28)

$$M_k(\vartheta) \cdot \psi_j^{(k)}(\vartheta, \theta_k(\vartheta)) = K_k(\vartheta) \cdot \psi_j^{(k)}(\vartheta, \theta_k(\vartheta)).$$

Wenn aber $i < k$ ist, wird

$$M_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta)) = K_i(\vartheta) \cdot \theta_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta)),$$

und nach der Definition der Zahl $K_i(\vartheta)$ (17) ist auch die Zahl

$$K_i(\vartheta)^2 \cdot \theta_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta))$$

durch keine anderen Primideale der i^{ten} Seite als $\mathfrak{p}_j^{(i)}$ teilbar. Aus Satz 25 folgt aber, dass

$$N_i(\vartheta) = K_i(\vartheta) \cdot \theta_i(\vartheta)$$

nicht durch $\mathfrak{p}_j^{(i)}$ teilbar sein kann, und folglich ist also für alle i

$$K_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta))$$

durch $\mathfrak{p}_j^{(i)}$, aber durch keine anderen Primideale der i^{ten} Seite teilbar. Diese Zahl kann weiter nur durch solche Primideale von $(p, \varphi(\vartheta))$ teilbar sein, welche zu den $i-1$ ersten Seiten gehören. Denn in der Summe

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

sind alle Glieder ausser dem letzten nach Satz 23 durch alle Primideale der Seiten $L_{i+1}, \ldots L_k$ teilbar.

Daraus sieht man leicht ein, dass das Ideal

$$I = [p, \varphi(\vartheta), N_1(\vartheta), \ldots, N_{i-1}(\vartheta), K_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta))]$$

eine Potenz von $\mathfrak{p}_j^{(i)}$ ist. Denn ein Primideal $\mathfrak{p}_j^{(s)}$ geht nicht in $K_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta))$ auf, wenn $s > i$ ist, wenn aber $s < i$ ist, geht dieses Ideal nicht in der Zahl $N_s(\vartheta)$ auf, wie aus dem Satze 23 folgt. Das Ideal $\mathfrak{p}_j^{(i)}$ geht dagegen in allen Zahlen des Ideals auf, während kein anderes Primideal der i^{ten} Seite diese Eigenschaft besitzt.

Es kommt jetzt nur darauf an, eine Zahl so zu bestimmen, dass sie durch $\mathfrak{p}_j^{(i)}$ genau in der ersten Potenz teilbar ist.

Wenn die Primidealzerlegung von p durch Satz 24 gegeben ist, folgt aus Satz 16, dass man auch

$$\varphi(\vartheta) = (\mathfrak{p}_1^{(i)} \cdot \mathfrak{p}_2^{(i)} \ldots \mathfrak{p}_{t_i}^{(i)})^{\varkappa_i} \cdot \Phi_i \qquad (i = 1, 2, \ldots k) \tag{32}$$

hat, wo das Ideal Φ_i durch kein Primideal der i^{ten} Seite teilbar ist. Man kann nun, da $\varkappa_i$ zu λ_i relativ prim ist, zwei ganze, rationale positive Zahlen z_i und y_i derart bestimmen, dass

$$z_i \cdot \varkappa_i - y_i \cdot \lambda_i = 1, \tag{33}$$

wo $y_i < \varkappa_i$ vorausgesetzt werden kann. Die Zahl

$$T_{i-1}(\vartheta)^{\varkappa_i - 1} \cdot \frac{\varphi(\vartheta)^{z_i}}{p^{y_i}} \tag{34}$$

ist dann ganz und durch $\mathfrak{p}_j^{(i)}$ genau in der ersten Potenz teilbar. Denn alle Primideale von p, welche nicht in $\varphi(\vartheta)$ aufgehen oder in $\varphi(\vartheta)$ aufgehen und zu den Seiten $L_1, L_2, \ldots L_{i-1}$ gehören, gehen in $T_{i-1}(\vartheta)^{\varkappa_i - 1}$ in einer höheren Potenz als in p^{y_i} auf. Ein Primideal der i^{ten} Seite geht im Nenner in der Potenz $y_i \cdot \lambda_i$, im Zähler nach (32) in der Potenz $z_i \cdot \varkappa_i$ auf, folglich nach (33) im Zähler genau ein Mal mehr als im Nenner. Ein Primideal der s^{ten} Seite, $s > i$, geht im Nenner in der Potenz $y_i \cdot \lambda_s$, im Zähler in der Potenz $z_i \cdot \varkappa_s$ auf, und es ist nach (2) und (33)

$$z_i \cdot \varkappa_s - y_i \cdot \lambda_s = \left(\frac{\varkappa_s}{\lambda_s} - \frac{y_i}{z_i}\right) z_i \cdot \lambda_s > \left(\frac{\varkappa_i}{\lambda_i} - \frac{y_i}{z_i}\right) z_i \cdot \lambda_s = \frac{\lambda_s}{\lambda_i}$$

und folglich

$$z_i \cdot \varkappa_s > y_i \cdot \lambda_s .$$

Die Zahl (34) ist also ganz und durch alle Primideale der i^{ten} Seite genau in der ersten Potenz teilbar.

Aus den Eigenschaften des Ideals I folgt nun leicht die Richtigkeit des Satzes:

Satz 25. Sei $N_1, N_2, \ldots N_k$ eine Reihe von Zahlen des Körpers, welche den Bedingungen des Satzes 23 genügen, d. h.

$$N_s = T_{s-1}(\vartheta)^{x_s-1} \cdot \theta_s(\vartheta) = K_s(\vartheta) \cdot \theta_s(\vartheta),$$

wo also

$$\theta_s(\vartheta) = \frac{\varphi(\vartheta)^{\lambda_s}}{p^{\varkappa_s}}$$

$$K_s(\vartheta) = T_{s-1}(\vartheta)^{x_s-1}.$$

Dann sind die Primideale $\mathfrak{p}_j^{(i)}$ des Satzes 24 durch

$$\mathfrak{p}_j^{(i)} = \left(p, \varphi(\vartheta), N_1, N_2, \ldots N_{i-1}, K_i(\vartheta) \cdot \frac{\varphi(\vartheta)^{z_i}}{p^{y_i}}, K_i(\vartheta) \cdot \frac{f_j^{(i)}(\vartheta)}{p^{\varepsilon_j^{(i)} \cdot \varkappa_i}}\right)$$

bestimmt, wo die positiven, ganzen rationalen Zahlen y_i und z_i durch

$$z_i \cdot \varkappa_i - y_i \cdot \lambda_i = 1, \quad y_i < \varkappa_i$$

verbunden sind.

In dieser Darstellung des Ideals kommen noch die Zahlen

$$T_s(\vartheta) = T_{s-1}(\vartheta)^{x_s-1} \cdot F_s(\vartheta, \theta_s(\vartheta))$$

vor, worin die noch unbestimmten Grössen x_s auftreten. Durch Satz 25 wird allgemein die Darstellung von $\mathfrak{p}_j^{(i)}$ gegeben, wenn nur vorausgesetzt wird, dass N_s durch alle Primideale von p teilbar ist ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zur s^{ten} Seite gehören. In der Bestimmung der Zahlen $T_s(\vartheta)$, § 1, war es aber notwendig die Zahl x_{s-1} so gross zu wählen, dass die Zahl

$$T_{s-1}(\vartheta)^{x_s-1} \cdot \theta_s(\vartheta)^{e_s+1} = T_{s-1}(\vartheta)^{x_s-1} \cdot \frac{\varphi(\vartheta)^{\lambda_s(e_s+1)}}{p^{\varkappa_s(e_s+1)}}$$

ganz und durch alle Primidealteiler von p ausser den Primidealen der i^{ten} Seite teilbar wurde, weil dies in den späteren Untersuchungen angewandt werden sollte. Es ist aber klar, dass man, um eine Reihe von Zahlen zu erhalten, welche den Satz 22 erfüllen, nur x_{s-1} so gross zu wählen braucht, dass

$$T_{s-1}(\vartheta)^{x_{s-1}} \cdot \frac{\varphi(\vartheta)^{e_s \cdot \lambda_s}}{p^{e_s \cdot x_s}} = T_{s-1}(\vartheta)^{x_{s-1}} \cdot \theta_s(\vartheta)^{e_s} \tag{35}$$

ganz und durch alle Primidealteiler von p ausser den Primidealen der i^{ten} Seite teilbar wird. Denn dann wird auch die Zahl

$$T_{s-1}(\vartheta)^{x_{s-1}} \cdot F_s(\vartheta, \theta_s(\vartheta)) = T_{s-1}(\vartheta)^{x_{s-1}} (\theta_s(\vartheta)^{e_s} + S_{s,1}(\vartheta) \cdot \theta_s(\vartheta)^{e_s-1} + \cdots + S_{s,e_s}(\vartheta))$$

ganz und kann folglich gleich $T_s(\vartheta)$ gesetzt werden, weil darin alle Primideale von p aufgehen ausser solchen, welche in $\varphi(\vartheta)$ aufgehen und zu den Seiten $L_{s+1}, \ldots L_k$ gehören.

Aus (35) folgt dann, dass ein Primideal der r^{ten} Seite im Nenner in einer Potenz $e_s \cdot x_s \cdot \lambda_r$ aufgeht, und es genügt daher sicher, wenn man $x_{s-1} > h_s \cdot \lambda$ wählt, wo λ die grösste der Zahlen $\lambda_1, \lambda_2, \ldots \lambda_{s-1}$ bedeutet. Dadurch wird es also immer möglich, die Zahlen $T_i(\vartheta)$ zu bestimmen. Für die Anwendungen ist es oft zweckmässig, die Exponenten x_s einzeln zu bestimmen, nachdem nach Satz 24 die Primidealzerlegung von p und dadurch auch von $\varphi(\vartheta)$ bestimmt ist und folglich ausgerechnet werden kann, in welchen Potenzen die Primideale im Nenner und Zähler von (35) aufgehen.

Wenn für eine Primzahl die Bedingungen des Satzes 24 erfüllt sind, rechnet man auch leicht eine untere Grenze für die Potenz der Primzahl p aus, in welcher sie in der Körperdiskriminante d aufgeht. Ein Primideal $\mathfrak{p}_j^{(i)}$ geht nämlich nach DEDEKIND[1], wenn λ_i nicht durch p teilbar ist, genau in der Potenz $\mathfrak{p}_j^{(i)\lambda_i - 1}$ in der Körperdifferente $\mathfrak{d}$ auf. Wenn aber λ_i durch p teilbar ist, geht dieses Ideal mindestens in der Potenz $\mathfrak{p}_j^{(i)\lambda_i}$ in $\mathfrak{d}$ auf.

Da nun

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

ist, wird d mindestens durch $p^{\varepsilon_j^{(i)} \cdot m(\lambda_i - 1)}$ teilbar, und da diese Überlegungen für alle Primideale der i^{ten} Seite richtig sind, so wird d auch durch

$$p^{m(\lambda_i - 1) \sum_{j=1}^{t_i} \varepsilon_j^{(i)}} = p^{m(\lambda_i - 1) e_i} = p^{m \cdot l_i - m \cdot e_i}$$

teilbar. Wenn man zuletzt die Primideale aller Seiten beachtet, folgt weiter, dass d durch

[1] DEDEKIND, (B): Über die Discriminanten endlicher Körper, Göttinger Abh. 1882. § 13.

$$\mathfrak{p}_i = \left(p, \varphi(\vartheta), N_1, \ldots N_{i-1}, K_i(\vartheta) \cdot \frac{\varphi(\vartheta)^{y_i}}{p^{z_i}}, N_{i+1}, \ldots, N_k\right)$$

bestimmt. Denn in diesem Ideale gehen nach Satz 23 nur Primideale der i^{ten} Seite auf, und $\mathfrak{p}_i$ geht in $K_i(\vartheta) \cdot \frac{\varphi(\vartheta)^{y_i}}{p^{z_i}}$ genau in der ersten Potenz auf, wenn $y_i \,.\, x_i - z_i \,.\, \lambda_i = 1$ ist. Dieser Fall trifft z. B. immer ein, wenn h_i zu l_i relativ prim ist.

Es sollen nun einige Zahlenbeispiele für die früheren Untersuchungen gegeben werden. Ich wähle als erstes das bekannte Beispiel von Dedekind, wo zum

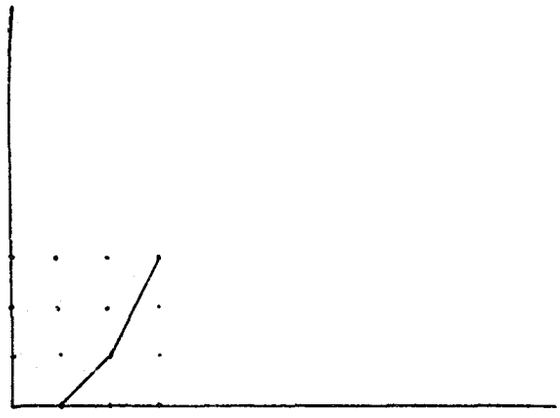

Fig. 5.

ersten Male die Existenz eines gemeinsamen, ausserwesentlichen Diskriminantenteilers eines Körpers nachgewiesen wurde.[1]

Es sei ϑ eine Wurzel der Gleichung

$$f(x) = x^3 - x^2 - 2x - 8 = 0.$$

Diese Gleichung ist irreduzibel, da sie keine rationale Wurzel besitzt, und wie eine einfache Rechnung zeigt, ist ihre Diskriminante gleich $-2^2 \,.\, 503$. Folglich kann nur die Primzahl 2 ein Indexteiler sein. Man hat nun

$$f(x) \equiv (x+1)x^2 \pmod 2,$$

und das Polygon von $f(x)(2, x)$ hat, wie man sofort sieht, die in Fig. 5. wiedergegebene Form. Daraus folgt aber, dass

$$2 = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$$

[1] Dedekind A. § 5.

das Produkt von 3 verschiedenen Primidealen ersten Grades sein muss, wo $\mathfrak{p}_1$ in $\vartheta+1$, $\mathfrak{p}_2$ und $\mathfrak{p}_3$ in ϑ aufgehen. Dies zeigt auch, dass 2 ein gemeinsamer, ausserwesentlicher Diskriminantenteiler des Körpers sein muss, weil es (mod 2) nur zwei verschiedene Primfunktionen ersten Grades gibt, nämlich x und $x+1$.[1]

Nach der ersten Bemerkung dieses Paragraphen kann man hier

$$\mathfrak{p}_1 = (2, \vartheta + 1)$$

setzen. Um die Ideale $\mathfrak{p}_2$ und $\mathfrak{p}_3$ zu bestimmen, beachte man, dass hier $\lambda_1 = \lambda_2 = 1$, $\varkappa_1 = 1$, $\varkappa_2 = 2$ und daher die Zahl

$$N = (\vartheta + 1) \cdot \frac{\vartheta}{2}$$

ganz und durch $\mathfrak{p}_3$ aber nicht durch $\mathfrak{p}_2$ teilbar ist. Weiter ist $x+2$ der Faktor der ersten Seite, und folglich

$$F = (\vartheta + 1) \cdot \frac{\vartheta + 2}{2}$$

ganz und durch $\mathfrak{p}_2$ aber nicht durch $\mathfrak{p}_3$ teilbar. Daher kann man

$$\mathfrak{p}_2 = \left(2, \vartheta, \frac{(\vartheta+1)(\vartheta+2)}{2}\right)$$

$$\mathfrak{p}_3 = \left(2, \vartheta, \frac{\vartheta(\vartheta+1)}{2}\right)$$

setzen. Durch eine einfache Rechnung überzeugt man sich, dass

$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 = (2, \vartheta),$$

und daraus wieder, dass wirklich

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 = (2)$$

ist.

Als ein anderes Beispiel soll der Körper $P(\vartheta)$ gewählt werden, der durch

$$f(\vartheta) = \vartheta^3 - 8\vartheta + 4 = 0$$

bestimmt ist. Die Diskriminante dieser Gleichung ist $2^4 : 101$, und folglich kann nur die Primzahl 2 ein Indexteiler sein. Das Polygon $(2, x)$ ist eine Gerade, wofür $\lambda = 3$, $\varkappa = 2$ ist. Dies zeigt erstens, dass $f(x)$ irreduzibel ist, und zweitens, dass

$$2 = \mathfrak{p}^3$$

[1] Dedekind A. § 4.

sein muss, wo das Primideal $\mathfrak{p}$ vom ersten Grade ist. Um $\mathfrak{p}$ zu bestimmen, beachte man, dass

$$\vartheta = \mathfrak{p}^2 \cdot \Theta$$

sein muss, wo Θ nicht durch $\mathfrak{p}$ teilbar ist. Die Zahl $\frac{\vartheta^2}{2}$ ist dann durch $\mathfrak{p}$ in genau der ersten Potenz teilbar, weil $2 \cdot \varkappa - 1 \cdot \lambda = 1$ ist. Man kann daher

$$\mathfrak{p} = \left(2, \frac{\vartheta^2}{2}\right)$$

setzen. In diesem Falle kann aber ϑ durch kein anderes Primideal als $\mathfrak{p}$ teilbar sein, was aus

$$4 = 8\vartheta - \vartheta^3$$

folgt, und daher ist

$$\mathfrak{p} = \left(\frac{\vartheta^2}{2}\right)$$

ein Hauptideal.

§ 6. Gemeinsame ausserwesentliche Diskriminantenteiler eines Körpers.

Mit Hilfe des Satzes 24 kann man nun in allen Fällen die folgende Aufgabe lösen:

Es seien die ganzen rationalen, positiven Zahlen

$$m_1, m_2, \ldots m_r$$

$$l_1, l_2, \ldots l_r$$

so gegeben, dass

$$m_1 \cdot l_1 + m_2 \cdot l_2 + \cdots + m_r \cdot l_r = n \tag{36}$$

ist. Man soll einen algebraischen Körper $P(\vartheta)$ n^{ten} Grades so bestimmen, dass eine beliebig gegebene Primzahl p die Zerlegung

$$p = \mathfrak{p}_1^{l_1} \cdot \mathfrak{p}_2^{l_2} \ldots \mathfrak{p}_r^{l_r}$$

besitzt, wo das Primideal $\mathfrak{p}_i$ vom Grade m_i ist.

Die Summe (36) kann in der Form

$$m^{(1)} \cdot (l_1^{(1)} + l_2^{(1)} + \cdots + l_{r_1}^{(1)}) + m^{(2)}(l_1^{(2)} + \cdots + l_{r_2}^{(2)}) + \cdots + m^{(s)}(l_1^{(s)} + \cdots + l_{r_s}^{(s)}) \tag{37}$$

geschrieben werden, wo die Zahlen $m^{(i)}$ alle von einander verschieden sind. Setzt man dann

$$l_1^{(i)} + l_2^{(i)} + \cdots + l_{r_i}^{(i)} = L^i,$$

so ist also

$$m^{(1)} \cdot L_1 + m^{(2)} \cdot L_2 + \cdots + m^{(s)} \cdot L_s = n.$$

Da es bekanntlich für einen Primzahlmodul p für alle Grade m Primfunktionen gibt, kann man eine Reihe von Primfunktionen (mod p)

$$\varphi_1(x), \varphi_2(x), \ldots \varphi_s(x)$$

aufstellen, wo $\varphi_i(x)$ vom Grade $m^{(i)}$ in x ist. Weiter bestimmt man zu den Zahlen

$$l_1^{(i)}, l_2^{(i)}, \ldots l_{r_i}^{(i)} \tag{38}$$

eine andere Reihe von Zahlen

$$h_1^{(i)}, h_2^{(i)}, \ldots h_{r_i}^{(i)} \tag{39}$$

derart, dass $h_j^{(i)}$ zu $l_j^{(i)}$ relativ prim ist, und

$$\frac{h_1^{(i)}}{l_1^{(i)}} < \frac{h_2^{(i)}}{l_2^{(i)}} < \cdots < \frac{h_{r_i}^{(i)}}{l_{r_i}^{(i)}}.$$

Es ist dann möglich, ein Polygon S_i zu konstruieren, wo die Projektionen auf die Y-Achse gleich den Zahlen (39) sind, während die Projektionen auf die X-Achse gleich den Zahlen (38) sind, also die Projektion des ganzen Polygones auf die X-Achse gleich L_i ist. Man bestimmt nun, was auf unendlich viele Weisen geschehen kann, ein Polynom $F_i(x)$ so, dass

$$F_i(x) \equiv \varphi_i(x)^{L_i}$$

und das Polygon $(p. \varphi_i(x))$ gleich S_i wird.

Setzt man nun

$$h_1^{(i)} + h_2^{(i)} + \cdots + h_{r_i}^{(i)} = H_i$$

und ist h eine ganze Zahl grösser als alle H_i, so werden in dem Polynome vom n^{ten} Grade

$$f(x) = F_1(x) \cdot F_2(x) \ldots F_s(x) + p^h \cdot M(x)$$

die Hauptpolygone $(p, \varphi_i(x))$ gleich den Polygonen S_i. Dabei bedeutet $M(x)$ ein beliebiges Polynom von höchstens $(n-1)^{\text{tem}}$ Grade. Wenn daher nur nach-

gewiesen wäre, dass man $M(x)$ so wählen könnte, dass $f(x)$ irreduzibel wäre, würde man nach Satz 24 die gestellte Aufgabe schon gelöst haben.

Sei daher

$$F_1(x) \cdot F_2(x) \ldots F_s(x) = x^n + a_1 \cdot x^{n-1} + \cdots + a_n$$

und

$$M(x) = b_1 \cdot x^{n-1} + b_2 \cdot x^{n-2} + \cdots + b_n,$$

so wird

$$f(x) = x^n + (a_1 + p^h \cdot b_1) x^{n-1} + (a_2 + p^h \cdot b_2) x^{n-2} + \cdots + a_n + p^h \cdot b_n,$$

wo die b_i nach Belieben gewählt werden können. Wenn nun q eine beliebige von p verschiedene Primzahl bedeutet, so kann man immer die Zahlen b_i derart bestimmen, dass

$$a_i + p^h \cdot b_i \equiv 0 \pmod{q} \quad (i = 1, 2, \ldots n),$$

aber

$$a_n + p^h \cdot b_n \not\equiv 0 \pmod{q^2}.$$

Wenn die Zahlen b_i auf diese Weise gewählt werden, ist also $f(x)$ nach dem Satze von Eisenstein irreduzibel, und daher die vorliegende Aufgabe gelöst. Es ist auch klar, dass sich durch diese Methode unendlich viele verschiedene Körper der gewünschten Art aufstellen lassen.

Auf Grund dieser Untersuchung kann man verschiedene wichtige Resultate über die Existenz der gemeinsamen, ausserwesentlichen Diskriminantenteiler ableiten.

Nach (37) bedeutet r_i die Anzahl der verschiedenen Primideale von p, welche vom Grade $m^{(i)}$ sind. Man kann nun in jedem einzelnen Falle entscheiden, ob diese Primzahl ein gemeinsamer, ausserwesentlicher Teiler der Gattungsdiskriminante ist oder nicht, indem man nach DEDEKIND[1] das folgende einfache Kriterium anwendet:

Damit eine Primzahl $p = \mathfrak{p}_1^{l_1} \cdot \mathfrak{p}_2^{l_2} \ldots \mathfrak{p}_r^{l_r}$, *wo das Primideal* $\mathfrak{p}_i$ *vom Grade* m_i *ist, ein gemeinsamer, ausserwesentlicher Diskriminantenteiler sei, ist notwendig und hinreichend, dass von den Ungleichheiten*

$$r_i > n(m^{(i)}) \qquad (i = 1, 2, \ldots s) \tag{40}$$

wenigstens eine erfüllt ist. Dabei bedeutet $n(m^{(i)})$ *die Anzahl der Primfunktionen (mod* p*) vom Grade* $m^{(i)}$.

[1] DEDEKIND A. § 4.

Wenn $m = a^{\alpha} . b^{\beta} \ldots$ die Primzahlzerlegung einer Zahl m ist, hat man bekanntlich

$$n(m) = \frac{1}{m}\left(p^m - \sum p^{\frac{m}{a}} + \sum p^{\frac{m}{ab}} - \ldots\right).$$

Da weiter immer $p \leqq \frac{n(n-1)}{2}$ sein muss, wenn p ein gemeinsamer, ausserwesentlicher Diskriminantenteiler ist, ist man im Stande, für ein gegebenes n alle Primzahlen p zu berechnen, welche in einem Körper n^{ten} Grades gemeinsame, ausserwesentliche Teiler sein können. Mittels (40) kann man nun auch für ein gegebenes p dieser Art alle verschiedene Wertesysteme

$$\left.\begin{matrix} m_1, m_2, \ldots m_r \\ l_1, l_2, \ldots l_r \end{matrix}\right\} \tag{41}$$

bestimmen, wofür

$$p = \mathfrak{p}_1^{l_1} . \mathfrak{p}_2^{l_2} \ldots \mathfrak{p}_r^{l_r}, \; N\mathfrak{p}_i = p^{m_i} \tag{42}$$

ein gemeinsamer, ausserwesentlicher Teiler in einem Körper sein muss, wo p diese Zerlegung in Primideale besitzt. Aus der Lösung der Aufgabe dieses Paragraphen folgt nun immer wirklich die Existenz solcher Körper:

Für jedes System (41) *und jede Primzahl* p, *wofür eine der Ungleichheiten* (40) *erfüllt ist, lassen sich, und zwar auf unendlich viele Weisen, solche Körper* n^{ten} *Grades bestimmen, dass* p *ein gemeinsamer, ausserwesentlicher Diskriminantenteiler mit der Primidealzerlegung* (42) *wird.*

Speziell folgt daraus: Wenn $p < n$ und $n \geqq 3$ ist, so gibt es nur p Primfunktionen ersten Grades (mod p). Wenn daher $p = \mathfrak{p}_1 . \mathfrak{p}_2 \ldots \mathfrak{p}_n$ sein soll, muss p ein gemeinsamer, ausserwesentlicher Teiler sein. Wenn $n \geqq 3$, gibt es also für jeden Grad unendlich viele Körper, worin gemeinsame, ausserwesentliche Diskriminantenteiler vorkommen.

§ 7. Behandlung der Ausnahmefälle.

In dem Satze 24 ist vorausgesetzt worden, dass $f(x)$ für alle Seiten der Polygone $(p, \varphi(x))$ in verschiedene Primfunktionen zerfallen soll. Nun ist es aber allgemein möglich, dass für gewisse Indexteiler auch mehrfache Primfunktionen für einige der Seiten vorkommen. Diesen allgemeinsten Fall werde ich jetzt behandeln.

Es sei also die Primfunktionzerlegung von $f_i(x)$ (mod L_i) durch (4) gegeben. Man untersucht dann wie früher, wann eine Zahl von der Form (20), $i \leqq k-1$, durch alle Primidealteiler von p teilbar sein kann. Wenn (20) durch alle Primidealteiler von p teilbar ist, dann ist es möglich auch eine Zahl b von der Form

$$b = K_i(\vartheta) \cdot \theta_i(\vartheta) \cdot (\theta_i(\vartheta)^\varepsilon + B_1(\vartheta) \cdot \theta_i(\vartheta)^{\varepsilon-1} + \cdots + B_\varepsilon(\vartheta)) \quad \varepsilon < e_i$$

so zu bestimmen, dass auch b durch alle Primideale von p teilbar ist. Hier soll wie früher

$$B(x, y) = y^\varepsilon + B_1(x) \cdot y^{\varepsilon-1} + \cdots + B_\varepsilon(x)$$

und

$$B'(x) = p^{\varepsilon \cdot \varkappa_i} \cdot B(x, \theta_i(x)) = \varphi(x)^{\varepsilon \cdot \lambda_i} + B_1(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{(\varepsilon-1)\lambda_i} + \cdots + B_\varepsilon(x) \cdot p^{\varepsilon \cdot \varkappa_i}$$

gesetzt werden.

Man bildet nun die Gleichung, welcher b genügt und wo alle Koeffizienten nach Satz 18 durch p teilbar sind. Durch dieselbe Schlussweise wie in § 2 folgt daraus, dass $B'(x)^n$ (mod L_i) durch $f_i(x)$ teilbar sein muss. Daraus kann man aber jetzt nicht mehr schliessen, dass $B'(x)$ (mod L_i) durch $f_i(x)$ teilbar sein muss, sondern nur, dass $B'(x)$ (mod L_i) durch das Produkt aller verschiedenen Primfunktionen von $f_i(x)$ (mod L_i), also durch

$$f_1^{(i)}(x) \cdot f_2^{(i)}(x) \ldots f_{t_i}^{(i)}(x)$$

teilbar ist. Folglich muss $B(x, y)$ und daher auch $A(x, y)$ (modd $p, \varphi(x)$) durch

$$\psi_1^{(i)}(x, y) \cdot \psi_2^{(i)}(x, y) \ldots \psi_{t_i}^{(i)}(x, y)$$

teilbar sein.

Für $i = k$ untersucht man die Zahlen (26), und es folgt hier in derselben Weise, dass auch eine solche Zahl nicht durch alle Primidealteiler von p teilbar sein kann, ausser wenn $A(x, y)$ (modd $p, \varphi(x)$) durch

$$\psi_1^{(k)}(x, y) \cdot \psi_2^{(k)}(x, y) \ldots \psi_{t_k}^{(k)}(x, y)$$

teilbar ist. Mit den Bezeichnungen (28) kann man diese Resultate folgendermassen zusammenfassen:

Eine Zahl

$$M_i(\vartheta) \cdot A(\vartheta, \theta_i(\vartheta)) = M_i(\vartheta)(A_1(\vartheta) \cdot \theta_i(\vartheta)^{e_i-1} + \cdots + A_{e_i}(\vartheta)) \tag{43}$$

kann nur dann durch alle Primideale von p teilbar sein, wenn $A(x, y)$ (modd $p, \varphi(x)$) durch das Produkt

$$f_1^{(i)}(x, y) \cdot f_2^{(i)}(x, y) \dots f_{t_i}^{(i)}(x, y)$$

teilbar ist.

Aus dieser Bemerkung folgt sofort, dass es für jede Seite Primideale gibt. Denn wenn es für die i^{te} Seite keine Primideale gäbe, so wäre schon $M_i(\vartheta)$ durch alle Primideale von p teilbar, was ja nicht möglich ist. Daher kann man mit Hilfe des Satzes 16 den folgenden Satz aussprechen:

Satz 26. Es sei $\varphi(x)$ eine Primfunktion, welche (mod p) in $f(x)$ aufgeht, und p ein Primideal, das gleichzeitig in p und $\varphi(\vartheta)$ aufgeht. Wenn dann p genau durch $\mathfrak{p}^s$, $\varphi(\vartheta)$ genau durch $\mathfrak{p}^t$ teilbar ist, so hat man

$$\frac{t}{s} = \frac{\varkappa_i}{\lambda_i}, \tag{44}$$

wo $\frac{\varkappa_i}{\lambda_i}$ eine der Neigungszahlen des Polygones $(p, \varphi(x))$ von $f(x)$ ist. Umgekehrt gibt es aber auch für alle Neigungszahlen des Polygones solche Primideale von $(p, \varphi(\vartheta))$, dass die Exponenten die Gleichung (44) erfüllen.

Ganz analog wie in § 2 folgt nun, dass die Zahl $M_i(\vartheta) \cdot F_i(\vartheta, \theta_i(\vartheta))$ und daher auch die Zahl

$$M_i(\vartheta) \cdot f_1^{(i)}(\vartheta)^{e_1^{(i)}} \dots f_{t_i}^{(i)}(\vartheta)^{e_{t_i}^{(i)}}$$

durch alle Primideale von p teilbar ist. Dadurch beweist man aber, dass die Zahlen $M_i(\vartheta) \cdot f_j^{(i)}(\vartheta)$ sicher alle durch mindestens ein Primideal der i^{ten} Seite teilbar sein müssen. Denn wäre dies nicht der Fall, müsste schon

$$M_i(\vartheta)^{t_i - 1} \cdot f_1^{(i)}(\vartheta)^{e_1^{(i)}} \dots f_{j-1}^{(i)}(\vartheta)^{e_{j-1}^{(i)}} \cdot f_{j+1}^{(i)}(\vartheta)^{e_{j+1}^{(i)}} \dots f_{t_i}^{(i)}(\vartheta)^{e_{t_i}^{(i)}}$$

und daher auch

$$M_i(\vartheta) \cdot f_1^{(i)}(\vartheta)^{e_1^{(i)}} \dots f_{j-1}^{(i)}(\vartheta)^{e_{j-1}^{(i)}} \cdot f_{j+1}^{(i)}(\vartheta)^{e_{j+1}^{(i)}} \dots f_{t_i}^{(i)}(\vartheta)^{e_{t_i}^{(i)}}$$

durch alle Idealteiler von p teilbar sein, was jedoch nach dem Bewiesenen unmöglich ist.

Weiter folgt, dass zwei Zahlen

$$M_i(\vartheta) \cdot f_{j_1}^{(i)}(\vartheta), \quad M_i(\vartheta) \cdot f_{j_2}^{(i)}(\vartheta)$$

nicht durch dieselben Primideale der i^{ten} Seite teilbar sein können. Denn man kann immer zwei solche Funktionen $A(x, y)$ und $B(x, y)$ bestimmen, dass

$$A(x, y) \cdot f_{j_1}^{(i)}(x, y) + B(x, y) \cdot f_{j_2}^{(i)}(x, y) \equiv 1 \pmod{p, \varphi(x)},$$

und wenn diese Kongruenz mit $M_i(\vartheta)^2$ multipliziert und $x = \vartheta$, $y = \theta_i(\vartheta)$ gesetzt wird, so folgt, dass auch $M_i(\vartheta)$ durch ein gemeinsames Primideal der i^{ten} Seite teilbar sein muss, was nach den Eigenschaften von $M_i(\vartheta)$ nicht möglich ist.

Aus diesen Bemerkungen folgert man, indem man sich erinnert, dass ein Primideal der i^{ten} Seite immer in p in einer Potenz aufgeht, die ein Multiplum von λ_i ist:

Satz 27. Sei

$$f(x) \equiv \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \ldots \varphi_s(x)^{e_s} \pmod{p}$$

die Primfunktionzerlegung von $f(x)$. Dann ist

$$p = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \ldots \mathfrak{a}_s,$$

wo die Ideale $\mathfrak{a}_t$ zu einander relativ prim sind und $\mathfrak{a}_t = (p, \varphi_t(\vartheta)^{e_t})$. Um ein Ideal $\mathfrak{a} = (p, \varphi(\vartheta)^e)$ weiter zu zerlegen, konstruiert man das Newtonsche Polygon $(p, \varphi(x))$ von $f(x)$ und bestimmt die Primfunktionzerlegung

$$f_i(x) \equiv f_1^{(i)}(x)^{e_1^{(i)}} \ldots f_{t_i}^{(i)}(x)^{e_{t_i}^{(i)}} \pmod{L_i}$$

für jede Seite des Polygones. Dann ist

$$\mathfrak{a} = (\mathfrak{a}_1^{(1)} \cdot \mathfrak{a}_2^{(1)} \ldots \mathfrak{a}_{t_1}^{(1)})^{\lambda_1} \ldots \left(\mathfrak{a}_1^{(k)} \ldots \mathfrak{a}_{t_k}^{(k)}\right)^{\lambda_k},$$

wo die Ideale $\mathfrak{a}_j^{(i)}$ alle zu einander relativ prim sind.

Man findet auch leicht, dass ein Ideal $\mathfrak{a}_j^{(i)}$ durch

$$\mathfrak{a}_j^{(i)} = \left(p, \varphi(\vartheta), N_1, \ldots N_{i-1}, K_i(\vartheta) \cdot \frac{\varphi(\vartheta)^{z_i}}{p^{y_i}}, K_i(\vartheta) \cdot \frac{f_j^{(i)}(\vartheta)^{e_j^{(i)}}}{p^{\varepsilon_j^{(i)} \cdot e_j^{(i)} \cdot \varkappa_i}}\right)$$

bestimmt ist.

Die Ideale des Satzes 27 brauchen also nicht Primideale zu sein. Man kann aber verschiedene Eigenschaften der Primideale ableiten, welche in $\mathfrak{a}_j^{(i)}$ aufgehen. Denn sei $\mathfrak{p}_j^{(i)}$ ein Primideal, das in $\mathfrak{a}_j^{(i)}$ und folglich auch in $M_i(\vartheta) \cdot \psi_j^{(i)}(\vartheta, \theta_i(\vartheta))$ aufgeht, dann kann eine Zahl von der Form (43) nicht durch $\mathfrak{p}_j^{(i)}$ teilbar sein,

ausser wenn $A(x, y)$ (modd $p, \varphi(x)$) durch $\psi_j^{(i)}(x, y)$ teilbar ist. Denn wäre dies nicht der Fall, so könnte man solche Funktionen $C(x, y)$ und $D(x, y)$ finden, dass

$$C(x, y) \cdot \psi_j^{(i)}(x, y) + D(x, y) \cdot A(x, y) \equiv 1 \text{ (modd } p, \varphi(x))$$

und folglich, wenn diese Kongruenz mit $M_i(\vartheta)^2$ multipliziert und $x = \vartheta, y = \theta_i(\vartheta)$ gesetzt würde, $M_i(\vartheta)^2$ durch $\mathfrak{p}_j^{(i)}$ teilbar wäre.

Daher folgt, dass der Grad von $\mathfrak{p}_j^{(i)}$ nicht kleiner als $\varepsilon_j^{(i)} \cdot m$ sein kann, und man kann sogar mit Hilfe des Satzes 8 beweisen, dass der Grad von $\mathfrak{p}_j^{(i)}$ immer durch $\varepsilon_j^{(i)} \cdot m$ teilbar sein muss.

Ich will in diesem Zusammenhange noch eine andere Bemerkung machen, die ganz einfach aus Satz 27 folgt. Durch den Satz 15 ist ein Kriterium gegeben, wann eine Primzahl in der Körperdiskriminante, aber nicht in dem Index aufgeht. Man kann nun auch fragen: Wann geht p in dem Index, aber nicht in der Körperdiskriminante auf? Da p in diesem Falle nur verschiedene Primidealteiler haben kann, folgt aus Satz 27:

Wenn p in dem Index, aber nicht in der Körperdiskriminante aufgehen soll, muss man

$$\lambda_1 = \lambda_2 = \cdots = \lambda_k = 1$$

haben, d. h. alle Neigungszahlen der Polygone müssen ganz sein.

Wenn dann für keine Primfunktionen und keine Seiten mehrfache Faktoren auftreten, so ist auch p wirklich ein Teiler des Index, aber kein Teiler der Körperdiskriminante. Wenn aber mehrfache Primfunktionen für die Seiten auftreten, bleibt die Frage noch unentschieden.

§ 8. Polygone höherer Stufen.

Durch den Satz 27 und folgende Bemerkungen ist man zu einem ganz analogen Verhältniss gekommen, wie früher durch die Untersuchungen des § 5. III, nur mit dem Unterschiede, dass man jetzt auf einer höheren Stufe steht, indem es sich da um die Zerlegung der Ideale $\mathfrak{a} = (p, \varphi(\vartheta)^e)$ handelte, die durch den Satz 27 in die Ideale $\mathfrak{a}_j^{(i)}$ zerlegt wurden, während jetzt eine weitere Zerlegung der Ideale $\mathfrak{a}_j^{(i)}$ bestimmt werden soll.

Dies geschieht nun in einer ganz analogen Weise. Ich werde mich aber der Einfachheit wegen auf einen speziellen Fall beschränken, nämlich den, dass das Polygon $(p, \varphi(x))$ eine Gerade ist. Durch die Verhältnisse in diesem Falle ge-

winnt man aber, ebenso wie früher, eine Übersicht über die Verhältnisse im allgemeinsten Falle.

Wie in § 7, III sei

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

das Polygon $(p, \varphi(x))$ eine Gerade L und

$$f(x) \equiv f_1(x)^{e_1} \dots f_s(x)^{e_s} \pmod{L}.$$

Man bildet nun eine Entwickelung $(L, f_i(x))$ ebenso wie früher die Entwickelung $(p, \varphi(x))$ von $f(x)$

$$f(x) = \sum_s Q_s(x) \cdot f_i(x)^s, \tag{45}$$

wo die $Q_s(x)$ Polynome von höchstens $(\varepsilon_i \cdot m - 1)^{\text{tem}}$ Grade in x sind. Wenn man hier ein jedes Glied $Q_s(x) \cdot f_i(x)^s$ ausrechnet, wird man nur solche Glieder in der Entwickelung $(p, \varphi(x))$ von $f(x)$ erhalten, welche durch Punkte auf oder oberhalb L abgebildet werden. Man zeichnet nun die mit L parallelen Geraden $L_1, L_2, \dots$ und untersucht wie in § 6, II, zu welcher von diesen Geraden das Polynom $Q_s(x) \cdot f_i(x)^s$ gehört. Nimmt man allgemein an, dass dieses Polynom zur Geraden L_{a_s} gehört, so repräsentiert man das Polynom in einem Koordinatensystem durch den Punkt (s, a_s). Zu jedem Gliede in der Entwickelung (45) gibt es dann einen Punkt, zu diesen Gitterpunkten konstruiert man ein Newtonsches Polygon, und dadurch kann man in analoger Weise die Idealzerlegungen der Ideale $\mathfrak{a}_j^{(i)}$ bestimmen. Wenn man durch die Ideale dieses Polygones nicht zu der Primidealzerlegung von p gelangt, muss man in gleicher Weise die Polygone der dritten Stufe konstruieren usw. Man sieht ein, dass eine gewisse Analogie zwischen der Primidealzerlegung und der Bestimmung der Reihenentwickelung einer algebraischen Funktion in der Umgebung einer singulären Stelle besteht.

Ich gehe auf die Beweise dieser Sätze nicht ein, weil die Verhältnisse hier ziemlich verwickelt werden. Dies ist insofern vielleicht nicht notwendig, weil es möglich ist, dass man in jedem Körper solche Zahlen θ bestimmen kann, dass diese einer Gleichung $f(\theta) = 0$ genügen, wo $f(x)$ die Forderungen des Satzes 24 erfüllt.

Dedekind[1] versuchte vor der Entdeckung der Existenz von gemeinsamen, ausserwesentlichen Diskriminantenteilern nachzuweisen, dass es in jedem Körper

[1] Dedekind A. § 4.

solche Zahlen gäbe, dass der Index nicht durch p teilbar wäre, »und mit deren Hülfe es folglich gelingen würde, die Bestimmung der Idealfaktoren von p auf die Theorie der höheren Congruenzen zurückzuführen».

Wenn aber

$$p = \mathfrak{p}_1^{l_1} \cdot \mathfrak{p}_2^{l_2} \cdots \mathfrak{p}_r^{l_r}, \quad N\mathfrak{p}_i = p^{m_i}$$

ist und unter den Zahlen m_i mehr gleiche vorkommen, als es verschiedene Primfunktionen vom Grade m_i (mod p) gibt, so ist es klar, dass der Satz von Dedekind nicht ausreichen kann. Es ist nun von Wichtigkeit zu bemerken, dass, wenn man mit Polygonen operiert, ein analoges Verhältniss nicht besteht, weil es nach § 6 immer möglich ist, wenn ein System von Zahlen (41) vorgelegt ist, die Primidealzerlegung von p nach Satz 24 zu bestimmen.

Zu diesen Untersuchungen werde ich in einer späteren Arbeit zurückkehren. Sie sind in der Weise von der grössten Wichtigkeit, als es durch die hier zwar noch fragliche Existenz einer Zahl θ immer möglich wurde, die Theorie der Ideale nicht auf höhere Kongruenzen, sondern auf die Theorie der Kongruenzen für Polygone aufzubauen. Es ist mir aber in der Tat gelungen nachzuweisen, dass es in jedem Körper solche Zahlen θ gibt.