WEITERE UNTERSUCHUNGEN ZUR THEORIE DER ALGEBRAISCHEN KÖRPER.

VON

ÖYSTEIN ORE

in KRISTIANIA.

In meiner Abhandlung »Zur Theorie der algebraischen Körper», Acta mathematica, Bd. 44[1], habe ich allgemein die Aufgabe behandelt, die Primidealzerlegung einer vorgelegten Primzahl p in einem Körper $P(\vartheta)$ zu bestimmen.

Es sei der Körper $P(\vartheta)$ durch die Gleichung

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

bestimmt, wo

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{2}$$

eine irreduzible Gleichung mit ganzen rationalen Koeffizienten bedeutet. Meine Aufgabe war dann, die Primidealzerlegung der Primzahl p direkt aus den arithmetischen Eigenschaften der Gleichung (2) abzuleiten und in der Weise die Dedekindschen Untersuchungen über Primideale zu verallgemeinern und zu vervollständigen. Bekanntlich versagen die Dedekindschen Methoden in dem Falle, dass die Primzahl p ein Indexteiler der natürlichen Ordnung

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

ist. Bei meinen eben erwähnten Untersuchungen, wo ich speziell diese Primzahlen untersuche, treten gewisse Ausnahmefälle auf, wofür die Bestimmung der Primideale sich besonders schwierig gestaltet. Der Zweck der vorliegenden Ar-

[1] Acta mathematica, Bd. 44, pp. 219—314. Diese Abhandlung wird im Folgenden mit a bezeichnet.

19—2454. *Acta mathematica.* 45. Imprimé le 16 juillet 1924.

beit ist zu zeigen, dass in jedem Körper solche Zahlen ω des Körpers existieren, dass bei der Gleichung, welcher ω genügt, solche Anomalien nicht eintreten können.

§ 1.

Es sei

$$f(x) \equiv \varphi_1(x)^{e_1} \cdot \varphi_2(x)^{e_2} \dots \varphi_s(x)^{e_s} \pmod{p} \tag{3}$$

die Primfunktionzerlegung von $f(x) \pmod{p}$, wo die Primfunktion $\varphi_i(x)$ allgemein vom Grade m_i ist.

Dann ist immer eine Idealzerlegung

$$p = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \dots \mathfrak{a}_s \tag{4}$$

möglich, wo keines der Ideale $\mathfrak{a}_i$ Einheitsideal ist. Diese Ideale sind ausserdem alle zu einander relativ prim und durch

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

bestimmt.[1]

Um nun aus (4) die Primidealzerlegung von p zu erhalten, muss man die Ideale $\mathfrak{a}_i$ in ihre Primidealfaktoren zerlegen. Dies geschieht nun in der Weise, dass man für jeden Primfunktionteiler $\varphi_i(x)$ von $f(x) \pmod{p}$ eine *Entwicklung* $(p, \varphi_i(x))$ bildet.

Es sei $\varphi(x)$ eine beliebige Primfunktion, welche $\pmod{p}$ in $f(x)$ aufgeht, also etwa

$$f(x) \equiv \varphi(x)^e \cdot \psi(x) \pmod{p}, \tag{5}$$

wo

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

ist.

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

$$f(x) = \sum_{i=1}^{t} p^{a_i} Q_i(x) \cdot \varphi(x)^i \tag{6}$$

darstellen, wo die Polynome $Q_i(x)$ höchstens vom Grade $m-1$ sind. Wenn dann auch die Exponenten a_i so gewählt werden, dass (wenn $Q_i(x) \not\equiv 0$ ist)

---

[1] Man sehe a. p. 265.

$$Q_i(x) \not\equiv 0 \pmod{p}$$

ist, wird die Summe (6) eine Entwicklung $(p, \varphi(x))$ von $f(x)$ genannt.

Zu den Gitterpunkten $(\alpha_i, t-i)$ kann man ein NEWTONSches Polygon konstruieren, das im Punkte (0, 0) anfängt und im Punkte (t, α_t) seinen Endpunkt hat.

Wegen der Kongruenz (5) folgt, dass es in diesem Polygone gewiss Seiten gibt, welche oberhalb der X-Achse liegen müssen. Die erste Seite des Polygons wird aber im allgemeinen mit der X-Achse zusammenfallen können. Die Gesamtheit der Seiten, welche nicht mit der X-Achse zusammenfallen, bilden zusammen ein Newtonsches Polygon, das ich das *Hauptpolygon* der Entwicklung $(p, \varphi(x))$ nenne.[1]

Die Seiten des Hauptpolygons werden mit

$$S_1, S_2, \ldots S_k$$

bezeichnet, wo die Seite S_i die Projektionen l_i und h_i auf die X-Achse bzw. Y-Achse besitzt. Die Grössen l_i und h_i sind beide ganze rationale Zahlen, und es soll

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

gesetzt werden, wo λ_i zu $\varkappa_i$ relativ prim ist.

Bezeichnet man mit $\psi_i(x)$ die Summe der Glieder in der Entwicklung $(p, \varphi(x))$, wofür die entsprechenden Punkte auf der Seite S_i liegen, so wird $\psi_i(x)$ die Form

$$\psi_i(x) = \varphi(x)^\alpha \cdot p^\beta \cdot (Q_\gamma(x) \cdot \varphi(x)^{l_i} + Q_{\gamma+\lambda_i}\varphi(x)^{l_i-\lambda_i} \cdot p^{\varkappa_i} + Q_{\gamma+2\lambda_i}(x) \cdot \varphi(x)^{l_i-2\lambda_i} \cdot p^{2\varkappa_i} + \cdots + Q_{\gamma+\varepsilon_i \cdot \lambda_i}(x) \cdot p^{h_i})$$

haben, wo die Exponenten α und β gewisse ganze rationale, positive Zahlen bedeuten und ebenso γ eine ganze rationale Zahl ist.

Setzt man hier

$$R_{i,s}(x) = Q_{\gamma+s \cdot \lambda_i}(x) \qquad (s = 0, 1, 2, \ldots \varepsilon_i),$$

so ist

$$\psi_i(x) = \varphi(x)^\alpha \cdot p^\beta \cdot \varphi_i(x),$$

---

[1] Man sehe a. Kap. II. § 2.

wo

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

Da nun allgemein

$$R_{i,0}(x) = R_{i-1,\varepsilon_{i-1}}(x) \not\equiv 0 \,(\mathrm{modd}\, p, \varphi(x))$$

ist, kann man ein Polynom $A_i(x)$ von höchstens $(m-1)^{\text{tem}}$ Grade so bestimmen, dass

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

Dann heisst das Polynom

$$f_i(x) = \varphi(x)^{l_i} + S_{i,1}(x) \cdot \varphi(x)^{l_i - \lambda_i} \cdot p^{\varkappa_i} + \cdots + S_{i,\varepsilon_i}(x)\, p^{h_i}, \tag{7}$$

wo

$$S_{i,s}(x) \equiv R_{i,s}(x) \cdot A_i(x) \,(\mathrm{modd}\, p, \varphi(x)),$$

der *Faktor der i^{ten} Seite* in der Entwicklung $(p, \varphi(x))$.

Das Polygon $(p, \varphi(x))$ von $f_i(x)$ ist gleich der i^{ten} Seite S_i; die Koeffizienten $S_{i,s}(x)$ kann man ausserdem $(\mathrm{modd}\, p, \varphi(x))$ reduziert annehmen, d. h. sie sollen höchstens vom Grade $m-1$ sein.

Wenn nun zwei Polynome $g(x)$ und $h(x)$ dasselbe geradlinige Polygon L besitzen, so sagt man

$$g(x) \equiv h(x) \,(\mathrm{mod}\, L),$$

wenn in der Differenz $g(x) - h(x)$ alle repräsentierenden Punkte oberhalb L liegen.

Den Faktor der i^{ten} Seite kann man dann eindeutig in Primfaktoren $(\mathrm{mod}\, S_i)$ zerlegen, so dass man

$$f_i(x) \equiv f_1^{(i)}(x) \cdot f_2^{(i)}(x) \ldots f_{t_i}^{(i)}(x) \,(\mathrm{mod}\, S_i) \tag{8}$$

hat, wo

$$f_j^{(i)}(x) = \varphi(x)^{\varepsilon_j^{(i)} \cdot \lambda_i} + S_{j,1}^{(i)}(x) \cdot p^{\varkappa_i} \cdot \varphi(x)^{\left(\varepsilon_j^{(i)} - 1\right)\lambda_i} + \cdots + S_{j,\varepsilon_j^{(i)}}^{(i)}(x) \cdot p^{\varepsilon_j^{(i)} \cdot \varkappa_i} \tag{9}$$

ein Polynom bedeutet, wofür das Polygon $(p, \varphi(x))$ eine Gerade mit der Neigung $\frac{\varkappa_i}{\lambda_i}$ ist, und ausserdem soll $f_j^{(i)}(x) \,(\mathrm{mod}\, S_i)$ *irreduzibel* sein, womit man bezeichnet, dass $f_j^{(i)}(x)$ nicht kongruent dem Produkte zweier Polynome sein kann, welche geradlinige Polygone von der Neigung $\frac{\varkappa_i}{\lambda_i}$ besitzen.

Setzt man

$$y = \frac{\varphi(x)^{\lambda_i}}{p^{\varkappa_i}},$$

so folgt aus (7)

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

Wenn dann $f_i(x)$ die Zerlegung (8) (mod S_i) besitzt, besteht auch eine Zerlegung

$$F_i(x, y) \equiv \psi_1^{(i)}(x, y) \cdot \psi_2^{(i)}(x, y) \ldots \psi_{t_i}^{(i)}(x, y) \,(\mathrm{modd}\, p, \varphi(x)),$$

wo y als unabhängige Variable betrachtet wird. Hier ist $\psi_j^{(i)}(x, y)\,(\mathrm{modd}\, p, \varphi(x))$ irreduzibel und ausserdem

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

Die Primfunktionzerlegungen (8) der Faktoren der Seiten spielen nun für die Primidealzerlegung von p im Körper $P(\vartheta)$ eine sehr wichtige Rolle, indem man nämlich folgendes beweisen kann:

Wenn die Primfunktionzerlegung von $f(x)\,(\mathrm{mod}\, p)$ durch (3) gegeben ist, so war, wie früher bemerkt,

$$p = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \ldots \mathfrak{a}_s$$

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

Um nun ein Ideal $\mathfrak{a} = (p, \varphi(\vartheta)^e)$ weiter zu zerlegen, bestimmt man für die Primfunktion $\varphi(x)$ die Entwicklung $(p, \varphi(x))$ von $f(x)$. Dann ist mit den früheren Bezeichnungen

$$\mathfrak{a} = P_1^{\lambda_1} \cdot P_2^{\lambda_2} \ldots P_k^{\lambda_k},$$

wo keines der Ideale P_i das Einheitsideal ist und diese Ideale ausserdem alle zu einander relativ prim sind.

Die Primfunktionzerlegung von $f_i(x)\,(\mathrm{mod}\, S_i)$ sei nun durch (8) gegeben, wo erstens vorausgesetzt werde, dass alle Primfunktionen $f_j^{(i)}(x)$ von einander verschieden seien. Wenn dies für alle Polygone $(p, \varphi(x))$ und alle Seiten S_i dieser Polygone der Fall ist, so hat das Ideal P_i die Primidealzerlegung

$$P_i = \mathfrak{p}_1^{(i)} \cdot \mathfrak{p}_2^{(i)} \dots \mathfrak{p}_{t_i}^{(i)},$$

wo das Primideal $\mathfrak{p}_j^{(i)}$ den Grad $\varepsilon_j^{(i)} \cdot m$ hat, also $N\mathfrak{p}_j^{(i)} = p^{\varepsilon_j^{(i)} \cdot m}$ ist.

Wenn zweitens nicht alle Primfunktionen in (8) verschieden sind, also etwa

$$f_i(x) \equiv f_1^{(i)}(x)^{e_1^{(i)}} \cdot f_2^{(i)}(x)^{e_2^{(i)}} \dots f_{t_i}^{(i)}(x)^{e_{t_i}^{(i)}} \pmod{S_i},$$

so ist auch

$$P_i = P_1^{(i)} \cdot P_2^{(i)} \dots P_{t_i}^{(i)}$$

eine Idealzerlegung von P_i, wo keines der Ideale $P_j^{(i)}$ das Einheitsideal ist und diese Ideale alle zu einander relativ prim sind, sie brauchen aber nicht Primideale zu sein.

In meiner oben zitierten Arbeit (a) habe ich auch Ausdrücke für die Primideale $\mathfrak{p}_j^{(i)}$ und im allgemeineren Falle für die Ideale $P_j^{(i)}$ als grösste gemeinsame Faktoren für Hauptideale angegeben. Die Primidealzerlegung der Primzahl p kann daher vollständig bestimmt werden, wenn man nur eine ganze primitive Zahl θ des Körpers bestimmen kann, so dass in der Gleichung, welcher θ genügt, für alle Seiten der Polygone $(p, \varphi(x))$ die entsprechenden Faktoren der Seiten keine mehrfache Primfunktionen besitzen.

Es sei $f(x) = 0$ die Gleichung, welcher eine ganze Zahl des Körpers genügt. Diese Gleichung soll im Folgenden *regulär in Bezug auf die Primzahl p* heissen, wenn sie die folgenden Eigenschaften besitzt:

1) $f(x)$ soll irreduzibel und vom Grade n sein.
2) Wenn $\varphi(x)$ eine Primfunktion $(\mathrm{mod}\, p)$ ist, welche $(\mathrm{mod}\, p)$ in $f(x)$ aufgeht, so sollen in dem Hauptpolygone $(p, \varphi(x))$ die Faktoren der Seiten S_i nie mehrfache Primfunktionteiler $(\mathrm{mod}\, S_i)$ besitzen.

Die Bestimmung der Primidealzerlegung der Primzahl p ist demnach auf die Bestimmung einer regulären Gleichung in Bezug auf p zurückgeführt. Es soll im Folgenden nachgewiesen werden, dass *es in jedem Körper und für jede Primzahl reguläre Gleichungen gibt.*

Weiter soll bewiesen werden, dass man diese regulären Gleichungen von einer speziellen Form annehmen darf.

§ 2.

Es sei in $P(\vartheta)$

$$\mathfrak{p} = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_r^{e_r} \tag{10}$$

die Primidealzerlegung der Primzahl p, wo allgemein

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

und folglich

$$e_1 m_1 + \cdots + e_r m_r = n. \tag{11}$$

Ich setze nun zunächst

$$p = \mathfrak{p}^e \cdot P, \tag{12}$$

wo das Ideal P nicht durch das Primideal $\mathfrak{p}$ teilbar ist; weiter wird

$$N\mathfrak{p} = p^m \tag{13}$$

angenommen.

Dann genügen alle ganze Zahlen λ des Körpers der Kongruenz

$$\lambda^{p^m} - \lambda \equiv 0 \pmod{\mathfrak{p}}, \tag{14}$$

und da es nach (13) p^m inkongruente Zahlen (mod $\mathfrak{p}$) gibt, so hat die Kongruenz (14) ebenso viele Wurzeln wie der Grad p^m der Kongruenz. Weiter ist aber auch

$$x^{p^m} - x \pmod{p}$$

kongruent dem Produkte aller Primfunktionen (mod p), deren Grade Teiler von m sind. Wenn daher $\varphi(x)$ eine beliebige Primfunktion m^{ten} Grades bedeutet, so ist folglich

$$x^{p^m} - x \equiv \varphi(x) \cdot \Phi(x) \pmod{p},$$

wo $\Phi(x)$ ein Polynom vom Grade $p^m - m$ bedeutet.

Nach (14) ergibt sich dann auch

$$\varphi(\lambda) \cdot \Phi(\lambda) \equiv 0 \pmod{\mathfrak{p}}$$

für jede ganze Zahl des Körpers. Da aber eine Kongruenz nicht mehr inkongruente Lösungen besitzen kann, als ihr Grad angibt, so zeigt dies, dass es m ganze, für den Modul $\mathfrak{p}$ inkongruente Zahlen

$$\alpha_1, \alpha_2, \ldots \alpha_m$$

des Körpers gibt, so dass

$$\varphi(\alpha_i) \equiv 0 \pmod{\mathfrak{p}} \qquad (i = 1, 2, \ldots m).$$

Es sei nun α eine beliebige dieser Zahlen. Wenn dann $\beta = R(\alpha)$ eine ganze Zahl des Körpers ist und $R(\alpha)$ ein Polynom in α, so kann β nur dann durch $\mathfrak{p}$ teilbar sein, wenn

$$R(x) \equiv 0 \,(\text{modd } p, \varphi(x)).$$

Sonst könnte man nämlich die Polynome $A(x)$ und $B(x)$ so bestimmen, dass

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

woraus für $x = \alpha$

$$B(\alpha) \cdot R(\alpha) \equiv 1 \pmod{\mathfrak{p}}$$

folgt.

Die Zahl α war also eine Lösung der Kongruenz

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

Es soll nun gezeigt werden, dass man dann aus α immer eine Lösung α_h der Kongruenz

$$\varphi(x) \equiv 0 \pmod{\mathfrak{p}^h} \tag{15}$$

herleiten kann, derart dass

$$\alpha_h \equiv \alpha \pmod{\mathfrak{p}}. \tag{16}$$

Es wird angenommen, dass dies für alle Exponenten bis $h-1$ bewiesen worden sei; dann soll gezeigt werden, dass, wenn α_{h-1} eine Wurzel der Kongruenz

$$\varphi(x) \equiv 0 \pmod{\mathfrak{p}^{h-1}} \tag{17}$$

mit $\alpha_{h-1} \equiv \alpha \pmod{\mathfrak{p}}$ ist, man daraus eine Wurzel α_h von (15) berechnen kann, wofür (16) gilt.

Ich beweise zunächst, dass

$$\varphi'(\alpha_{h-1}) \equiv \varphi'(\alpha) \not\equiv 0 \pmod{\mathfrak{p}}$$

ist. Dies folgt leicht daraus, dass eine Primfunktion (mod p) immer (mod p) zu ihrer Derivierten relativ prim ist. Man kann nämlich dann die Polynome $A(x)$ und $B(x)$ so bestimmen, dass

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

und für $x=\alpha$ folgt daraus

$$B(\alpha).\varphi'(\alpha)\equiv 1 \pmod{\mathfrak{p}},$$

d. h. $\varphi'(\alpha)$ kann nicht durch $\mathfrak{p}$ teilbar sein.

Dies zeigt, dass man die Kongruenz

$$\varphi(\alpha_{h-1})+\gamma.\varphi'(\alpha_{h-1})\equiv 0 \pmod{\mathfrak{p}^h} \tag{18}$$

immer lösen kann, und da $\varphi(\alpha_{h-1})$ nach (17) durch $\mathfrak{p}^{h-1}$ teilbar ist, muss auch die Wurzel γ der Kongruenz (18) mindestens durch $\mathfrak{p}^{h-1}$ teilbar sein.

Die ganze Zahl

$$\alpha_h=\alpha_{h-1}+\gamma$$

ist dann eine Wurzel der Kongruenz (15). Man hat nämlich

$$\varphi(\alpha_{h-1}+\gamma)=\varphi(\alpha_{h-1})+\gamma\varphi'(\alpha_{h-1})+\frac{\gamma^2}{2!}\varphi''(\alpha_{h-1})+\ldots. \tag{19}$$

Hier sind die Zahlen

$$\frac{\varphi''(\alpha_{h-1})}{2!},\ \frac{\varphi'''(\alpha_{h-1})}{3!},\ldots.$$

wie man leicht einsieht, alle ganz, und da γ^2 durch $\mathfrak{p}^{2h-2}$ teilbar ist, sind die Glieder

$$\frac{\gamma^2}{2!}\varphi''(\alpha_{h-1}),\ \frac{\gamma^3}{3!}\varphi'''(\alpha_{h-1}),\ldots$$

sicher durch $\mathfrak{p}^h$ $(h\geqq 2)$ teilbar. Es ist daher nach (19) und (18)

$$\varphi(\alpha_h)\equiv\varphi(\alpha_{h-1}+\gamma)\equiv\varphi(\alpha_{h-1})+\lambda\cdot\varphi'(\alpha_{h-1})\equiv 0 \pmod{\mathfrak{p}^h}.$$

Weiter ist

$$\alpha_h\equiv\alpha_{h-1}\equiv\alpha \pmod{\mathfrak{p}}.$$

Es ist folglich bewiesen, dass man immer eine ganze Zahl α des Körpers bestimmen kann, so dass $\varphi(\alpha)$ durch $\mathfrak{p}^h$ teilbar wird, wobei h beliebig angenommen werden kann.

Diese Zahl α kann man aber auch so wählen, dass für ein gegebenes h die Zahl $\varphi(\alpha)$ genau durch $\mathfrak{p}^h$, d. h. durch $\mathfrak{p}^h$ aber nicht durch $\mathfrak{p}^{h+1}$ teilbar wird.

Wenn dies nämlich für α nicht der Fall ist, so muss $\varphi(\alpha)\equiv 0 \pmod{\mathfrak{p}^{h+1}}$ sein. Man setzt dann $\alpha_1=\alpha+\beta$, wo die ganze Zahl β genau durch $\mathfrak{p}^h$ teilbar ist, und so folgt

$$\varphi(\alpha_1)=\varphi(\alpha)+\beta\cdot\varphi'(\alpha)+\beta^2\frac{\varphi''(\alpha)}{2!}+\cdots$$

woraus

$$\varphi(\alpha_1)\equiv\beta\cdot\varphi'(\alpha)\not\equiv 0 \pmod{\mathfrak{p}^{h+1}}.$$

Es seien nun

$$\mathfrak{p}_1,\ \mathfrak{p}_2,\ \ldots\ \mathfrak{p}_s$$

diejenigen Primidealteiler von p, deren Grade gleich m sind, wofür also $N\mathfrak{p}_i=p^m$. Weiter soll p durch $\mathfrak{p}_i^{e_i}$ teilbar sein. Den Zahlen

$$e_1,\ e_2,\ \ldots\ e_s$$

kann man dann eine andere Reihe von positiven, ganzen rationalen Zahlen

$$h_1,\ h_2,\ \ldots\ h_s$$

so zuordnen, dass allgemein h_i zu e_i relativ prim ist.

Nach den eben durchgeführten Hilfsuntersuchungen kann man nun, wenn $\varphi(x)$ eine beliebige Primfunktion (mod p) vom Grade m bedeutet, die Zahlen

$$\alpha_1,\ \alpha_2,\ \ldots\ \alpha_s$$

so bestimmen, dass

$$\varphi(\alpha_i)\equiv 0 \pmod{\mathfrak{p}_i} \qquad (i=1,\ 2,\ \ldots\ s)$$

und weiter auch so, dass

$$\left.\begin{aligned}&\varphi(\alpha_i)\equiv 0 \pmod{\mathfrak{p}_i^{h_i}}\\ &\varphi(\alpha_i)\not\equiv 0 \pmod{\mathfrak{p}^{h_i+1}}\end{aligned}\right\} \quad (i=1,\ 2,\ \ldots\ s) \qquad (20)$$

Die ganze rationale Zahl h wird nun beliebig fest angenommen, jedoch so, dass h grösser als alle h_i ist. Dann sind die Kongruenzen

$$\vartheta\equiv\alpha_i \pmod{\mathfrak{p}_i^h} \qquad (i=1,\ 2,\ \ldots\ s)$$

immer lösbar, und da

$$\varphi(\vartheta)\equiv\varphi(\alpha_i) \pmod{\mathfrak{p}_i^h} \qquad (i=1,\ 2,\ \ldots\ s),$$

so folgt wegen (20), dass auch

$$\varphi(\vartheta) \equiv 0 \pmod{\mathfrak{p}_i^{h_i}}$$
$$\varphi(\vartheta) \not\equiv 0 \pmod{\mathfrak{p}_i^{h_i+1}} \qquad (i = 1, 2, \ldots s)$$

ist.

§ 3.

Ich schreibe nun die Primidealzerlegung (10) von p in der Form

$$p = \mathfrak{a}_{m_1} \cdot \mathfrak{a}_{m_2} \cdots \mathfrak{a}_{m_s},$$

wo das Ideal $\mathfrak{a}_{m_i}$ die Primidealzerlegung

$$\mathfrak{a}_{m_i} = \mathfrak{p}_{1,m_i}^{e_{1,m_i}} \cdot \mathfrak{p}_{2,m_i}^{e_{2,m_i}} \cdots \mathfrak{p}_{r_i,m_i}^{e_{r_i,m_i}} \qquad (i = 1, 2, \ldots s) \tag{21}$$

besitzt, wo alle Primideale $\mathfrak{p}_{j,m_i}$ den Grad m_i haben.

Zu den Zahlen

$$e_{1,m_i},\ e_{2,m_i}, \ldots, e_{r_i,m_i} \qquad (i = 1, 2, \ldots s)$$

kann man eine andere Reihe von positiven, ganzen rationalen Zahlen

$$h_{1,m_i}, h_{2,m_i}, \ldots h_{r_i,m_i}$$

so bestimmen, dass immer h_{j,m_i} zu e_{j,m_i} relativ prim ist und ausserdem

$$\frac{h_{1,m_i}}{e_{1,m_i}} < \frac{h_{2,m_i}}{e_{2,m_i}} < \cdots < \frac{h_{r_i,m_i}}{e_{r_i,m_i}}, \tag{22}$$

was offenbar immer möglich ist.

Es sei nun

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

eine Reihe von Primfunktionen (mod p) derart, dass $\varphi_i(x)$ vom Grade m_i ist. Nach § 2 ist es dann immer möglich, ganze Zahlen des Körpers

$$\vartheta_1, \vartheta_2, \ldots \vartheta_s$$

so zu bestimmen, dass

$$\varphi_i(\vartheta_i) \equiv 0 \left(\mathrm{mod}\ \mathfrak{p}_{j,m_i}^{h_{j,m_i}}\right) \qquad (j = 1, 2, \ldots r_i)\ (i = 1, 2, \ldots s),$$

aber auch

$$\varphi_i(\vartheta_i) \not\equiv 0 \pmod{\mathfrak{p}_{j,m_i}^{h_{j,m_i}+1}} \qquad (j=1,2,\ldots r_i)\ (i=1,2,\ldots s).$$

Die Zahl H wird nun grösser als alle Zahlen

$$h_{j,m_i} \qquad (j=1,2,\ldots r_i)\ (i=1,2,\ldots s)$$

gewählt. Da dann die Ideale

$$A_i=(\mathfrak{p}_{1,m_i}\mathfrak{p}_{2,m_i}\ldots\mathfrak{p}_{r_i,m_i})^H \qquad (i=1,2,\ldots s)$$

alle zu einander relativ prim sind, so sind die Kongruenzen

$$\theta\equiv\vartheta_i \pmod{A_i} \qquad (i=1,2,\ldots s)$$

sicher auflösbar. Für die ganze Zahl θ hat man dann

$$\varphi_i(\theta)\equiv\varphi_i(\vartheta_i) \pmod{A_i} \qquad (i=1,2,\ldots s),$$

und folglich ist die Zahl

$$\varphi_i(\theta) \qquad (i=1,2,\ldots s)$$

durch die Ideale

$$\mathfrak{p}_{j,m_i} \qquad (j=1,2,\ldots r_i)$$

genau in der Potenz h_{j,m_i} teilbar.

Es wird nun die Gleichung

$$F(x)=0$$

gebildet, welcher die in dieser Weise bestimmte Zahl θ genügt, und *es soll gezeigt werden, dass diese Gleichung eine reguläre Gleichung in Bezug auf die Primzahl p sein muss.*

Die Primfunktionzerlegung von $F(x)$ sei durch

$$F(x)\equiv\Psi_1(x)^{a_1}\cdot\Psi_2(x)^{a_2}\ldots\Psi_t(x)^{a_t} \pmod{p}$$

gegeben. Man kann dann zunächst zeigen, dass unter den Primfunktionen $\Psi_i(x)$ alle Primfunktionen $\varphi_i(x)$ vorkommen müssen. Es ist nämlich

$$\Psi_1(\theta)^{a_1}\cdot\Psi_2(\theta)^{a_2}\ldots\Psi_t(\theta)^{a_t}\equiv 0 \pmod{p}$$

und folglich das Produkt

$$\Pi(\theta) = \Psi_1(\theta) \cdot \Psi_2(\theta) \ldots \Psi_l(\theta)$$

durch alle Primidealteiler von p teilbar. Nun kann aber eine Zahl $\Pi(\theta)$ nur dann durch den Primidealteiler $\mathfrak{p}$ von p teilbar sein, wenn

$$\Pi(x) \equiv 0 \,(\mathrm{modd}\, p, \varphi(x)),$$

wo $\varphi(x)$ die Primfunktion (mod p) ist, wofür $\varphi(\theta) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$. Daher muss $\Pi(x) \,(\mathrm{mod}\, p)$ durch alle Primfunktionen $\varphi_i(x)$ teilbar sein.

Man kann darum

$$F(x) \equiv \varphi_1(x)^{a_1} \cdot \varphi_2(x)^{a_2} \ldots \varphi_s(x)^{a_s} \cdot Q(x) \,(\mathrm{mod}\, p), \tag{23}$$

schreiben, wo $Q(x)$ ein Polynom ist, das durch keine der Primfunktionen $\varphi_i(x)$ (mod p) teilbar ist. Weiter sind alle a_i grösser als Null.

Man bilde dann die Polygone $(p, \varphi_i(x))$ für $F(x)$. Da nun $\varphi_i(\theta)$ durch $\mathfrak{p}_{j,m_i}^{h_{j,m_i}}$ teilbar ist, folgt nach Satz 26 (a), dass es in dem Hauptpolygone $(p, \varphi_i(x))$ sicher eine Seite mit der Neigungszahl

$$\frac{h_{j,m_i}}{e_{j,m_i}} \qquad (j = 1, 2, \ldots r_i) \tag{24}$$

gibt. Da weiter h_{j,m_i} zu e_{j,m_i} relativ prim ist, muss diese Seite eine Projektion auf die X-Achse besitzen, deren Länge ein Multiplum von e_{j,m_i} ist, also etwa $\varepsilon_{j,m_i} \cdot e_{j,m_i}$. Da weiter keine andere Neigungszahlen als (24) vorkommen können, da sonst $\varphi_i(\theta)$ nach dem eben zitierten Satze auch durch andere Primidealteiler von p als

$$\mathfrak{p}_{1,m_i}, \mathfrak{p}_{2,m_i} \ldots \mathfrak{p}_{r_i,m_i}$$

teilbar würde, so muss nach (23) die Gesamtprojektion des Hauptpolygones $(p, \varphi_i(x))$ auf die X-Achse gleich a_i sein, folglich

$$\sum_{j=1}^{r_i} \varepsilon_{j,m_i} e_{j,m_i} = a_i,$$

und daraus folgt

$$\sum_{i=1}^{s} a_i \cdot m_i = \sum_{i=1}^{s} m_i \sum_{j=1}^{r_i} \varepsilon_{j,m_i} \cdot e_{j,m_i}. \tag{25}$$

Wenn nun $F(x)$ den Grad N hat und q den Grad von $Q(x)$ bedeutet, so ist nach (23)

$$N = q + \sum_{i=1}^{s} a_i m_i,$$

und die Gleichung (25) ergibt dann

$$N = q + \sum_{i=1}^{s} m_i \sum_{j=1}^{r_i} \varepsilon_{j,m_i} \cdot e_{j,m_i}. \tag{26}$$

Da aber nach (21)

$$N(\mathfrak{a}_i) = p^{m_i \sum_{j=1}^{r_i} e_{j,m_i}},$$

so ist

$$N(\mathfrak{p}) = p^{\sum_{i=1}^{s} m_i \sum_{j=1}^{r_i} e_{j,m_i}},$$

also

$$n = \sum_{i=1}^{s} m_i \sum_{j=1}^{r_i} e_{j,m_i}$$

und folglich, da $\varepsilon_{j,m_i} \geqq 1$,

$$\sum_{j=1}^{s} m_i \sum_{j=1}^{r_i} \varepsilon_{j,m_i} \cdot e_{j,m_i} \geqq \sum_{i=1}^{s} m_i \sum_{j=1}^{r_i} e_{j,m_i} = n,$$

wo das Gleichheitszeichen nur dann richtig ist, wenn alle $\varepsilon_{j,m_i} = 1$ sind. Dann ergibt sich aus (26)

$$N \geqq q + n,$$

und da $N \leqq n$ vorausgesetzt werden kann, erhält man $q = 0$ und

$$\sum_{j=1}^{s} m_i \sum_{j=1}^{r_i} \varepsilon_{j,m_i} \cdot e_{j,m_i} = n,$$

also alle $\varepsilon_{j,m_i} = 1$. *$F(x)$ wird also irreduzibel und vom Grade n.*

Aus $q = 0$ folgt $Q(x) = 1$ und daher

$$F(x) \equiv \varphi_1(x)^{a_1} \cdot \varphi_2(x)^{a_2} \dots \varphi_s(x)^{a_s} \pmod{p}.$$

Da immer $\varepsilon_{j,m_i}=1$ ist, wird weiter das Polygon $(p, \varphi_i(x))$ aus r_i Seiten bestehen, welche die Projektionen

$$e_{1,m_i}, e_{2,m_i}, \ldots e_{r_i,m_i}$$

auf die X-Achse besitzen, während die Projektionen auf die Y-Achse gleich

$$h_{1,m_i}, h_{2,m_i}, \ldots h_{r_i,m_i}$$

sind. Da e_{j,m_i} zu h_{j,m_i} relativ prim ist, werden die Faktoren aller Seiten sicher für diese Seiten irreduzibel, und können daher keine mehrfachen Primfunktionen für diese Seiten enthalten.

Die Gleichung $F(x)=0$ ist folglich regulär in Bezug auf p.

Man sieht weiter ein, dass man immer eine solche reguläre Gleichung des Körpers bestimmen kann, dass die Faktoren der Seiten alle irreduzibel sind. Wenn eine Seite die Neigungszahl $\frac{\varkappa}{\lambda}$ hat, so kann man die reguläre Gleichung auch so wählen, dass der Faktor dieser Seite von der Form

$$\varphi^{\lambda}(x)+Q(x)\,.\,p^{\varkappa}$$

wird, wo $Q(x)$ ein Polynom von höchstens $(m-1)^{\text{tem}}$ Grade ist.

§ 4.

Man kann folglich immer für die Untersuchung eines algebraischen Körpers eine reguläre Gleichung in Bezug auf die Primzahl p zu Grunde legen, und in diesem Falle gestaltet sich die Bestimmung der Eigenschaften der Primzahl p besonders einfach.

Wenn die Primfunktionzerlegung der regulären Gleichung $f(x)=0$ durch (3) gegeben ist, so gibt (4) eine Idealzerlegung von p an. Wenn weiter durch (8) die Primfunktionzerlegung des Faktors der i^{ten} Seite in der Entwicklung $(p, \varphi(x))$ von $f(x)$ gegeben ist, so hat das Ideal $\mathfrak{a}$ die Primidealzerlegung

$$\mathfrak{a}=(\mathfrak{p}_1^{(1)}\,.\,\mathfrak{p}_2^{(1)}\,..\,\mathfrak{p}_{t_1}^{(1)})^{\lambda_1}\,.\,(\mathfrak{p}_1^{(2)}\,..\,\mathfrak{p}_{t_2}^{(2)})^{\lambda_2}\ldots(\mathfrak{p}_1^{(k)}\,..\,\mathfrak{p}_{t_k}^{(k)})^{\lambda_k},$$

wo der Grad des Primideals $\mathfrak{p}_j^{(i)}$ gleich $m\,.\,\varepsilon_j^{(i)}$ ist.

Durch das Dedekindsche Kriterium[4] kann man immer bestimmen, wann eine

[4] DEDEKIND, R.: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Göttinger Abhandlungen. 1878. § 2.

vorgelegte Primzahl p ein Teiler der Körperdiskriminante, aber kein Teiler des Index ist. Unter Anwendung von Polygonen kann man das Dedekindsche Kriterium folgendermassen aussprechen:

A. Die Primzahl p ist ein Teiler der Körperdiskriminante, aber kein Teiler des Index dann und nur dann, wenn alle Polygone $(p, \varphi(x))$ von $f(x)$ geradlinig sind und für diese Geraden entweder $h_1=1$ oder $l_1=1$ ist.

Wenn die Gleichung $f(x)=0$ in Bezug auf p regulär ist, kann man auch ein einfaches Kriterium für Indexteiler angeben. Soll nämlich p ein Teiler des Index, aber kein Teiler der Körperdiskriminante sein, so kann in der Primidealzerlegung von p kein Primidealteiler mehrfach vorkommen. Folglich müssen alle λ_i gleich 1 sein, und daher sind alle Neigungszahlen $\frac{h_i}{l_i}$ ganz.

Man kann daher den folgenden Satz aussprechen:

B. Wenn $f(x)=0$ eine reguläre Gleichung in Bezug auf p ist, so ist die Primzahl p dann und nur dann ein Teiler des Index, aber kein Teiler der Körperdiskriminante, wenn in sämtlichen Polygonen $(p, \varphi(x))$ alle Neigungszahlen $\frac{h_i}{l_i}$ ganz sind.

Dabei ist natürlich vorausgesetzt, dass in der Primfunktionzerlegung (3) von $f(x)$ mehrfache Primfunktionfaktoren (mod p) vorkommen, d. h. dass die Primzahl p ein Teiler der Diskriminante der Gleichung $f(x)=0$ ist.

Wenn $f(x)$ nicht regulär ist, so ist die Ganzzahligkeit aller Neigungszahlen $\frac{h_i}{l_i}$ zwar eine notwendige, aber keine hinreichende Bedingung dafür, dass p ein Teiler des Index, aber kein Teiler der Körperdiskriminante ist.

Wenn $f(x)$ regulär und die Primzahl p ein Teiler der Diskriminante von $f(x)$ ist, und keiner der Fälle A oder B eintritt, so ist die Primzahl p ein gemeinsamer Teiler des Index und der Körperdiskriminante.