Werk

Label: Article

Jahr: 1939

PURL: https://resolver.sub.uni-goettingen.de/purl?31311028X_0068|log43

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Über die Reduzibilität eines Polynoms mit ganzen algebraischen Koeffizienten nach einem Primideal; Anwendung auf die Faktorzerlegung der Polynome in algebraischen Zahlkörpern.[1])

Štefan Schwarz, Praha.

Herausgegeben mit Unterstützung des Masarykfondes bei dem Nationalforschungsrat.

(Eingegangen am 10. Jänner 1938.)

Unter einer ganzen algebraischen Zahl n-ten Grades verstehen wir eine komplexe Zahl, die einer im Körper der rationalen Zahlen irreduziblen Gleichung n-ten Grades mit ganzen rationalen Koeffizienten und mit höchstem Koeffizienten 1 genügt.

Der Körper der rationalen Zahlen sei K.

Wir betrachten Polynome der Gestalt

$$f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n, \tag{1}$$

wo α_i ganze algebraische Zahlen des Körpers $K(\vartheta)$ sind (ϑ primitives Element). Durch π bezeichnen wir die Primideale dieses Körpers.

Ein Polynom $f(x)$ nennt man reduzibel (mod π) d. h.

$$f(x) \equiv g(x) \,.\, h(x) \pmod{\pi}, \text{ oder } f(x) - g(x) \,.\, h(x) \equiv 0 \pmod{\pi}, \tag{2}$$

wo g, h, wieder ganze algebraische Koeffizienten besitzen, wenn jeder Koeffizient von (2) eine Zahl des Ideals π ist (oder auch — was dasselbe bedeutet — durch das Primideal π teilbar ist).

Im Folgenden werden wir als Koeffizienten der Polynome Elemente des Körpers der Restklassen nach dem Primideal π (π fest) $K_\pi(\vartheta)$ zulassen und werden deswegen oft direkt die Gleich-

[1]) Diese Arbeit ist ein neugefaßter Teil meiner Disertation, die an der Karlsuniversität im Sommer 1937 vorgelegt wurde.

heit $f(x) = g(x) \,.\, h(x) \pmod{\pi}$ schreiben. Wo kein Mißverständnis zu befürchten ist — z. B. im ganzen ersten Teile — lassen wir das Zeichen (mod π) weg.

Erster Teil.

I.

Es sei $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ ein Polynom aus $K_\pi(\vartheta)$. [Es genügt sich auf Polynome mit dem höchsten Koeffizienten 1 (Einsklasse) zu beschränken.]

Die ganzen alg. Zahlen α_i (Repräsentanten der Klassen) können soviele Werte annehmen wieviel die Anzahl der Restklassen beträgt, also $N(\pi)$ (Norm von π). Die Anzahl aller Polynome n-ten Grades aus $K_\pi(\vartheta)$ ist also $N(\pi)^n$. Einige unter ihnen sind in $K_\pi(\vartheta)$ reduzibel — andere irreduzibel.

Nun führen wir die verallgemeinerte Galoissche Imaginäre ein. Es soll ein ganz bestimmtes irreduzibles Polynom $f(x)$ n-ten Grades gewählt werden. Durch das Symbol j bezeichnen wir die Größe, die dieser Gleichung genügt, d. h. $j^n + \alpha_1 j^{n-1} + \ldots + \alpha_n \equiv 0 \pmod{\pi}$ gilt. Wir adjungieren diese Größe j zum Körper $K_\pi(\vartheta)$; dann gilt:

1. $K_\pi(\vartheta; j)$ ist ein endlicher Körper, dessen Elemente von der Gestalt $\omega_0 + \omega_1 j + \ldots + \omega_{n-1} j^{n-1}$ sind [wo $\omega_i \in K_\pi(\vartheta)$] und die Anzahl der Elemente dieses Körpers beträgt $N(\pi)^n$.

2. Die sämtlichen Körperelemente des Körpers $K_\pi(\vartheta; j)$ genügen der Gleichung

$$x^{N(\pi)^n} - x = 0. \tag{3}$$

3. Das Polynom (3) ist durch jedes irreduzible Polynom n-ten Grades aus $K_\pi(\vartheta)$ teilbar. (Ist $n = n' \,.\, n''$, so gilt dies auch für irreduzible Polynome n'-ten resp. n''-ten Grades.)

4. Ist j eine Nullstelle des in $K_\pi(\vartheta)$ irreduziblen Polynoms $f(x)$ vom Grad n, so sind die sämtlichen Nullstellen durch

$$j,\ j^{N(\pi)},\ j^{N(\pi)^2},\ \ldots,\ j^{N(\pi)^{n-1}}, \tag{4}$$

gegeben.

II.

In erster Reihe stellen wir ein Kriterium für die Reduzibilität eines gegebenen Polynoms (mod π) auf. Dies ist eine Verallgemeinerung eines ähnlichen Satzes, der von Herrn Prof. K. Petr stammt und in dieser Zeitschrift **66** (1936—37), S. 85—94 veröffentlicht wurde.

Es sei $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ das gegebene Polynom aus $K_\pi(\vartheta)$, welches wir untersuchen wollen. Das Polynom möge keine mehrfache Wurzeln besitzen [d. h. die Diskriminante ist nicht durch die Nullklasse (mod π) gegeben]. Wir konstruieren mittels der gegebenen Gleichung $f(x) = 0$ folgende Ausdrücke

$$
\begin{aligned}
x^{0.N(\pi)} &= 1, \\
x^{1.N(\pi)} &= \gamma_{10} + \gamma_{11}x + \gamma_{12}x^2 + \ldots + \gamma_{1,n-1}x^{n-1}. \\
x^{2.N(\pi)} &= \gamma_{20} + \gamma_{21}x + \gamma_{22}x^2 + \ldots + \gamma_{2,n-1}x^{n-1}. \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x^{(n-1)N(\pi)} &= \gamma_{n-1,0} + \gamma_{n-1,1}x + \gamma_{n-1,2}x^2 + \ldots + \gamma_{n-1,n-1}x^{n-1}.
\end{aligned}
$$

Die notwendige Bedingung dafür, daß das Polynom $f(x)$ in $K_\pi(\vartheta)$ in ein Produkt von in $K_\pi(\vartheta)$ irreduziblen Polynomen der Grade $l_1, l_2, \ldots, l_r$ zerlegbar sei, ist, daß man die charakteristische Gleichung dieser Substitution d. h.

$$
\begin{vmatrix}
1-\lambda, & 0, & \ldots, & 0 \\
\gamma_{10}, & \gamma_{11}-\lambda, & \ldots, & \gamma_{1,n-1} \\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\
\gamma_{n-1,0}, & \gamma_{n-1,1}, & \ldots, & \gamma_{n-1,n-1}-\lambda
\end{vmatrix} = 0
$$

in der Gestalt $(\lambda^{l_1} - 1) \cdot (\lambda^{l_2} - 1) \ldots (\lambda^{l_r} - 1) = 0$ schreiben kann. Diese Bedingung ist auch hinreichend, falls keine identische Gleichheit $(\lambda^{l_1} - 1) \ldots (\lambda^{l_r} - 1) = (\lambda^{l'_1} - 1) \ldots (\lambda^{l'_{r'}} - 1)$ besteht, in der die Menge der ganzen Zahlen $(l_1, \ldots, l_r)$ nicht mit der Menge $(l'_1, \ldots, l'_{r'})$ identisch ist. Dies gilt insbesondere, wenn $p > n$, wo p diejenige rationale Primzahl bedeutet, deren Teiler π ist.

Den Beweis führen wir nicht explicite durch, da er mit dem Beweise des Satzes von Herrn Prof. Petr übereinstimmt, mit der einzigen Modifikation, daß es hier nötig ist sich des Satzes 4 zu bedienen, statt eines formal einfacheren Satzes, mit welchem wir in dem dort betrachteten Spezialfalle bereits auskommen.

III.

a)

Das Produkt der Linearfaktoren $f_1(x)$ von $f(x)$ ist der größte gemeinsame Teiler von $f(x)$ und $x^{N(\pi)} - x$. Es gilt

$$f(x) = f_1(x) \cdot h_1(x),$$

wo $h_1(x)$ nur irreduzible Faktoren mindestens 2-ten Grades enthält. Der g. g. Teiler von $h_1(x)$ und $x^{N(\pi)^2} - x$ gibt das Produkt von irreduziblen Bestandteilen zweiten Grades usw. So erhält man sukzessiv

$$f(x) = f_1(x) \cdot f_2(x) \ldots f_k(x),$$

wo $f_h(x)$ nur Polynome h-ten Grades als irreduzible Teiler besitzt.

[Bemerkung. Was die Berechnung des g. g. Teilers anbelangt, verfahren wir folgendermaßen. Durch sukzessive Potenzierung berechnen wir

$$x^{N(\pi)^h} = \delta_1 x^{n-1} + \delta_2 x^{n-2} + \ldots + \delta_n$$

und suchen dann den größten gemeinsamen Teiler von $f(x)$ und $\delta_1 x^{n-1} + \ldots + (\delta_{n-1} - 1)\, x + \delta_n$. Siehe übrigens Abschnitt IV der genannten Arbeit.]

b)

Es bleibt uns also nur die Aufgabe übrig, das Polynom $f_h(x)$ (sein Grad sei m) in Polynome h-ten Grades zu zerlegen. Es ist $m = h \cdot l$, wo l die Anzahl der irreduziblen Bestandteile bedeutet.

Die Wurzeln von $f_h(x)$ lassen sich in folgenden Reihen darstellen

$$\begin{gathered} j_1,\ j_1^{N(\pi)},\ j_1^{N(\pi)^2},\ \ldots,\ j_1^{N(\pi)^{h-1}} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ j_l,\ j_l^{N(\pi)},\ j_l^{N(\pi)^2},\ \ldots,\ j_l^{N(\pi)^{h-1}} \end{gathered}$$

Die Wurzeln in einzelnen Zeilen gehören denselben irreduziblen Faktoren an.

Wir wählen eine beliebige ganze symmetrische Funktion $\Phi(t_1, \ldots, t_h)$ der Größen $t_1, \ldots, t_h$. Wenn wir $t_1, \ldots, t_h$ durch die Wurzeln z. B. der ersten Reihe ersetzen, wird der Ausdruck $\Phi(j_1, \ldots, j_1^{N(\pi)^{h-1}})$ Funktion einer einzigen Veränderlichen j_1, die wir durch $F(j_1)$ bezeichnen wollen.

Offenbar gilt

$$\begin{gathered} u_1 = F(j_1) = F(j_1^{N(\pi)}) = \ldots = F(j_1^{N(\pi)^{h-1}}). \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_l = F(j_l) = F(j_l^{N(\pi)}) = \ldots = F(j_l^{N(\pi)^{h-1}}). \end{gathered}$$

Die Größen $u_1, u_2, \ldots, u_l$ sollen der Gleichung

$$g(u) = u^l + g_1 u^{l-1} + \ldots + g_l = 0 \tag{5}$$

genügen. Den Wert der Koeffizienten g_i können wir in $K_\pi(\vartheta)$ berechnen, da für die λ-ten Potenzsummen [x_i sind die Wurzeln von $f_h(x) = 0$]

$$u_1^\lambda + u_2^\lambda + \ldots + u_l^\lambda = \frac{1}{h}\{F^\lambda(j_1) + \ldots + F^\lambda(j_1^{N(\pi)^{h-1}})\} +$$

$$+ \frac{1}{h}\{F^\lambda(j_2) + \ldots + F^\lambda(j_2^{N(\pi)^{h-1}})\} + \ldots =$$

$$= \frac{1}{h}\{F^\lambda(x_1) + F^\lambda(x_2) + \ldots + F^\lambda(x_m)\}, \quad (\lambda = 1, 2, \ldots, l) \qquad (6)$$

gilt und die Ausdrücke (6) kann man, als symmetrische Funktionen der Wurzeln der Gleichung $f_h(x)$ aus $K_\pi(\vartheta)$, wirklich berechnen.

Dabei ist wesentlich, daß alle Wurzeln der Gleichung (5) Elemente aus $K_\pi(\vartheta)$ sind; $f_h(x)$ ist nämlich nach der Voraussetzung in ein Produkt von irreduziblen Polynomen h-ten Grades zerlegbar und $u_1 = F(j_1), \ldots$ usw. sind symmetrische Funktionen der Wurzeln einzelner Faktoren, also aus $K_\pi(\vartheta)$.

Wir können also die u_i als bekannt annehmen.

Durch geeignete Wahl der Funktion F ist es stets möglich zu erreichen, daß die Größen $u_1, \ldots, u_l$ voneinander verschieden sind. Es genügt z. B. bei unbestimmten t die Funktion in der Gestalt

$$u_\varrho = (t - j_\varrho) \ldots (t - j_\varrho^{N(\pi)^{h-1}})$$

zu wählen; denn die Gleichung $u_\varrho = u_\tau$ kann nur dann bestehen, wenn alle $j_\varrho, \ldots$ mit $j_\tau, \ldots$ identisch sind, was nur für $\varrho = \tau$ der Fall ist.

Wir zeigen nun, daß durch die Bestimmung der Größen u_i $(i = 1, \ldots, l)$ aus $K_\pi(\vartheta)$ das Problem der Faktorzerlegung schon als gelößt angesehen werden kann.

Es ist zweierlei Verfahren möglich.

α) Das Polynom $F(x) - u_i$ und das gegebene Polynom $f_h(x)$ haben die Wurzeln $j_i, \ldots, j_i^{N(\pi)^{h-1}}$ gemein, und falls u_i eine einfache Wurzel von $g(x)$ ist, nur diese. Darum gibt der g. g. Teiler von $f(x)$ und $F(x) - u_i$ die gesuchten irreduziblen Faktoren.

β) Oft ist das folgende Verfahren bequemer.

Wir behaupten: Wird eine beliebige symmetrische Funktion $S(j_\varrho, \ldots, j_\varrho^{N(\pi)^{h-1}}) = \varphi(j_\varrho)$ gewählt, dann ist diese durch die Größe $u_\varrho = F(j_\varrho)$ rational ausdrückbar und es ist also möglich ihren Wert in $K_\pi(\vartheta)$ anzugeben.

Beweis: Wir konstruieren den Ausdruck

$$H(u) = \frac{\varphi(j_1)}{u - F(j_1)} + \frac{\varphi(j_2)}{u - F(j_2)} + \ldots + \frac{\varphi(j_l)}{u - F(j_l)} = \frac{1}{h}\sum_{i=1}^{m}\frac{\varphi(x_i)}{u - F(x_i)},$$

wo die Summe sich auf alle Wurzeln der gegebenen Gleichung $f_h(x) = 0$ bezieht. Die rechte Seite zeigt, daß dieser Ausdruck eine gebrochene symmetrische Funktion der Wurzeln des gegebenen Polynoms ist und er wird zu einer ganzen Funktion $G(u)$ mit bekannten Koeffizienten aus $K_\pi(\vartheta)$, wenn wir ihn mit dem Polynome (5) multiplizieren; also

$$G(u) = g(u) \cdot \left[\frac{\varphi(j_1)}{u - F(j_1)} + \ldots + \frac{\varphi(j_l)}{u - F(j_l)} \right]. \qquad (7)$$

Wir setzen $u = u_\varrho = F(j_\varrho)$ ein und erhalten $\varphi(j_\varrho) = \frac{G(u_\varrho)}{g'(u_\varrho)}$, wo der Strich die Ableitung nach u bezeichnet. Damit ist der Satz bewiesen.

Wir wählen nun, der Reihe nach, statt der Funktion S die elementarsymmetrischen Funktionen der Größen $j_\varrho, \ldots, j_\varrho^{N(\pi)^{h-1}}$; so erhält man die Koeffizienten jenes der irreduziblen Faktoren, der gerade diese Größen als Wurzeln besitzt. Dies führen wir für jedes ϱ durch, erhalten so alle irreduziblen Faktoren und das Polynom $j_h(x)$ ist in Polynome h-ten Grades zerlegt.

Zusatz. Wir führen folgende Bezeichnung ein: Ein Polynom nennen wir normiert, wenn der Koeffizient seiner höchsten Potenz gleich 1 ist. Nach dem Vorhergehenden ist es evident, daß die Faktorzerlegung von $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ in $K_\pi(\vartheta)$ in lauter normierte Polynome möglich ist.

Zweiter Teil.

Wir zeigen nun, wie die Überlegungen des ersten Teiles die Zerlegung der Polynome im Körper der rationalen Zahlen K, resp. in irgendeiner algebraischen Erweiterung desselben, ermöglichen.

I.

Wir brauchen zwei Hilfssätze.

Hilfssatz A. Hat das Polynom $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ *(im Körper aller komplexen Zahlen) einen Faktor r-ten Grades* $(1 \leqq r \leqq n)$, *so sind die Koeffizienten desselben, dem absoluten Betrage nach, nicht größer als die Zahl* $D_r = Min\ (B_r, C_r)$, wo

$$B_r = 2^r \cdot \sqrt[r]{|\alpha_0|^2 + \ldots + |\alpha_n|^2} \leqq 2^r \{|\alpha_0| + \ldots + |\alpha_n|\}, \quad 1 \leqq r \leqq n$$

$$C_r = \{|\alpha_0| + \ldots + |\alpha_n|\}, \text{ für } r = n,\ n-1,$$

$$C_r = \{|\alpha_0| + \ldots + |\alpha_n|\} \cdot n \cdot (n-1) \ldots (r+2),$$

für $1 \leqq r \leqq n-2$.

Beweis. 1. Die Koeffizienten der Faktoren von $f(x) = \alpha_0 (x - x_1) \ldots (x - x_n)$ sind dem absoluten Betrage nach höchstens gleich denjenigen von $f(x) = |\alpha_0| \cdot (x + |x_1|) \ldots (x + |x_n|)$. Also der Faktor r-ten Grades, dessen Nullpunkte

$x_{\nu_1}, \ldots, x_{\nu_r}$ sind, hat die Koeffizienten höchstens gleich $|\alpha_0| \cdot (1 + |x_{\nu_1}|) \ldots (1 + |x_{\nu_r}|)$. Dieses Produkt kann nun nach einer Methode von J. Schur (siehe Pólya-Szegö: Aufgaben II. S. 265) abgeschätzt werden, und wir erhalten gerade die genannte Zahl B_r.

2. Die Zahl C_r (die für höhere r günstiger ist) erhalten wir folgendermaßen. Ist α ein Nullpunkt von $f(x)$, so ist $f(x) = (x - \alpha) \cdot g(x)$ und die Koeffizienten von $g(x)$, also des Quotienten $\frac{f(x)}{x - \alpha}$ sind der Reihe nach gleich α_0, $\alpha_0\alpha + \alpha_1$, $\alpha_0\alpha^2 + \alpha_1\alpha + \alpha_2, \ldots$ Ist $|\alpha| \leqq 1$, so sind sie höchstens gleich $\sum_i |\alpha_i|$. Ist $|\alpha| > 1$, so folgt aus $f\left(\frac{1}{y}\right) = \left(\frac{1}{y} - \alpha\right) \cdot g\left(\frac{1}{y}\right)$ nach Umformung — da nun $\left|\frac{1}{\alpha}\right| < 1$ — dasselbe Resultat. Spalten wir nun von $g(x)$ nacheinander die einzelnen Linearfaktoren ab, so erhalten wir als obere Abschätzung für den absoluten Betrag der Koeffizienten des gebliebenen Polynoms die Zahl C_r.

Bemerkung. Zerfällt also $f(x)$ beliebig, so sind die Koeffizienten der einzelnen Faktoren dem absoluten Betrage nach nicht größer als die Zahl $D = \operatorname{Max} D_r$ $(r = 1, \ldots, n)$.

Hilfssatz B. Es sei $f(x)$ ein normiertes Polynom in $K(\vartheta)$. Es sei (π) Hauptideal, wo π eine unzerlegbare Zahl ist, die das Ideal erzeugt. π sei kein Teiler der Diskriminante von $f(x)$. Ist die Zerlegung des Polynoms $f(x) \pmod{\pi}$ in normierte irreduzible Faktoren bekannt, so ist es immer möglich durch rationale Operationen seine eindeutige normierte Zerlegung $\pmod{\pi^2}$ anzugeben.

Der Beweis gibt gleich das Konstruktionsverfahren.

Die Zerlegung von $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ in normierte irreduzible Faktoren sei

$$f(x) \equiv f_1(x) \ldots f_k(x) \pmod{\pi}$$

d. h.

$$f(x) = f_1(x) \ldots f_k(x) + \pi \cdot \varphi(x).$$

[$\varphi(x)$ bedeutet ein Polynom aus $K(\vartheta)$, dessen Grad kleiner als der Grad von $f(x)$ ist.] Bekanntlich gibt es k Polynome $\varphi_1(x), \varphi_2(x), \ldots, \varphi_k(x)$ [der Grad von $\varphi_\nu(x)$ ist kleiner als der Grad von $f_\nu(x)$], die folgender Relation genügen:

$$\frac{\varphi(x)}{f_1 \cdot f_2 \ldots f_k} \equiv \frac{\varphi_1}{f_1} + \frac{\varphi_2}{f_2} + \ldots + \frac{\varphi_k}{f_k} \pmod{\pi}.$$

[Partialbruchzerlegung von $\frac{\varphi(x)}{f_1 \cdot f_2 \ldots f_k}$ in $K_\pi(\vartheta)$; die φ_ν sind

(mod π) eindeutig bestimmt; dabei ist nötig, daß alle f_k voneinander verschieden seien; durch Voraussetzung über π und der Diskriminante ist dies gesichert.]

Dann gilt aber

$$f(x) \equiv (f_1 + \pi\varphi_1) \cdot (f_2 + \pi\varphi_2) \ldots (f_k + \pi\varphi_k). \pmod{\pi^2} \qquad (*)$$

Denn, um diese Identität zu beweisen, genügt es an der linken Seite $f = f_1 \ldots f_k + \pi\varphi$ zu schreiben und an der rechten Seite ausmultiplizieren. Da sich die Ausdrücke $f_1 \cdot f_2 \ldots f_k$ wegheben, kann man durch π teilen, womit man zu der identisch geltenden Partialbruchzerlegung gelangt.

Aus der Gestalt von (*) sieht man, daß die Faktoren normiert bleiben.

Ähnlich — da wir die Zerlegung (mod π^2) schon kennen — kann man die Zerlegung von $f(x)$ (mod π^3) usw. bestimmen.[2])

II.

Wir betrachten in $K(\vartheta)$ das Polynom $f(x) = x^n + \alpha_1 x^{n-1} + + \alpha_2 x^{n-2} + \ldots + \alpha_n$ (mit ganzen algebraischen Koeffizienten), das eine von Null verschiedene Diskriminante besitzt.

Wir wählen ein beliebiges Primideal (π) aus $K(\vartheta)$, welches ein Hauptideal ist — also π ganz algebraisch — für praktische Zwecke am bequemsten eine rationale Primzahl, die in dem betrachteten Körper unzerlegbar ist. π soll nicht die Diskriminante teilen.

Die Zerlegung von $f(x)$ in normierte irreduzible Faktoren (mod π) sei

$$f(x) \equiv f_1(x) \cdot f_2(x) \ldots f_m(x) \pmod{\pi}. \qquad (8)$$

Wir konstruieren nun, von (8) ausgehend, die Zerlegung mod π^2, $\pi^3, \ldots, \pi^k$ so weit, bis $|\pi^k| > 2D$ (π ist eine ganze alg. Zahl, $|\pi| > 1$)

$$f(x) \equiv f^*_1(x) \cdot f^*_2(x) \ldots f^*_m(x) \pmod{\pi^k}.$$

Ich behaupte: ist das Polynom $f(x)$ in $K(\vartheta)$ in m Faktoren zerlegbar, so müssen die Polynome $f^*_h(x)$ ($h = 1, \ldots, m$) [wo wir

[2]) Die Zerlegung (*) ist eindeutig; denn wäre $f \equiv f'_1 \cdot f'_2 \ldots f'_{k'}$ (mod π^2) eine andere Zerlegung, so wäre auch $f \equiv f'_1 \ldots f'_{k'}$ (mod π) und nun hat man aus der Eindeutigkeit der Zerlegung $f \equiv f_1 \cdot f_2 \ldots f_k$ (mod π): $k = k'$; $f_1 \equiv f'_1, \ldots, f_k \equiv f'_k$ (mod π) d. h. $f'_1 = f_1 + \pi\varphi_1$ usw., und die Zahlen $\varphi_1, \ldots$ usw. sind eindeutig bestimmt.

Es sei bemerkt, daß die Zerlegung eines Polynoms nach einem Primzahlpotenzmodul (also auch π^ν, $\nu > 1$) in irreduzible Faktoren im allgemeinen nicht eindeutig sein muß. Wohl aber in unserem Falle, wo wir die Polynome normiert denken und wo keine mehrfachen Faktoren existieren ist die Eindeutigkeit erfüllt. Den allgemeinen Fall siehe bei Oynstein Ore im III. B. der „Algebra“ von Fricke.

uns die Koeffizienten an die „absolut kleinsten Reste“ (mod π^k) reduziert denken], mit den normierten Faktoren der Zerlegung des gegebenen Polynoms in $K(\vartheta)$ übereinstimmen. Denn die Grade der Faktoren sind dann notwendig gleich und was die Koeffizienten anbelangt, unterscheiden sich die Koeffizienten von $f^*_h(x)$ von den Koeffizienten der eventuellen Faktoren von $f(x)$ nur um ein Vielfaches $\gamma \,.\, \pi^k$, wo γ eine ganze Zahl ist; da aber $|\, \gamma\pi^k \,| > 2 \,|\, \gamma \,|\, . D$, muß $\gamma = 0$, da sonst der Faktor einen Koeffizienten hätte, der dem absoluten Betrage nach größer als D wäre, was aber nach Satz A als unmöglich gefunden wurde. Dabei wird der Begriff des „absolut kleinsten Restes“ im Sinne des absoluten Betrages einer komplexen Zahl gemeint.

Es ist wohl möglich, daß das Polynom in $K(\vartheta)$ weniger als m Faktoren besitzt. Auch in diesem Falle kommen in erster Reihe die Polynome $f^*_1, f^*_2, \ldots, f^*_m$ in Betracht. Irgend eines von ihnen könnte Teiler von $f(x)$ sein. Nun konstruieren wir weiter die Polynome $f^*_i \,.\, f^*_k$, reduzieren sie (mod π^k) an absolut kleinsten Reste, dann sind dies wieder mögliche Faktoren. Denn das so gebaute Polynom kann in $K(\vartheta)$ irreduzibel sein, aber zufällig (mod π) zerfällt es und wird darum in der Zerlegung (mod π^k) durch zwei Polynome vertreten. So fahren wir fort. Es ist also nötig, folgende Polynome zu konstruieren und zu untersuchen [die stets an absolut kleinsten Reste (mod π^k) reduziert gemeint sind]:

$$\begin{aligned} &\text{Polynome } f^*_i \text{ der Anzahl } \binom{m}{1}, \\ &\text{„} \qquad f^*_i \,.\, f^*_k \text{ der Anzahl } \binom{m}{2}, \\ &\text{„} \qquad f^*_i \,.\, f^*_k \,.\, f^*_l \text{ der Anzahl } \binom{m}{3}. \end{aligned} \tag{9}$$

usw.

Wir haben also $2^m - 2$ Polynome, die als einzige mögliche Faktoren in Betracht kommen, wodurch die Aufgabe an wenig Proben reduziert wird (es genügt schon $2^{m-1} - 2$), die in der Praxis vielfach unnötig sind, da wir aus den Graden, Absolutgliedern usw. die Antwort nach der Frage über die Reduzibilität gleich bekommen.

Zusatz. Wir betrachteten bis jetzt nur Polynome mit dem höchsten Koeffizienten 1. Sei nun dieser gleich der Zahl α_0. Wir multiplizieren das gegebene Polynom mit der Zahl α, wo $\bar{\alpha}\alpha_0 \equiv 1 \pmod{\pi}$. Wie im Vorgehenden zerlegen wir $\bar{\alpha} \,.\, f(x)$ mod $\pi, \pi^2 \ldots$ Die Untersuchung ändert sich nur in dem Sinne, daß nun außer den Polynomen (9) auch diejenigen Polynome zu

untersuchen sind, die aus ihnen durch Multiplizieren mit jedem Teiler der Zahl α_0 entstehen. Solcher Zahlen gibt es im Sinne der Teilbarkeit nur endlich viele, so daß die Anzahl der Polynome endlich bleibt.

Beispiele.

Einige Beispiele sollen zur Erläuterung dienen.

1. Es soll im Körper der Restklassen (mod 5) K_5 das folgende Polynom zerlegt werden, von welchem bekannt ist (wie man nach II oder IIIa erkennt), daß es in K_5 in drei Polynome zweiten Grades zerlegbar ist.

$$f_1(x) = x^6 + x^5 + x^4 + x^3 + 3x^2 + 4x + 2. \tag{10}$$

Hier ist $\pi = p = 5$ und da wir im Ringe der ganzen rationalen Zahlen uns befinden $N(\pi) = p = 5$.

Wir wählen in IIIb die Funktion $\Phi(t_1, t_2) = t_1 \,.\, t_2$, $F(j) = j \,.\, j^5 = j^6$. Die Größen $u_i = F(j_i)$ (es ist klar, daß sie die Absolutglieder der gesuchten Faktoren darstellen), genügen wegen

$$u_1^{\lambda} + u_2^{\lambda} + u_3^{\lambda} = \tfrac{1}{2} s_{6\lambda} \quad (\lambda = 1, 2, 3)$$

der Gleichung $g(u) = u^3 + 2u^2 + 4u + 3$, also $u_1 = 1$, $u_2 = 3$, $u_3 = 4$. [Die Potenzsummen sind aus (10) durch sukzessive Potenzierung leicht zu finden.] Der größte g. Teiler von (10) und $x^6 - 1$, $x^6 - 3$, $x^6 - 4$ gibt der Reihe nach die gesuchten Faktoren.

Hier ist es aber vorteilhaft, nach der zweiten Methode zu verfahren.

Um den negativ genommenen Koeffizienten v_i bei x zu finden, schreiben wir $\varphi(x) = x + x^5$

$$H(x) = \frac{1}{2} \sum_{i=1}^{6} \frac{x_i + x_i^5}{u - x_i^6} = \frac{1}{2} \sum_{i=1}^{6} \frac{x_i + x_i^5}{u} \cdot \left\{ 1 + \frac{x_i^6}{u} + \frac{x_i^{12}}{u^2} + \ldots \right\}.$$

Den periodischen Charakter der Potenzsummen s_k betrachtend (auf die ausführliche Untersuchung dieser Periodizität gehen wir nicht ein), erhalten wir vier geometrische Reihen und durch Summieren

$$H(u) = \frac{s_1 u^3 + s_7 u^2 + s_{13} u + s_{19}}{u^4 - 1}.$$

Weiter

$$G(u) = (u^3 + 2u^2 + 4u + 3) \,.\, \frac{4u^3 + 3u^2 + 4u + 3}{u^4 - 1},$$

schließlich

$$v = \frac{G(u)}{g'(u)} = \frac{-u^2 + u + 1}{3u^2 + 4u + 4}.$$

Wenn man nun $u_1 = 1$ einsetzt, bekommt man $v_1 = -4$; für $u_2 = 3$, $v_2 = 0$; für $u_3 = 4$ ist $v_3 = -2$.

Es ist also

$$f_1(x) = (x^2 + 4x + 1) \cdot (x^2 + 3) \cdot (x^2 + 2x + 4).$$

Bemerkung. Ähnlich findet man allgemein, bei der Wahl

$$\Phi(t_1, \ldots, t_h) = t_1 \cdot t_2 \ldots t_h, \; F(j) = j^q, \; q = \frac{p^h - 1}{p - 1}$$

für den Ausdruck, der zu dem negativ genommenen Koeffizienten bei x^{h-1} gehört

$$G(u) = g(u) \cdot \frac{s_1 u^{p-2} + s_{1+q} u^{p-3} + \ldots + s_{1+(p-2)q}}{u^{p-1} - 1}.$$

Jedenfalls muß bei dieser Wahl von Φ die Gleichung $g(u)$ nicht alle Wurzeln verschieden haben und dann bekommen wir so nur einen Teil der Faktoren.

2. Es ist im Bereiche der ganzen Gausschen Zahlen das Polynom

$$f_2(x) = x^3 + (1 - i)\, x^2 + (5 - i)\, x - (1 + 8i) \qquad (11)$$

zu zerlegen.

Als Modul wählen wie die rationale Primzahl $\pi = 3$. Diese ist bekanntlich auch im Ringe der ganzen Gausschen Zahlen unzerlegbar. $N(3) = 0$. Die Klassen mod 3 sind $a + bi$, $a, b = 0, \pm 1$. (Wir nehmen die absolut kleinsten Reste.) Um zu erfahren, wie (11) (mod 3) zerfällt, berechnen wir aus (11) sukzessiv die Potenzen

$$\begin{aligned} x^3 &\equiv (i - 1)\, x^2 + (i + 1)\, x + (1 - i) \\ x^4 &\equiv (1 - i)\, x^2 + (-1 - i)\, x - i \\ x^8 &\equiv x + (i - 1) \qquad \pmod 3 \\ x^9 &\equiv x^2 + (i - 1)\, x \\ x^{18} &\equiv (1 - i)\, x^2 + (1 - i)\, x. \end{aligned}$$

Die charakteristische Gleichung

$$\begin{vmatrix} 1 - \lambda & 0 & 0 \\ 0 & i - 1 - \lambda & 1 \\ 0 & 1 - i & 1 - i - \lambda \end{vmatrix} \equiv (1 - \lambda)\,(\lambda^2 - 1) \pmod 3$$

zeigt, daß (11) (mod 3) in einen Faktor ersten und zweiten Grades zerfällt.

Der Linearfaktor ist der größte g. Teiler von (11) und $x^9 - x \equiv$ $\equiv x^2 + (i + 1)\, x$, also der Ausdruck $x + i + 1$.

Den Faktor zweiten Grades erhält man durch Dividieren

$$f_2 \equiv (x + i + 1) \cdot (x^2 + ix + i). \pmod 3$$

Um die Zerlegung in $K(i)$ zu finden, genügt es, die Zerlegung nach

einem solchen mod 3^k zu bestimmen, daß

$$3^k > 2\Sigma\,|\,\alpha_i\,| = 2\,(1 + \sqrt{2} + \sqrt{26} + \sqrt{65}),$$

also $k = 4$.

Wir versuchen die Ausdrücke α, $\beta x + \gamma$ so zu bestimmen, damit

$$x^3 + (1 - i)\,x^2 + (5 - i)\,x - (1 + 8i) \equiv$$
$$\equiv (x + i + 1 + 3\alpha)\,.\,[x^2 + ix + i + 3\,(\beta x + \gamma)] \pmod{3^2}$$

sei.

Dies führt zu der Relation

$$\frac{-ix^2 + (2 - i)\,x - 3i}{(x + i + 1)\,.\,(x^2 + ix + i)} \equiv \frac{\alpha}{x + i + 1} + \frac{\beta x + \gamma}{x^2 + ix + i} \pmod 3$$

und daraus $\alpha = -i$, $\beta = 0$, $\gamma = 1 - i$.
Also

$$f_2 \equiv (x + 2i + 1)\,(x^2 + ix + 3 - 2i) \pmod{3^2}. \qquad (12)$$

(Wir reduzieren die Koeffizienten an absolut kleinste Reste $a + bi$, $a, b = 0, \pm 1, \ldots, \pm 4$). Wenn wir nun die Zerlegung (mod 3^3) bestimmen, so bekommen wir ebenfalls das Ergebnis von (12), weil das Produkt der beiden Faktoren gerade (11) gibt.

Wir haben hier also die Zerlegung gleich bei erstem Schritte gefunden und in (12) kann man direkt Gleichheit — die in $K(i)$ gilt — schreiben, womit unsere Aufgabe gelößt ist.

3. Es ist in $K(\sqrt{-3})$ das Polynom

$$f_3 = 2x^3 + (5\sqrt{-3} - 1)\,x^2 + (-1 - \sqrt{-3})\,x + (-4 + 2\sqrt{-3}) \qquad (13)$$

zu zerlegen.

Jede ganze Zahl des Körpers ist der Gestalt $a + b\omega$, $\omega = \frac{1 + \sqrt{-3}}{2}$, a, b ganz rational. Wir führen deswegen $\sqrt{-3} = 2\omega - 1$ ein. Die Größe ω erfüllt $\omega^2 - \omega + 1 = 0$. Das Polynom (13) geht in

$$f_3 = 2\,[x^3 + (5\omega - 3)\,x^2 - \omega x + (2\omega - 3)]$$

über. Als Modul wählen wir $\pi = 5$. [Nach den bekannten Eigenschaften des quadratischen Körpers ist klar, daß (5) hier ein Primideal ist.] $N(5) = 25$.

Aus dem Polynome

$$\overline{f}_3 = x^3 + (5\omega - 3)\,x^2 - \omega x + (2\omega - 3) \qquad (13a)$$

erhält man durch sukzessives Potenzieren (mod 5), mit Berücksichtigung von $\omega^2 = \omega - 1$,

$$
\begin{aligned}
x^3 &\equiv 3x^2 + \omega x + (3 - 2\omega)\\
x^4 &\equiv (\omega - 1)\,x^2 + (\omega + 3)\,x + (4 + 4\omega)\\
x^8 &\equiv (3\omega + 4)\,x^2 + (1 - \omega)\,x + (2\omega - 3) \pmod 5\\
x^{16} &\equiv (2\omega + 1)\,x^2 + (\omega - 1)\,x + (3\omega + 2)\\
x^{24} &\equiv 1.
\end{aligned}
$$

Daraus geht gleich hervor, daß $\overline{f}_3 \pmod 5$ in drei Linearfaktoren zerfällt. Von den Größen $a + b\omega$, a, $b = 0, \pm 1, \pm 2$ genügen die folgenden drei der Gleichung (13a)

$$2\omega + 2,\ -\omega,\ -\omega + 1.$$

Also

$$\overline{f}_3 \equiv (x + \omega)\,.\,(x + \omega - 1)\,.\,(x - 2\omega - 2) \pmod 5.$$

Die Summe der Absolutbeträge der Koeffizienten von (13) ist < 20, es genügt also die Zerlegung (mod 5^2) und (mod 5^3) zu bestimmen. Wir setzen

$$\overline{f}_3 \equiv (x + \omega + 5\alpha)\,.\,(x + \omega - 1 + 5\beta)\,.\,(x - 2\omega - 2 + 5\gamma) \pmod{5^2},$$

durch Einsetzen von (13a)

$$
\frac{\omega x^2 + (\omega - 1)\,x - 1}{(x + \omega)\,(x + \omega - 1)\,(x - 2 - 2\omega)} \equiv \frac{\alpha}{x + \omega} + \frac{\beta}{x + \omega - 1} + \frac{\gamma}{x - 2\omega - 2} \pmod 5,
$$

$$\alpha = 2\omega,\ \beta = 0,\ \gamma = 4\omega,$$

$$\overline{f}_3 \equiv (x + 11\omega)\ \ (x + \omega - 1)\ \ (x - 7\omega - 2) \pmod{25}.$$

Es sei weiter

$$\overline{f}_3 \equiv (x + 11\omega + 25\alpha)\,.\,(x + \omega - 1 + 25\beta)\,.\,(x - 2 - 7\omega + 25\gamma); \pmod{5^3},$$

setzt man wieder (13a) ein

$$
\frac{(4\omega - 3)\,x - 1 - 3\omega}{(x + 11\omega)\,(x + \omega - 1)\,(x - 2 - 7\omega)} \equiv
$$

$$
\equiv \frac{\alpha}{x + 11\omega} + \frac{\beta}{x + \omega - 1} + \frac{\gamma}{x - 2 - 7\omega} \pmod 5,
$$

$$\alpha = 2\omega + 2,\ \beta = 0,\ \gamma = 3\omega - 2,$$

$$\overline{f}_3 \equiv (x + 61\omega + 50)\,.\,(x + \omega - 1)\,.\,(x - 57\omega - 52) \pmod{125}.$$

Diese Zerlegung zeigt gleich, daß der erste und dritte Faktor der rechten Seite nicht in Betracht kommen können, da der Absolutbetrag der Koeffizienten größer als 20 ist. Dagegen teilt der zweite Faktor, wie man sich durch Einsetzen überzeugt, das gegebene Polynom.

Den Teiler zweiten Grades bekommt man durch Dividieren, oder bequemer aus dem Polynome

$$(x + 61\omega + 50)(x - 57\omega - 52) = x^2 + (4\omega - 2)x - 9499\omega + 877$$

nach Reduktion (mod 125) an absolut kleinsten Reste, d. h.

$$x^2 + (4\omega - 2)x + (\omega + 2).$$

Wir haben also schließlich

$$f_3(x) = 2(x + \omega - 1) \cdot [x^2 + (4\omega - 2)x + (\omega + 2)].$$

4. Es ist im kubischen Körper $K(\vartheta)$, wo ϑ der Gleichung $\vartheta^3 + \vartheta + 1 = 0$ genügt, das Polynom

$$f_4 = 5x^2 + (1 - \vartheta + \vartheta^2)x + (3\vartheta - 2) \tag{14}$$

zu zerlegen.

Da die Diskriminante dieses Körpers $d = -31$ ist, kann die Basis der ganzen Zahlen in der Gestalt $1, \vartheta, \vartheta^2$ geschrieben werden. Die Zahl 2 ist zu d prim und $\vartheta^3 + \vartheta + 1$ (mod 2) irreduzibel, also ist 2 in $K(\vartheta)$ nach dem bekannten Satze unzerlegbar. Als Modul kann also 2 gewählt werden.

$$\begin{aligned} f_4 &\equiv x^2 + (1 + \vartheta + \vartheta^2)x + \vartheta \pmod 2. \\ x^2 &\equiv (1 + \vartheta + \vartheta^2)x + \vartheta \\ x^4 &\equiv \vartheta x + \vartheta \qquad\qquad \pmod{(2)} \\ x^8 &\equiv x + (1 + \vartheta + \vartheta^2). \end{aligned}$$

Daraus, da $x^{N(2)} = x^8$ nicht kongruent x ist, sieht man augenscheinlich, daß (14) — da es schon mod (2) irreduzibel ist — auch in $K(\vartheta)$ irreduzibel ist.

Bemerkung. Es ist selbstverständlich nicht notwendig als Modul eine rationale Primzahl zu wählen, wie wir es in den Beispielen getan haben. Es kann auch ein anderes Hauptideal gewählt werden; dies hat sogar den Vorteil, daß die Norm nicht zu hoch ausfällt. Der Nachteil ist hier aber die Konstruktion der absolut kleinsten Reste, die schließlich auch für eine rationale Primzahl, beim Körper höheren als zweiten Grades, genug mühsam sein kann. Im spezielen Falle des Körpers der rationalen Zahlen fallen natürlich alle Schwierigkeiten weg.

Zum Schluß möchte ich Herrn Prof. Dr. K. Petr für Anregung und Hilfe bei der Gestaltung dieser Arbeit meinen herzlichsten Dank sagen.

*