Zur Reduzibilität von Polynomen in der Kongruenztheorie

Von

S. Lubelski (Warszawa).

Mit der Frage der Reduzibilität eines quadratischen Polynoms hat sich Gauss[1]) beschäftigt; danach haben G. Rados [2]). Pólya-Szegö [3]) und M. Hall[4]) auf die Tatsache hingewiesen, dass man mit analytischen Hilfsmitteln ohne Schwierigkeit beweisen kann, dass ein quadratisches irreduzibles Polynom für unendlich viele primzahlige p modulo p irreduzibel ist. Diesen Satz verallgemeinern wir mit elementaren Mitteln folgendermassen:

Jedes Trinom ax^2+bx+c, *wo* $a, b\,c$ *ganzzahlig sind und* $d=b^2-4ac$ *keine negative Quadratzahl ist, hat unendlich viele Primteiler* $q \equiv -1 \pmod 4$. *Dabei existiert unterhalb* $\sqrt{D}$ *mindestens eine solche Zahl* q (s. Satz 1 und Folgerung).

Um den Satz I auf beliebige ganze rationale Polynome zu verallgemeinern und dabei auch notwendige und hinreichende Bedingungen für die Gültigkeit dieses Satzes in Bezug auf beliebige Polynome aufzustellen, bieten wir zunächst den Beweis eines Satzes

welcher der Permutationstheorie angehört (s. Hilfssatz 4).

---

[1]) Disquisitiones Arithmeticae, Art. 129.

[2]) G. Rados: Über Kongruenzbedingungen der rationalen Lösbarkeit von algebraischen Gleichungen, Math. Annalen 87 S. 78—81 (1922).

[3]) Pólya-Szegö: Aufgaben und Lehrsätze aus der Analysis II, Abschn. VIII, Aufgabe 100 (1925).

[4]) M. Hall: Quadratic Residues in Factorisation: Bull. Am. Math Soc. $39/10$ (1933) 758.

Von ihm ausgehend können wir den arithmetischen Teil der Bauerschen Sätze [5]) in fasslicherer Weise darstellen. Ferner erhalten wir

notwendige und hinreichende Bedingungen dafür, dass die Diskriminante einer Galoisschen Resolvente Quadrat eines Elementes des grundlegenden vollkommenen Körpers sein soll; bezw. ... , dass eine einfach transitive reguläre Gruppe zur alternierenden Gruppe gehören soll (s. Satz III und Folgerung),

aus welchen sich unmittelbar ein wichtiger Pellet-Stickelberg-Voronoï'scher Satz [6]) ergibt.

Die folgenden Erwägungen sind schon von analytisch algebraischen Methoden abhängig. Im Grunde fusst alles auf dem wohlbekannten Kroneckerschen Dichtigkeitssatz. Nach Hinweis auf die verschiedenartigen unmittelbaren Anwendungen dieses Satzes, bieten wir den Beweis des folgenden Satzes:

Dafür, dass ein ganzzahliges irreduzibles Polynom $f(x)$ höchstens endlich viele Primteiler $q \equiv -1 \pmod 4$ hat, ist es notwendig und hinreichend, dass $f(x)$ durch die Form $f_1(x)^2 + f_2(x)^2$ darstellbar sei, wo $f_1(x)$, $f_2(x)$ desgleichen ganzzahlige Polynome sind (s. Satz IV),

welcher als Verallgemeinerung eines Bauerschen Satzes [7]) angesehen werden kann.

§ 1.

Hilfssatz 1: *Mit endlich vielen Ausnahmen sind alle Primteiler der Form*

$$f(x,y) = a x^2 + b x y + c y^2, \quad d = b^2 - 4 a c = d_1^2 d_2.$$

wo a, b, c, d_1, d_2 beliebige ganze rationale Zahlen bezeichnen, auch Primteiler der Form

$$f_1(x) = x^2 - d_2;$$

und umgekehrt, sind alle Primteiler von $f_1(x)$ gleichzeitig auch Primteiler von $f(x,y)$.

[5]) M. Bauer: 1) Über einen Satz von Kronecker, Arch. d. Math. u. Physik, Dritte Reihe, 6 (1903), 218—9. 2) Über Kreisteilungsgleichungen ib. S. 220. 3) Über zusammengesetzte Körper ib. 220—221.

[6]) A. E. Pellet: Sur la décomposition d'une fonction entière mod p. Comptes Rendus, 86, 1878, 1071—2. G. Voronoï: Sur une propriété du discriminant des fonctions entières. Verh. d. III Math. Kongress. Heidelberg (Leipzig 1904).

[7]) s. z. B. E. Landau: Handbuch der Lehre von der Verteilung der Primzahlen. Leipzig und Berlin 1909. S. 440—2. Verallgemeinerung s. M. Bauer, Über die arithmetische Reihe, Journal f. Math. 131 (1906) S. 265—6.

Beweis. Es genügt zu beweisen, dass alle Primteiler der Form $f(x,y)$ mit endlich vielen Ausnahmen auch Primteiler der Form $a x^2 + b x + c$ sind.

Dies ergibt sich unmittelbar aus der Tatsache, dass für primzahliges p aus

$$f(x_0, y_0) \equiv 0 \pmod p, \quad (p, c\,y) = 1$$

die Kongruenz

$$a z^2 + b z + c \equiv 0 \pmod p, \quad z \equiv \frac{x}{y} \pmod p$$

entsteht.

Hilfssatz 2: *Ist*

$$f(x,y) = a x^2 + b x y + c y^2, \; a > 0,$$

eine binäre primitive quadratische Form und existieren solche ganze rationale Zahlen x_0, y_0, für welche

$$f(x_0, y_0) \equiv -1, -2, 3 \pmod 8, \tag{1}$$

so gibt es unendlich viele Primzahlen $q \equiv -1 \pmod 4$, für die, bei entsprechenden x_0, y_0, mit $(x_0, y_0) = 1$,

$$f(x_0, y_0) \equiv 0 \pmod q \tag{2}$$

[d. h. $f(x,y)$ hat unendlich viele Primteiler $q \equiv -1 \pmod 4$].

Beweis: Zunächst bemerken wir, dass man aus den Kongruenzen (1) ohne Schwierigkeit erhält, dass die Form $f(x,y)$ mindestens einen Primteiler $q \equiv -1 \pmod 4$ hat.

Es seien

$$q_1, \; q_2, \; \ldots, \; q_r, \; \ldots, \; q_t$$

alle Primteiler von $f(x,y)$, die $\equiv -1 \pmod 4$ sind. Da $f(x,y)$ primitiv ist, so findet man solche Zahlen ξ_r, η_r, für die

$$[f(\xi_r, \eta_r), q_r] = 1. \tag{3}$$

Eins der Paare $\xi_r = 1$, $\eta_r = 0$; $\xi_r = 0$, $\eta_r = 1$; $\xi_r = 1$, $\eta_r = 1$ erfüllt nämlich (3). Nun können wir Zahlen ξ, η finden, welche die Kongruenzen

$$\xi \equiv \xi_r \pmod{q_r}, \quad \eta \equiv \eta_r \pmod{q_r}$$

$$\xi \equiv x_0 \pmod 8, \quad \eta \equiv y_0 \pmod 8$$

erfüllen; dabei kann, da $a > 0$ ist, ξ in Bezug auf η so gross angenommen werden, dass $f(\xi, \eta) > 0$ ist.

Nun ist

$$f(\xi, \eta) \equiv f(x_0, y_0) \pmod 8,$$

und nach (2) hat also $f(x,y)$ noch einen Primteiler $q \equiv -1 \pmod 4$, welcher von den Primteilern (2) verschieden ist.

Hilfssatz 3: *Ist $D>0$, so hat x^2-D unendlich viele Primteiler q, derart dass*

(1) $$q \equiv -1 \pmod 4.$$

Beweis: Es genügt zu beweisen, dass x^2-D mindestens einen Primteiler von der Form (1) hat. Wäre nämlich q ein solcher Primteiler, so würde q durch eine binäre quadratische Form $ax^2+bxy+cy^2$ der Determinante $4D$ darstellbar sein, wo eine der Zahlen a, c offenbar >0 ist. Nach dem vorigen Hilfssatze, hat also $ax^2+bxy+cy^2$ unendlich viele solche Primteiler. Demnach wird auch x^2-D, nach Hilfssatz 1, unendlich viele solche Primteiler haben. Wenn D einen Primteiler $q \equiv -1 \pmod 4$ hat, ist demnach der Satz trivial. Für $D \equiv 1 \pmod 4$ wird

$$(2x_0)^2 - D \equiv -1 \pmod 4,$$

und für $D \equiv 2 \pmod 4$ wird

$$(2t+1)^2 - D \equiv -1 \pmod 4.$$

Da, nach Hilfssatz 2, D quadratfrei angenommen werden kann [also $(D, 4) \leqslant 2$], ist somit der Satz bewiesen.

Anmerkung: Dieser Satz ist übrigens eine unmittelbare Folgerung eines Bauerschen Satzes, welcher folgendermassen lautet:

„Es sei $\Phi(x) = c_0 x^n + \ldots + c_n$ eine ganzzahlige Funktion. Es möge die Gleichung $\Phi(x) = 0$ mindestens eine reelle Wurzel von ungerader Vielfachheit haben. Dann hat die Form Φ unendlich viele Primteiler $4y-1$" [7]).

Satz I: *Jedes Trinom ax^2+bx+c, wo a, b, c ganzzahlig sind und $d = b^2-4ac$ keine negative Quadratzahl ist, hat unendlich viele Primteiler $q \equiv -1 \pmod 4$.*

Beweis. Den Hilfssätzen 1 und 3 gemäss genügt es den Satz für quadratfreie $\frac{d}{4}$ zu beweisen. Ist $\frac{d}{4} \equiv 1 \pmod 4$, so hat die Zahl $\frac{d}{4}$, und demnach auch die Form x^2-d, einen Primteiler $q \equiv -1 \pmod 4$. Ist $\frac{d}{4} \equiv 2 \pmod 4$, so hat $(2t+1)^2 - \frac{d}{4}$ einen solchen Primteiler. Wir

können also $\frac{d}{4} \equiv -1 \pmod 4$ annehmen. In diesem Falle gehört aber $(-1)^{\frac{k-1}{2}}$ zum System der Charaktere einer binären quadratischen Form $f(x,y)$ der Determinante d, wobei $k = f(x,y)$ ist. Nun müssen die Charaktere für quadratfreies $\frac{d}{4}$ so angenommen werden, dass ihr Produkt gleich 1 sein soll, im übrigen können sie beliebige Werte ± 1 annehmen [8]). Es finden sich also für $\frac{d}{4} \equiv -1 \pmod 4$ solche binäre quadratische Formen, deren Charakter $(-1)^{\frac{k-1}{2}}$ gleich -1 ist. Gewisse Formen stellen also Zahlen k dar, für welche $(-1)^{\frac{k-1}{2}} \equiv -1$ ist d. h. $k \equiv -1 \pmod 4$ ist. Nach Hilfssatz 2 ist demnach der Satz bewiesen.

Folgerung 1. *Ist $0 < D \equiv 1 \pmod 8$, so findet man unterhalb der Zahl $\sqrt{D}$ eine Primzahl $q \equiv -1 \pmod 4$, welche Nichtrest mod D ist.*

Beweis. Gemäss Satz 1 findet sich mindestens eine Primzahl $q \equiv -1 \pmod 4$, für welche $\left(\frac{-D}{q}\right) = 1$ ist. Es sei $Q \equiv -1 \pmod 4$ die kleinste Primzahl, für welche

(1) $$z^2 + D \equiv 0 \pmod{2Q}$$

lösbar ist, und z_0 die kleinste natürliche Zahl, welche Lösung von (1) ist. Da

$$z_0^2 \equiv D \equiv 1 \pmod 8,$$

so ist $z_0^2 + D = 2QQ_1$, wo $Q_1 > 1$ einen Primteiler $q_1 \equiv -1 \pmod 4$ haben muss. Der Annahme gemäss ist $Q_1 \geqslant q_1 \geqslant Q$. Da $0 < z_0 < Q$ ist, so muss $Q^2 + D \geqslant 2Q^2$ sein, woraus $Q < \sqrt{D}$ folgt. Nun haben wir aus $\left(\frac{D}{Q}\right) = -1$, dass $\left(\frac{Q}{D}\right) = -1$ $\left[\left(\frac{Q}{D}\right)$ — Jacobisches Symbol$\right]$, d. h., dass Q Nichtrest von D ist.

Anmerkung. Gauss hat bewiesen [1]), dass für eine Primzahl $D \equiv 1 \pmod 8$ unterhalb $2\sqrt{D}+1$ ein Nichtrest liegt. W. Bock [9]) zeigte, dass diese Grenze auf $\sqrt{D}$ herabgesetzt werden kann.

[8]) E. Cahen: Théorie des nombres II, Paris 1924, S. 399—404, 554—557.

[9]) W. Bock. Zusatz zu dem Artikel 129 der Disquisitiones Arithmeticae von Gauss. Hamb. Mitt. 5 (1920) S. 307—309.

Folgerung 2: *Für jedes Trinom $f(x)=ax^2+bx+c$ (a, b, c ganzzahlig und $b^2-4ac=d$ keine Quadratzahl) existieren unendlich viele Primteiler $q\equiv -1 \pmod 4$, durch welche $f(x)$ nicht teilbar ist.*

Beweis. Nach Hilfssatz 1 genügt es den Satz für die Form x^2-d zu beweisen. Da alle Primteiler $q\equiv -1 \pmod 4$ von x^2+d keine Primteiler von x^2-d sind, so ist der Satz beweisen.

Anmerkung: Dieser Satz kann als Verallgemeinerung eines Satzes von Rados [2]) angesehen werden, welcher mittels des Dirichletschen Satzes über die arithmetische Progression bewiesen hat, dass $f(x)$ für unendlich viele Primzahlen p modulo p nicht zerlegbar ist, wenn nur d keine Quadratzahl ist (vgl. auch die (analytischen) Beweise von Pólya-Szegö [3]) und M. Hall [4])), d. h. dass wenn ein quadratisches Polynom $f(x)$ algebraisch irreduzibel ist, sich unendlich viele Pimzahlen p finden, für die $f(x)$ modulo p irreduzibel ist. Nun hat D. Hilbert [10]) an einem speziell konstruierten Beispiel gezeigt, dass Polynome vierten Grades existieren, welche modulo p stets reduzibel sind. Diese Eigenschaft haben, mit gewissen Ausnahmen, die Kreisteilungspolynome:

Satz II: *Jedes Kreisteilungspolynom $K_n(x)$, wo für primzahliges p und natürliches t:*

$$n\neq 2,\ 4,\ p^t,\ 2p^t,$$

ist für jede Primzahl P mit $(P, n)=1$ modulo P reduzibel.

Beweis. Ist für die Primzahl P und für die natürliche Zahl M

(1) $$P^M\equiv 1 \pmod n,$$

so ist das Polynom

$$x^{nM-1}-1$$

durch x^n-1 und demnach durch $K_n(x)$ teilbar. Ist m die kleinste natürliche Zahl, für welche (1) besteht, so ist $K_n(x)$ mod P durch irreduzible Polynome von höchstens m-ten Grade teilbar. Da die Zahlen $n\neq 2,\ 2,\ p^t,\ 2p^t$ keine Primitivwurzeln haben, so muss $m<\frac{\varphi(n)}{2}$ sein, wo $\varphi(n)$ die Eulersche Funktion bezeichnet. Demnach ist $K_n(x)$ mod P stets reduzibel.

§ 2.

Wir gehen jetzt zur Verallgemeinerung des Satzes I auf beliebige ganzzahlige Polynome über. Dazu beweisen wir zunächst einen Hilfssatz, welcher der Theorie der Permutationen angehört und welchen wir in unseren Erwägungen oft anwenden werden.

[10]) D. Hilbert: Über diophantische Gleichungen, Gött. Nachr. 1897, S. 53; Werke II 388—9; vgl. auch das Beispiel von A. Hurwitz, bei Pólya-Szegö [3]), Abschn. VIII, Aufg. 129.

Hilfssatz 4: *Dafür, dass die Ordnung m einer transitiven Permutationsgruppe G der Gradzahl n einer Permutation S von G gleich sein soll, ist es notwendig und hinreichend, dass jede Permutation S von G aus Zyklen von gleicher Ordnung bestehen soll.*

Beweis. Die Notwendigkeit der Bedingungen kann unmittelbar leicht eingesehen werden. Die transitive Gruppe G führt nämlich eine beliebige Ziffer k in eine beliebige andere über. Nehmen wir an, dass die Anzahl der Elemente von G der Anzahl der Ziffern gleich ist, so können nicht zwei verschiedene Permutationen die Ziffer k in ein und dieselbe Ziffer überführen. Da die Einheitspermutation keine Ziffer umstellt, so muss eine Permutation $S\neq 1$ jede Ziffer in eine andere überführen, d. h., S hat keine eingliedrige Zyklen. Es sei $S=C_1C_2\dots C_a$, wobei $C_1, C_2, \dots, C_a$ Zyklen sind, die keine gemeinsamen Ziffern haben. Ist r_k die Ordnung von C_k und ist z. B. $r_1\leqq r_k$, so erhalten wir

$$C_1^{r_1}C_2^{r_2}\dots C_a^{r_a}=S^{r_1}.$$

Da $C_1^{r_1}=1$, so hat S^{r_1} eingliedrige Zyklen, was nur dann möglich ist, wenn $S^{r_1}=1$. Dies tritt aber nur dann ein, wenn $r_1=r_2=\dots=r_k$ ist.

Um zu beweisen, dass die Bedingungen hinreichend sind, benutzen wir einen Jordanschen Satz [11]), welcher folgendermassen lautet:

Ist G transitiv, so gibt es mindestens $n-1$ Permutationen, welche alle Ziffern umstellen. Existieren in G mehr als $n-1$ solche Permutationen, so finden sich in G auch solche, welche weniger als $n-1$ Ziffern umstellen.

Nun ist, für transitives G, $n\leqq m$. Wäre also $n<m$, so gäbe es Permutationen $S\neq 1$, die gewisse Ziffern nicht umstellen. Da alle Zyklen von S von gleicher Ordnung sind, so muss $S=1$ sein, was unmöglich ist. Demnach ist $n=m$.

Wir weisen jetzt auf einen Dedekindschen Satz hin, welcher von wesentlicher Bedeutung bei diesen Erwägungen ist und der folgendermassen formuliert werden kann:

Dedekindscher Satz [12]): *Ist für ein ganzzahliges Polynom $f(x)$ und primzahliges p, das in der Diskriminante von $f(x)$ nicht aufgeht,*

$$f(x)\equiv f_1(x)f_2(x)\dots f_k(x) \pmod p,$$

[11]) C. Jordan: Journal de math. (2), 17, 1872, S. 351.

[12]) R. Dedekind: Zur Theorie der Ideale, Gött. Nachr. 1894.

wo $f_1(x), f_2(x), \ldots f_k(x)$ mod p irreduzibel und ihre Grade den natürlichen Zahlen $n_1, n_2, \ldots n_k$ entsprechend gleich sind, so enthält die Galoissche Gruppe von $f(x)$ eine Permutation, die aus Zyklen der Ordnungen $n_1, n_2, \ldots n_k$ besteht.

Anmerkung: Einen wesentlich neuen Beweis, welcher auf der Galoisschen Theorie von Schatunowskij-Loewy beruht, hat neuerdings N. Tschebotarëw [13]) geboten.

Schatunowskisches Prinzip [14]): Ist $\Phi(x_1, x_2, \ldots x_k)$ eine symmetrische ganze Funktion der Argumente $x_1, x_2, \ldots x_k$ mit ganzen rationalen Koeffizienten und ist für eine natürliche Zahl m

$$f(x) = (x-\xi_1)(x-\xi_2)\ldots(x-\xi_k) \equiv$$

$$\equiv (x-\eta_{i1})(x-\eta_{i2})\ldots(x-\eta_{ik}) \pmod m,$$

so ist

$$\Phi(\xi_1, \xi_2, \ldots \xi_k) \equiv \Phi(\eta_{i1}, \eta_{i2}, \ldots, \eta_{ik}) \pmod m.$$

Der Beweis ist klar., vgl. z. B. S. Lubelski: Zur Theorie der höheren Kongruenzen, Journal für Math. 162 (1930) S. 66—67.

Folgerung: *Sind $f(x)$ und $f_1(x)$ zwei ganzzahlige Polynome, so existieren unendlich viele Primzahlen p, für welche sich diese Polynome gleichzeitig* mod p *linear zerlegen.*

Beweis. Ist

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n, \qquad f_1(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m,$$

so erhalten wir: $a_0^{n-1} f(x) = \varphi(y)$ und $b_0^{m-1} f_1(x) = \varphi_1(y)$ sind ganzzahlige Polynome von y, wo $y = a_0 x$, bzw. $y = b_0 x$. Ist $\varphi(y)$ mod p, wo p eine gewisse in $a_0 b_0$ nicht aufgehende Primzahl ist, linear zerlegbar, so ist es auch $f(x)$. Wir können also annehmen, dass $a_0 = b_0 = 1$ ist. Offenbar können wir auch $f(x)$ und $f_1(x)$ als irreduzible Polynome annehmen. Es sei $K(\alpha)$ ein endlicher normaler Körper, welcher die Wurzeln von $f(x)$ und $f_1(x)$ enthält. Sind $x_1, x_2, \ldots x_k$ die Wurzeln von $f(x)$ und $x_1, x_2, \ldots x_g$ die Wurzeln von $f_1(x)$, so finden sich solche ganze rationale Polynome $\varphi(\alpha)$, $\psi(\alpha)$, für welche $x_1 = \varphi(\alpha)$, $x_1 = \psi(\alpha)$.

Es sei jetzt $F(x)$ das irreduzible Polynom, für welches $F(\alpha) = 0$ ist.

[13]) N. Tschebotarëw: Grundlagen der Galoisschen Theorie (russisch) Leningrad-Moskau 1934, S. 160—1.

[14]) S. O. Schatunowskij: Über die Bedingungen der Existenz von n verschiedenen Wurzeln einen Kongruenz n-ten Grades modulo primzahliges p (russisch), Bull. de la Soc. Phys.-Math. de Kasan (2) XII (1902), S. 33—49.

Sind $\alpha_1, \alpha_2, \ldots \alpha_k$ die verschiedenen Wurzeln von $F(x)$ und ist

$$\overline{f(x)} = \prod_{i=1}^{N} (x - \varphi(\alpha_i)); \quad \overline{f_1(x)} = \prod_{i=1}^{N} (x - \psi(\alpha_i)),$$

so ist $f(x) \mid \overline{f(x)}$ und $f_1(x) \mid \overline{f_1(x)}$. Ist für eine Primzahl p, $F(x)$ mod p linear zerlegbar, so sind nach dem Schatunowskischen Prinzip auch $\overline{f(x)}$ und $\overline{f_1(x)}$ mod p linear zerlegbar, und demnach sind es zugleich $f(x)$ und $f_1(x)$. Es bleibt also noch zu beweisen, dass für unendlich viele Primzahlen p, $F(x)$ mod p linear zerlegbar ist. Nun gibt es unendlich viele Primzahlen p_k, für die ganze rationale Zahlen a_k existieren, so dass $F(a_k) \equiv 0 \pmod{p_k}$. Es sei

$$F(x) \equiv F_1(x) F_2(x) \ldots F_t(x) \pmod{p_k},$$

wo $F_1(x), \ldots F_t(x)$ mod p_k irreduzibel sind. Nach dem Dedekindschen Satze, enthält die Galoissche Gruppe von $F(x)$ eine Permutation S, wo $S = C_1 C_2 \ldots C_a$ und $C_1, C_2, \ldots, C_a$ Zyklen bezeichnen, die keine gemeinsamen Ziffern haben, und deren Ordnungen den Graden von $F_1(x), \ldots, F_k(x)$ entsprechend gleich sind. Nach Hilfssatz 4 müssen $C_1, C_2, \ldots, C_a$ eingliedrig sein, d. h. $F(x)$ mod p_k zerfällt linear.

Satz III. *Es sei $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$, wo $a_0, a_1, \ldots, a_n$ Elemente eines vollkommenen Körpers K sind, ein normales Polynom* (d. h. es sei seine eigene Galoissche Resolvente).

I *Ist n ungerade, so ist die Diskriminante Quadrat eines Elementes von K.*

II *Ist n gerade und hat die Galoissche Gruppe G von $f(x)$, eine zyklische Untergruppe von Grade 2^m, wo $(2^{m+1}, n) = 2^m$ ist, so ist D kein Quadrat eines Elementes von K.*

III *Ist $2^m > 1$ und D kein Quadrat eines Elementes von K, so hat die Galoissche Gruppe G von $f(x)$ eine zyklische Untergruppe vom Grade 2^m.*

Beweis I. Bekanntlich ist der Ausdruck

$$P = (x_1 - x_2)(x_1 - x_3)\ldots(x_{n-1} - x_n) \tag{1}$$

entweder Wurzel einer quadratischen Gleichung mit Koeffizienten aus K oder P gehört zu K. Nun kann der erste Fall nicht vorkommen. Es gehört nämlich P zum Körper $K(\alpha)$, der aus K nach Adjunktion einer Wurzel α von $f(x)$ entsteht. Nach einem bekannten Satze, ist jedes Element $\psi(\alpha)$ von $K(\alpha)$ Wurzel einer Gleichung, deren Grad m Teiler von n ist. Da n ungerade ist, muss P zum Grundkörper gehören.

Zweiter Beweis von I: Nach Hilfssatz 4 ist jede Permutation S von G regulär. Die Anzahl k der Zyklen von S ist also ungerade Ist μ die Anzahl der Transpositionen, welche S darstellen, so ist

$$\mu \equiv n - k \pmod 2 \tag{2}$$

(vgl. z. B. H. Weber Lehrbuch der Algebra I, Braunschweig 1895, S. 495), also ist μ stets für jede Permutation von G eine gerade Zahl, und somit muss P zu K gehören.

II Der Annahme gemäss ist $f(x)$ normal, d. h. seine Galoissche Gruppe G ist von der Ordnung n. Dabei ist jede Permutation von G n-zifferig. Nach Hilfssatz 4 ist also jede Permutation von G regulär. Es sei jetzt $S = C_1 C_2 \dots C_k$ die Permutation, deren Potenzen die zyklische Gruppe bilden, wobei $C_1, C_2, \dots C_k$ Zyklen ohne gemeinsame Elemente sind, und welche eine gleiche Anzahl r von Ziffern haben. Es sei also $S^r = 1$. Nehmen wir an, dass die Ordnung der zyklischen Untergruppe

$$S, S^2, \dots S^{2^m}$$

2^m beträgt, so muss $r = 2^m$ sein, also ist $k = \frac{n}{2^m}$ eine ungerade Zahl. Ist μ die Anzahl der Transpositionen, so erhalten wir nach (2), dass μ zugleich ungerade ist. Wenden wir die Permutation S auf das Produkt (1) an, so muss P sein Zeichen ändern und kann also nicht zu K gehören.

III Es sei jetzt $2^m > 1$ und D kein Quadrat eines Elementes von K. Der Ausdruck P gehört also nicht zum Rationalitätsbereich, d. h. G muss mindestens eine Permutation S enthalten, welche durch eine ungerade Anzahl von Transpositionen μ darstellbar ist. Nach Formel (1) muss k ungerade sein. Es sei $S = C_1 C_2 \dots C_k$, wobei die Zyklen $C_1, \dots, C_k$, nach Hilfssatz 4, dieselbe Ordnung $t = \frac{n}{k}$ haben. Es muss also $2^m | t$ sein und die zyklische Gruppe $S, S^2, \dots S^t$, wo $S, S^2, \dots S^t$ offenbar voneinander verschieden sind, hat eine zyklische Untergruppe von Grade 2^m.

Anmerkung: Die Voraussetzung von III, dass $2^m > 1$, ist wesentlich. Wir haben nämlich nach einem Radosschen Satze [15]): die Diskriminante D_n einer Kreisteilungsgleichung K_n, wo $n = 2^m > 2$ ist, beträgt

$$D_n = (2^{n-1})^{2n-1}.$$

[15]) G. Rados: Crelle's Journal 131, 49 (1906).

Also ist D_n Quadratzahl. Andererseits existeren zyklische Polynome vom Grade 2^m. Für $2^m = 4$ s. H. Weber: Lehrbuch der Algebra II, Braunschweig 1896, S. 101—7, 111—21). Ferner gibt es mod p irreduzible Polynome von beliebigen Grade 2^m.

Anmerkung. Wie mich Herr N. Tschebotaröw in liebenswürdiger Weise aufmerksam gemacht hat, kann man den gruppentheoretischen Kern dieses Satzes folgendermassen formulieren:

Jede einfach transitive Permutationsgruppe von Ordnung und Grad n ist dann und nur dann in der alternierenden Gruppe n-ten Grades enthalten, wenn ihre 2-Sylowgruppe nicht zyklisch ist.

Folgerung (Der Pellet-Stickelberg-Voronoïsche Satz): *Ist D die Diskriminante des ganzzahligen Polynoms $f(x)$ und ist v die Anzahl der* mod p *irreduziblen Faktoren von $f(x)$, wo p eine Primzahl ist, die in der Zahl D nicht aufgeht, so ist*

$$\left(\frac{D}{p}\right) = (-1)^{n+v},$$

wobei $\left(\frac{D}{p}\right)$ das Legendresche Symbol ist und n den Grad von $f(x)$ bezeichnet.

Beweis. Ist D_1 die Diskriminante von $f_1(x)$ und D_2 die von $f_2(x)$, wo $f_1(x)$ und $f_2(x)$ ganzzahlige Polynome sind, so ist bekanntlich für die Diskriminante D von $f(x) = f_1(x) f_2(x)$

$$D = D_1 D_2 \, R(f_1(x), f_2(x))^2,$$

wo $R(f_1(x), f_2(x))$ die Resultante von $f_1(x)$ und $f_2(x)$ bezeichnet. Es genügt also, den Satz nur für irreduzible $f(x)$ zu beweisen. Nun haben wir, dass die Galoissche Gruppe von $f(x)$ mod p zyklisch ist (s. z. B. A. Speiser: Theorie der Gruppen von endlicher Ordnung, Berlin 1927, S. 56—71). Nach dem vorigen Satze (s. Fall I und II) ist D für ungerades n Quadrat und für gerades n kein Quadrat eines Elementes des Galoisfeldes.

§ 3.

Hilfssatz 5: *Ist $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$, wo $a_1, a_2, \dots, a_n$ ganze rationale Zahlen sind, ein Produkt von k irreduziblen Polynomen und hat $f(x)$* mod p_g, *wo p_g eine Primzahl ist, v_{p_g} lineare Faktorem, so ist*

$$\lim_{s \to 1} \frac{\sum_{g=1}^{\infty} v_{p_g} p_g^{-1-s}}{\log \frac{1}{s-1}} = k.$$

Beweis. Wäre der Satz für $k=1$ bewiesen, so wäre er auch für beliebiges k bewiesen. Es sei also $f(x)$ irreduzibel. Durchläuft $\mathfrak{p}_g$ alle Primideale ersten Grades des Körpers $k(\alpha)$, wo α eine beliebige Wurzel von $f(x)$ ist, so ist (s. z. B. D. Hilbert [16]), oder Hurwitz [17])

$$\lim_{s\to 1}\frac{\sum n(\mathfrak{p}_g)^{-s}}{\log\frac{1}{s-1}}=1,$$

wo $n(\mathfrak{p})$ die Norm von $\mathfrak{p}$ bezeichnet. Ist die rationale Primzahl p_g genau durch v_p Primideale ersten Grades teilbar, so erhält man, dass

$$\sum_{n(\mathfrak{p})\leqq x} n(\mathfrak{p})=\sum_{p\leqq x} v_p\, p^{-s},$$

und nach einem bekannten Dedekindschen Satze, dass $f(x)$ genau v_p lineare Faktoren mod p hat.

Ähnlich können wir unmittelbar einen Wegnerschen [18]) Satz verallgemeinern.

Satz IV: *Hat eine ganzzahlige Funktion* $F(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ *mit endlich vielen Ausnahmen* mod p, *wo* p *eine beliebige Primzahl ist, mindenstens* v *lineare Faktoren* (v *eine konstante natürliche Zahl*), *so ist* $f(x)$ *durch ein Produkt von* v *Polynomen teilbar.*

Beweis. Zunächst bemerken wir, dass man $a_0=1$ annehmen kann. Das Polynom $\varphi(y)=a_0^{n-1}f(x)$, wo $y=a_0x$ hat nämlich mod p, wo $(p,a_0)=1$, dieselbe Anzahl von Faktoren, wie $f(x)$. Nach der Voraussetzung ist $v_p\geqq v$, also ist

$$k=\lim\frac{\sum v_p p^{-s}}{\log\frac{1}{s-1}}\geqq v\,\frac{\sum p^{-s}}{\log\frac{1}{s-1}}=v,$$

wo k die Anzahl der irreduziblen Faktoren ist, deren Produkt $f(x)$ ergibt,

[16]) D. Hilbert: Die Theorie der algebr. Zahlkörper. Jhrb. d. deut. Math. Ver. 4 (1897) § 50; Werke I S. 143.

[17]) Hurwitz — Gassman: Beziehungen zwischen den Primidealen. Math Zeitsch. 25 (1926), 668.

[18]) U. Wegner. Zur Arithmetik der Polynome, Math. Ann. 105 (1931), 628—631; vgl. auch H. Hasse Zwei Bemerkungen zu der Arbeit von U. Wegner, ib. 106 (1932), 455—6; L v. d. Waerden. Noch eine Bemerkung. zu der Arbeit von U. Wegner. ib. 109 (1934); für $k=v$ vgl. [2]) S. 81—3.

Folgerung 2: *Es seien* K_1 *und* K_2 *zwei Galoissche Körper, welche durch die Wurzeln von* $f_1(x)=x^n+a_1x^{n-1}+\ldots+a_n$ *und* $f_2(x)=x^m+b_1x^{m-1}+\ldots+b_m$, ($a_1, a_2, \ldots a_n$, $b_1, b_2, \ldots b_m$ *ganzzahlig*) *gebildet werden.* K_1 *ist dann und nur dann ein Teiler von* K_2, *wenn mit* $f_2(x)$ *auch* $f_1(x)$ mod p (p *Primzahl*) *linear zerfällt.*

Anmerkung: Obwohl dieser wichtige wohlbekannte Kroneckersche Satz hier keine Anwendung findet, bieten wir doch seinen Beweis, da wir glauben, dass er sehr einfach ist, vgl. z. B. [19])

Beweis. Es sei $F_1(x)$ die Galoissche Resolvente von $f_1(x)$ und $F_2(x)$ die von $f_2(x)$. Zerfällt $f_1(x)$, sobald $f_2(x)$ mod p zerfällt, so folgt nach dem Schatunowskischen Prinzip (vgl. auch den Beweis der Folgerung des Hilfssatzes 4), dass mit $F_2(x)$ auch $F(x)$ mod p linear zerfällt, Ist $F(x)$ ein beliebiges normales Polynom, so folgt aus Hilfssatz 4, wenn $F(x)$ eine Wurzel mod p hat, dass $F(x)$ linear zerfällt. Bezeichnet also v_p die Anzahl der Wurzeln von $F(x)$ mod p, so ist entweder $v_p=0$ oder $v_p=N$, wo N den Grad von $F(x)$ bezeichnet. Nach dem vorstehenden Hilfssatze haben wir also

$$\Delta=\lim\frac{\sum w_p p^{-s}}{\log\frac{1}{s-1}}=\frac{1}{N},\quad w_p=0,1.$$

Wäre K_1 kein Teilkörper von K_2, so würde der kleinste Körper K, der K_1 und K_2 enthält, von K_2 verschieden sein. Ist $F(x)$ das normale Polynom, dessen Wurzeln K bilden, so erhält man für die entsprechenden Primzahlen p die Gleichung (1). Nach dem Schatunowskischen Prinzip ergibt sich, dass $F(x)$ dann und nur dann mod p zerfällt, wenn $F_2(x)$ mod p zerfällt. Ist also N_2 der Grad von $f_2(x)$, so muss auch $\Delta=\frac{1}{N_2}$ sein. Hieraus folgt $N_2=N$.

Umgekehrt, ist der Normalkörper K_1 ein Teiler des Normalkörpers K_2, so erhalten wir, nach dem Schatunowskischen Prinzip, dass mit $f_1(x)$ auch $f_2(x)$ mod p linear zerfällt.

Hilfssatz 6: *Es seien* $\varphi(x)$, $\varphi_1(x)$ *und* $\varphi_2(x)$ *ganzzahlige Polynome, wobei* $(\varphi_1(x), \varphi_2(x))=1$ *ist und für welche die Kongruenz*

$$\varphi_1(x)^2-D\varphi_2(x)^2\equiv 0 \pmod{\varphi(x)} \qquad D\not\equiv 1 \pmod 4 \tag{3}$$

[19]) N. Tschebotarów: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebener Substitutionsklasse gehören. Math. Annalen 95, 212—214 (1925).

besteht. Ist $K(\sqrt{D})$ einklassig, so gibt es solche ganzzahligen Polynome $f_1(x)$ und $f_2(x)$, dass

$$\varphi(x) = f_1(x)^2 - D f_2(x)^2$$

gilt.

Beweis. Es sei $F(x)$ beliebiges Polynom mit Koeffizienten, die ganze Zahlen des Körpers $K(\sqrt{D})$ sind. Ähnlich, wie im rationalen Körper, kann man den Satz beweisen, dass $F(x)$, bis auf Einheiten des Körpers $K(\sqrt{D})$, eindeutig als Produkt endlich vieler irreduziblen Polynome mit Koefizienten, die zugleich ganze Zahlen des Körpers $K(\sqrt{D})$ sind, dargestellt werden kann. Nun können wir die Kongruenz (3) in der Form

$$(\varphi_1(x) + \sqrt{D}\,\varphi_2(x))(\varphi_1(x) - \sqrt{D}\,\varphi_2(x)) \equiv 0 \pmod{\varphi(x)}$$

darstellen. Es existieren also solche Primteiler $P_1(x)$, $P_2(x)$, ... $P_k(x)$ von $\varphi_1(x) + \sqrt{D}\,\varphi_2(x)$, für welche

$$\varphi(x) = \varepsilon P_1(x)\overline{P_1(x)}\,P_2(x)\overline{P_2(x)} \ldots P_k(x)\overline{P_k(x)},\quad \varepsilon - \text{Einheit},$$

wo $\overline{P_i(x)}$ $(i = 1, 2, \ldots k)$ Koeffizienten hat, welche zu den Koeffizienten von $P_i(x)$ konjugiert sind. Ist

$$P_1(x) \ldots P_k(x) = U(x) + \sqrt{D}\,V(x)$$

wo $U(x)$ und $V(x)$ ganzzahlige Polynome sind, so ist entsprechend

$$\overline{P_1(x)} \ldots \overline{P_k(x)} = U(x) - \sqrt{D}\,V(x).$$

Demnach erhalten wir, dass $\varphi(x)$ durch die Form $\pm(U(x)^2 - D\,V(x)^2)$ darstellbar ist.

Satz V: *Dafür, dass ein ganzzahliges irreduzibles Polynom $f(x)$ höchstens endlich viele Primteiler $q \equiv -1 \pmod 4$ habe, ist es notwendig und hinreichend, dass $f(x)$ durch die Form $f_1(x)^2 + f_2(x)^2$ darstellbar sei, wo $f_1(x)$, $f_2(x)$ ganzzahlige Polynome sind.*

Beweis. Ist $f(x)$ durch die Form $f_1(x)^2 + f_2(x)^2$ darstellbar, so ist es einleuchtend, dass $f(x)$ höchstens endlich viele Primteiler $q \equiv -1 \pmod 4$ hat, nämlich diejenigen q, für die gleichzeitig die Kongruenzen

$$f_1(x) \equiv f_2(x) \equiv 0 \pmod q$$

bestehen d. h., sobald die Resultante von $f_1(x)$ und $f_2(x)$ durch q teilbar ist. Wir wollen also beweisen, dass diese Bedingung hinreichend ist. Es habe $f(x)$ mod v, mit endlich vielen Ausnahmen, eine reelle Wurzel dann

und nur dann, wenn $p \equiv 1 \pmod 4$, d. h., wenn zugleich auch $x^2 + 1 \equiv 0 \pmod p$ ist. Nun wenden wir den folgenden Bauerschen Satz [20]) an:

„K_v sei ein algebraischer Zahlkörper, definiert durch die rationale ganzzahlige irreduzible Gleichung $f_v(x) = 0$, G_v der zugehörige Galoissche Körper, A_v die Menge der Primzahlen, für die $f_v(x) \equiv 0 \pmod p$ in lineare Faktoren zerfällt, B_v die Menge der Primzahlen, für die diese Kongruenz mindestens eine ganze rationale Wurzel besitzt $(v = 1, 2)$. K_1 enthält dann und nur dann G_2, wenn B_1 (abgesehen von endlich vielen Ausnahmen) eine Teilmenge von A_1 ist".

Ist also $K(\alpha)$ ein Körper, welcher von einer Wurzel α des Polynoms $f(x)$ gebildet wird, so gehört zu diesem Körper die Zahl i. Es sei $\varphi(\alpha) = i$, d. h. $\varphi^2(\alpha) + 1 = 0$, wo $\varphi(\alpha)$ ein rationalzahliges Polynom von α ist. Das Polynom $\varphi^2(x) + 1$ hat also eine gemeinssame Wurzel mit dem irreduziblen Polynom $f(x)$ und demnach ist $\varphi^2(x) + 1$ durch $f(x)$ teilbar. Nach Hilfssatz 7 ist also der Satz bewiesen.

Anmerkung: Hat $f(x)$ eine reelle Wurzel, so kann nicht $fx)$ durch eine Summe zweier Quadrate darstellbar sein, und demnach hat die ganzzahlige Funktion $f(x)$, nach dem vorigen Satze unendlich viele Primteiler $q \equiv -1 \pmod 4$. Diesen Satz hat zuerst M. Bauer bewiesen [7]).

---

[20]) M. Bauer: Zur Theorie der algebraischen Zahlkörper. Math. Annalen 77 353—356 (1916).

(Eingegangen am 10. März 1935).