Zur Reduzibilität von Polynomen in der Kongruenztheorie. Zweite Abhandlung[1]).

Von

S. Lubelski (Warszawa).

Wir wollen hier zunächst auf die Sätze, die in der ersten Abhandlung entwickelt sind, ausführlicher eingehen. Vor allem geben wir eine Anwendung des Satzes I[1]), aus dem die Existenz unendlich vieler Primteiler $q \equiv -1 \bmod 4$ von ax^2+bx+c mit nichtquadratzahligem $d=4ac-b^2$ folgt. Diese führt nämlich zu einer Arithmetisierung des von Schur[2]) gegebenen Beweises für einen, auf Kreisteilungskörper beschränkten Hilbertschen Satz betreffend die Lösbarkeit von $-1=x^2+y^2+z^2+t^2$ (vgl. Satz 1 dieser Abhandlung). Ferner verallgemeinern wir den Satz II[1]) folgendermassen:

Voraussetzung: *$f(x)$ ist ein ganzes ganzzahliges, nicht normales, irreduzibles Polynom, $\varphi(x)$ ist eine Galoissche Resolvente von $f(x)$, D die Diskriminante von $\varphi(x)$ und x eine rationale Primzahl, für die $(p, D)=1$.*

Behauptung: *$\varphi(x)$ ist* mod p *zerlegbar* (s. Satz 2).

Des weiteren kann man den erwähnten Satz I[1]) in zwei Richtungen, einerseits auf beliebige Polynome und andererseits auf beliebige Moduln, erweitern. Zu diesem Behufe beweisen wir folgenden Satz:

[1]) Vgl. S. Lubelski: Zur Reduzibilität von Polynomen in der Kongruenztheorie. Acta Arithmetica 1 (1936), S. 169—183.

[2]) Vgl. E. Landau: Über die Darstellung definiter Funktionen durch Quadrate. Math. Annalen 62 (1906), S. 279—281.

Voraussetzung: *$f(x)$ ist ein beliebiges, ganzes ganzzahliges Polynom, m eine beliebige natürliche Zahl, $\mathfrak{B}$ die volle multiplikative Restgruppe* mod m *und $\mathfrak{B}_1$ eine Untergruppe von $\mathfrak{B}$. P ist eine Primzahl, die* mod m *zu $\mathfrak{B}_1$ nicht gehört und die Teiler von $f(x)$, aber kein Teiler der Diskriminante D von $f(x)$ ist.*

Behauptung: *Es existieren unendlich viele Primzahlen p, die mod m zu $\mathfrak{B}_1$ nicht gehören und Primteiler von $f(x)$ sind* (s. Satz 3).

Die Voraussetzung hinsichtlich der Zahl P im vorstehenden Satze ist von wesentlicher Bedeutung, denn, wie wir in dieser Arbeit zeigen (vgl. Satz 4), *existiert ein ganzes ganzzahliges Polynom $\varphi(x)$, dessen Primteiler mit endlich vielen Ausnahmen nur zu $\mathfrak{B}_1$ gehören.* Der Beweis dieses Satzes ermöglicht uns nebenbei die folgende Verallgemeinerung eines Kummerschen[3]) Satzes zu geben:

Ist $f(x)$ ein ganzes ganzzahliges irreduzibles Polynom vom Grade n, dessen Wurzeln zum Körper der m-ten Einheitswurzeln gehören, wobei

$$m = P^t, \quad 2P^t, P \neq 2,$$

wo P prim und t eine natürliche Zahl bezeichnet, so ist $f(x)$ dann und nur dann für primzahlige p, $(p, 2m)=1$, mod p *linear zerlegbar, wenn p Wurzel der Kongruenz*

$$x^{\frac{\varphi(m)}{n}} - 1 \equiv 0 \pmod{m}$$

ist (s. Satz 5).

Für $t=1$ erhält man den Satz von Kummer[3]).

In den weiteren Betrachtungen ersetzen wir das Schatunowskische Prinzip, vgl.[1]) S. 8, durch das viel allgemeinere Schursche Prinzip. Dadurch erhalten wir unter anderem die folgende Verallgemeinerung eines Nagellschen[4]) Satzes:

Voraussetzung: *K ist ein algebraischer Körper, K_1 ein Unterkörper von K, p eine rationale Primzahl, die kein ausserwesentlicher Diskriminantenteiler von K und K_1 ist. $\mathfrak{p}$ ist ein Primidealteiler von p in K vom g* ten Grade.

Behauptung. *p enthält in K_1 einen Primidealteiler $\mathfrak{P}$ vom Grade g', wo g' Teiler von g ist* (s. Satz 6).

[3]) E. E. Kummer: Journ. für Math., 30 (1846), S. 107—116; vgl. auch[5]) und[9]).

[4]) T. Nagell: Ein Beitrag zur Theorie der höheren Kongruenzen. Skrifter Oslo 1923 (1924), Nr. 813, S. 1—6.

Aus diesem Satze folgern wir in unmittelbarer Weise den ersten Teil des Kronecker-Bauerschen Einbettungssatzes. Für den zweiten (viel wichtigeren) Teil dieses Satzes geben wir zugleich mittels der Kroneckerschen Dichtigkeitsformel einen neuen, einfachen Beweis (s. Satz 7).

Dann zeigen wir, wieso man die Theorie der algebraisch-auflösbaren Polynome vom Primzahlgrad gänzlich arithmetisieren kann. In dieser Richtung liegen bereits einige spezielle Resultate von U. Wegner [5]) vor, jedoch reichen seine Methoden nicht aus, um zu unserem nachstehenden allgemeinen Ergebnis zu gelangen. Wir beweisen demnach den folgenden Satz:

Damit das ganze ganzzahlige Polynom $f(x)$ vom Primzahlgrad n algebraisch-auflösbar sei, ist notwendig und hinreichend, dass

1) die Primzahlen p, für die $f(x)$ mod p linear zerlegbar ist, mit endlich vielen Ausnahmen, bezüglich einer gewissen natürlichen Zahl m, mod m einer Untergruppe $\mathfrak{B}_1$ der vollen multiplikativen Restgruppe $\mathfrak{B}$ von m gehören,

2) die Faktorgruppe $\mathfrak{B}/\mathfrak{B}_1$ zyklisch sei,

3) die Primzahlen p, die zu $\mathfrak{B}_1$ gehören und für die $f(x)$ mod p einen Linearfaktor hat, mit endlich vielen Ausnahmen die Eigenschaft haben, dass für sie $f(x)$ mod p linear zerlegbar ist (s. Satz 9).

Ist $\mathfrak{B}_1$ durch $nx \pm 1$ repräsentiert, so erhalten wir den vorerwähnten wichtigen Wegnerschen Satz [5]).

Ferner geben wir, wiederum mittels des Kronecker-Bauerschen Einbettungssatzes, die folgende Verallgemeinerung des Satzes V [1]):

Damit ein normiertes ganzes ganzzahliges Polynom $f(x)$ mit endlich vielen Ausnahmen nur Primteiler haben soll, die zugleich Primteiler der Form $x^2 - Dy^2$ sind, D-quadratfrei, ist notwendig und hinreichend, dass $4f(x)$ durch die Form $f_1(x)^2 - Df_2(x)^2$ darstellbar sei, wo $f_1(x)$ und $f_2(x)$ ganze ganzzahlige Polynome sind (s. Satz 10).

Schliesslich bemerken wir, dass wir auf die Vertiefung anderer von uns gelieferten Sätze in einer künftigen Arbeit noch zurückkommen werden.

§ 1.

In § 1. der ersten Abhandlung haben wir einen Radosschen Satz, für den Fall eines quadratischen Polynoms, folgendermassen verschärft:

[5]) U. Wegner: Ein Satz über auflösbare Polynome vom Primzahlgrad, Math. Annalen 105 (1931), S. 256 — 261.

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 $q \equiv -1 \bmod 4$.

Als Anwendung dieses Satzes arithmetisieren wir den Schurschen Beweis [2]) des folgenden Satzes:

Satz 1: *Im Körper K_m der m-ten Einheitswurzel ist die Gleichung $-1 = x^2 + y^2 + z^2 + t^2$ stets lösbar.*

Beweis. Wir wollen den Schurschen Beweis von jener Stelle weiter führen, von wo aus er nicht ganz arithmetisch war. Infolgedessen genügt es, ohne Zuhilfenahme des Dirichletschen Satzes über arithmetische Progression, zu zeigen, dass für eine Primzahl $p \equiv 1 \bmod 8$ ein Nichtrest $q \equiv 3 \bmod 4$ existiert. Denn (für $q \equiv 3 \bmod 8$ ist der Satz in [2]) arithmetisch bewiesen. Wäre $q \equiv 7 \bmod 8$; so) betrachtet man, wie in [2]) S. 280, für $q^{\frac{p-1}{2}} + 1 = hp$, die Produkte

$$(1) \qquad \left(\prod_{n=0}^{p-1} x^n\right)\left(\prod_{i=0}^{h-1} x^{ip}\right) = \prod_{j=0}^{hp-1} x^j = \prod_{u=0}^{hp-2} x^u + x^{hp-1}$$

$$(2) \qquad = \left(\prod_{v=0}^{q-1} x^v\right)\left(\prod_{t=0}^{q-1} x^{tq}\right) \cdot \ldots \cdot \left(\prod_{w=0}^{q-1} x^{wq^{\frac{p-1}{2}-1}}\right) + x^{hp-1}.$$

Da

$$4\frac{x^q - 1}{x - 1} = X_1(x)^2 + qX_2(x)^2, \qquad 4\prod_{t=0}^{q-1} x^{tq^s} = X_1(x^{q^s})^2 + qX_2(x^{q^s})^2,$$

wo $X_1(x)$ und $X_2(x)$ ganze ganzzahlige Polynome bezeichnen, so ist nach der Eulerschen Identität auch der Ausdruck (2) durch die Form $f_1(x)^2 + qf_2(x)^2 + x^{hp-1}$ mit ganzen rationalzahligen $f_1(x)$ und $f_2(x)$ darstellbar. Für gewisse ganze rationale Zahlen a, b, c, d, ist $q = a^2 + b^2 + c^2 + d^2$. Also existieren solche ganze rationalzahlige Polynome $F_i(x)$, $i = 1, 2, 3, 4, 5$, für die der Ausdruck (1) durch die Form $\sum F_i(x)^2 + x^{hp-1}$ darstellbar ist. Setzt man in (1) und in (2) für x eine primitive p-te Einheitswurzel v ein, so ergibt sich

$$0 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 + \varepsilon^2 + v^{-1}; \quad -1 = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2 + \varepsilon^2)\left(v^{\frac{p+1}{2}}\right)^2;$$

$$1^2 + \alpha_1^2 + \beta_1^2 + \gamma_1^2 + \delta_1^2 + \varepsilon_1^2 = 0; \quad -(1 + \alpha_1^2)^2 = \alpha_2^2 + \beta_2^2 + \gamma_2^2 + \delta_2^2;$$

$$-1 = \alpha_3^2 + \beta_3^2 + \gamma_3^2 + \delta_3^2.$$

Nun enthält nach dem Satze I [1]) das Binom $x^2 + p$ Primteiler der Form $q \equiv 3 \bmod 4$, d. h.

$$\left(\frac{-p}{q}\right) = -\left(\frac{p}{q}\right) = 1.$$

Mithin folgt aus dem quadratischen Reziprozitätsgesetz, dass $\left(\frac{q}{p}\right) = -1$, womit der Satz 1 bewiesen ist.

§ 2.

Desgleichen verschärfen wir den Satz II [1]) folgendermassen:

Satz 2. Voraussetzung: *$f(x)$ ist ein ganzes ganzzahliges, nicht normales, irreduzibles Polynom. $\varphi(x)$ ist eine Galoissche Resolvente von $f(x)$, D die Diskriminante von $\varphi(x)$ und p eine rationale Primzahl, für die $(p, D) = 1$.*

Behauptung: *$\varphi(x)$ ist* mod p *zerlegbar.*

Beweis. Es sei p eine Primzahl für die das normale Polynom $\varphi(x)$ mod p unzerlegbar ist. Ist $(p, D) = 1$, wo D die Diskriminante von $f(x)$ bezeichnet, so folgt nach einem Dedekindschen Satz (vgl. [1]) S. 7—8), dass die Galoissche Gruppe $\mathfrak{B}$ von $\varphi(x)$ eine Permutation enthält, die nur aus einem einzigen Zyklus besteht. Da $\varphi(x)$ normal ist, so ist $\mathfrak{B}$ regulär und mithin ist $\mathfrak{B}$ zyklisch (vgl. z. B. [1]) Hilfssatz 4). Nach dem wohlbekannten Kronecker-Weberschen Einbettungssatz [17]) gehören die Wurzeln von $f(x)$ einem Kreisteilungskörper an, welcher mit K bezeichnet werden möge.

Da die Automorphismengruppe von K Abelsch ist, so würde auch $f(x)$ normal sein. Dies widerspricht aber der Annahme in Bezug auf $f(x)$. Also ist $\varphi(x)$, für fast alle Primzahlen p, mod p zerlegbar.

Beispiel: Das Polynom $x^n - a$, wo a eine ganze rationale Zahl bezeichnet, die keine n-te Potenz einer ganzen rationalen Zahl ist, ist offenbar nicht normal. Also hat ihre Resolvente die genannte Eigenschaft.

§ 3.

Wir kehren wieder zum Satze I [1]) zurück, um ihn auf beliebige Polynome und Moduln zu verallgemeinern. Wir beweisen nämlich den folgenden Satz:

Satz 3. Voraussetzung: *$f(x)$ ist ein beliebiges ganzes ganzzahliges Polynom, m eine beliebige natürliche Zahl, $\mathfrak{B}$ die volle multiplikative Restgruppe* mod m *und $\mathfrak{B}_1$ eine Untergruppe von $\mathfrak{B}$. P, wo $(P, m) = 1$, ist eine Primzahl, die* mod m *zur $\mathfrak{B}_1$ nicht gehört und die Teiler von $f(x)$, aber kein Teiler der Diskriminante D von $f(x)$ ist.*

Behauptung: *Es existieren unendlich viele Primzahlen p, die* mod m *zu $\mathfrak{B}_1$ nicht gehören und die Primteiler von $f(x)$ sind.*

Beweis: I. Nach Voraussetzung ist der Primteiler P von $f(x)$ relativ prim zur Diskriminante D von $f(x)$. Es ist also für jede natürliche Zahl n die Kongruenz

$$f(x) \equiv 0 \pmod{P^n}$$

lösbar. Nehmen wir an, dass P^a die höchste Potenz von P sei, für die $f(x)$ für jedes x teilbar ist, so existiert eine Zahl ρ_n, für die

$$(f(\rho_n),\ P^{n+1}) = P^n,$$

wenn nur $n \geqq a$ ist. Ferner sei δ die Invariante von $f(x)$, d. h. die grösste natürliche Zahl, durch die $f(x)$, bei beliebigen x, stets teilbar ist. Mit

$$\delta_1,\ \delta_2, \ldots,\ \delta_s$$

bezeichnen wir sämtliche verschiedenen Primteiler von m, die in δ nicht aufgehen. Es existiert dann für jede natürliche Zahl δ_i, $i = 1, 2, \ldots, s$, eine ganze Zahl z_i, für die

$$(f(z_i),\ \delta_i) = 1, \quad i = 1, 2, \ldots, s.$$

Ferner können wir, da $(P, m) = 1$, eine ganze Zahl ζ finden, für die

$$\rho_a + P^{a+1}\zeta \equiv z_i \pmod{\delta_i},\ i = 1, 2, \ldots, s;$$

$$\rho_a + P^{a+1}\zeta \equiv r_j \pmod{d_j^{a_j+1}},\ d_j \neq P,\ j = 1, 2, \ldots, t;$$

$$\delta = d_1^{a_1} d_2^{a_2} \ldots d_t^{a_t}, \quad (f(r_j),\ d_j^{a_j+1}) = d_j^{a_j},$$

wo d_j verschiedene Primteiler von δ bezeichnen. Demzufolge enthält die Invariante Δ_v von $f(r + m^v x)$, wo v eine beliebige natürliche Zahl bezeichnet und

$$r = \rho_a + P^{a+1}\zeta$$

ist, nach der Taylorschen Entwicklung nur solche Primteiler, die zugleich in δ aufgehen, denn ist δ' ein Teiler von Δ_v, für den $(\delta', m) = 1$, so gilt auch δ'/δ, da $r + m^v x$ mit x zugleich ein volles Restsystem mod δ' durchläuft. Bezeichnen wir jetzt mit m^b eine Potenz von m, die durch $d_i^{a_i}$ teilbar ist, wenn nur $d_i | m$ ist, so enthält die Invariante Δ von $f(r + Mx)$, wo $M = m^{b+1}$, da $(f(r), \delta^2) = \delta$ ist, nur solche Teiler von M, die zugleich in δ aufgehen. Demnach ist $\Delta = \pm\delta$.

II Mit

(1) $$p_1, p_2, \ldots, p_h,$$

bezeichnen wir diejenigen Primteiler von $f(r+Mx)$, die zur Gruppe $\mathfrak{B}$, aber nicht zur Gruppe $\mathfrak{B}_1$ mod m gehören. Die Folge (1) ist sicherlich nicht leer, da P zu ihr gehört. Es ist nun zu beweisen, dass die Folge (1) unendlich sei. Wir führen den Beweis indirekt, indem angenommen wird, dass die Folge (1) nur aus P und endlich vielen

(2) $$p_1, p_2, \ldots p_g$$

besteht, wo $p_w, w=1,2,\ldots,g$, keine Teiler von δ sind. Dann existiert für jede Zahl p_w, eine ganze Zahl l_w, wo

$$(f(r+Ml_w),\ p_w)=1.$$

Nun existiert nach I. für jede Primzahl d_j, wo $\delta=d_1^{a_1}\ldots d_t^{a_t}$, eine ganze Zahl R_j, mit der Eigenschaft, dass

$$(f(r+MR_j),\ d_j^{a_j+1})=d_j^{a_j}.$$

Mit ξ bezeichnen wir eine ganze Zahl, die den folgenden Kongruenzen

$$\xi\equiv 0 \pmod{P^{a+1}},\quad \xi\equiv l_w \pmod{p_w},\quad \xi\equiv R_j \pmod{d_j^{a_j+1}}$$

genügt. Es ist also

$$(f(r+M\xi),\ \delta^2 p_w)=\delta,\quad w=1,2,\ldots,g.$$

Andererseits existieren, da $(P,M)=1$, solche ganze Zahlen u_1, t_1, für die

$$\rho_{a+1}+P^{a+2}u_1=r+Mt_1.$$

Es ist also

$$(f(r+Mt_1),\ P^{a+2})=P^{a+1}.$$

Jetzt bestimmen wir eine ganze Zahl η, die den Kongruenzen

$$\eta\equiv t_1 \pmod{P^{a+2}},\quad \eta\equiv R_j \pmod{d_j^{a_j+1}},\quad \eta\equiv l_w \pmod{p_w},$$

wo $j=1,2,\ldots,t, d_j\neq P;\ w=1,2,\ldots,g$, genügt. Die Primteiler von

$$A=\frac{f(r+M\xi)}{\delta},\qquad B=\frac{f(r+M\eta)}{P\delta}$$

sind also von den Zahlen d_j und von den Zahlen der Folge (2) verschieden, sowie zu m relativ prim. Nun ist

$$f(r+M\xi)\equiv f(r+M\eta) \pmod{M}$$

und mithin ist, da $M=m^{b+1}$ und m^b durch $d_j^{a_j}$ teilbar ist, wenn nur $d_j|m$,

$$A\equiv BP \pmod{m}.$$

Nach unserer Annahme müssen die Primteiler von B zu $\mathfrak{B}_1$ gehören A gehört also mod m nicht zur Gruppe $\mathfrak{B}_1$ und daher enthält A einen Primteiler, der mod m weder in $\mathfrak{B}_1$ noch in der Folge (2) aufgeht. Demnach ist der Satz bewiesen.

Als Folgerung dieses Satzes erhalten wir auf rein arithmetischem Wege folgenden Satz über die Verteilung der Primzahlen.

Folgerung. *Bilden die Klassen, die aus den ganzen Zahlen b_k, $k=1,2,\ldots,n$,* mod m *entstehen, eine Untergruppe $\mathfrak{B}_1$ der vollen multiplikativen Restgruppe $\mathfrak{B}$* mod m, *so existiert eine ganze Zahl b, die von b_k, $k=1,2,\ldots,n$,* mod m *verschieden ist und für die $mx+b$ unendlich viele Primzahlen enthält.*

Beweis. Es genügt im vorstehenden Satze $f(x)=x$ zu setzen.

Jetzt werden wir ein Gegenstück zum Satze 3 beweisen. Damit wird auch gezeigt werden, dass die Voraussetzungen des Satzes 3 wesentlich sind.

Satz 4. Voraussetzung: *m ist eine gewisse natürliche Zahl, $\mathfrak{B}_1$ eine gewisse Untergruppe der* mod m *vollen multiplikativen Restgruppe $\mathfrak{B}$.*

Behauptung: *Es existiert ein ganzes ganzzahliges Kreisteilungspolynom $f(x)$, das mit endlich vielen Ausnahmen nur Primteiler hat, die* mod m *zu $\mathfrak{B}_1$ gehören. Dabei ist der Grad von $f(x)$ dem Index von $\mathfrak{B}_1$ in Bezug auf $\mathfrak{B}$ gleich. Umgekehrt ist $\varphi(x)$ ein Kreisteilungspolynom, so entspricht $\varphi(x)$ eine gewisse Gruppe $\mathfrak{B}_1$ mit den genannten Eigenschaften.*

Beweis. I. Mit

$$k_j,\quad j=1,2,\ldots,v$$

bezeichnen wir ein Repräsentantensystem der Gruppe $\mathfrak{B}_1$, d. h. ein System verschiedener Zahlen mit der Eigenschaft, dass jede Zahl, die mod m zur Gruppe $\mathfrak{B}_1$ gehört, einer und nur einer Zahl von (1) mod m kongruent ist. Ferner bezeichnen wir mit $\mathfrak{K}(\varepsilon)$ den m-ten Kreisteilungskörper, d. h. den Körper der m-ten primitiven Einheitswurzel ε. Die Automorphismengruppe $\mathfrak{A}$ von $\mathfrak{K}(\varepsilon)$ kann man mittels der Paare $(\varepsilon, \varepsilon^t)$ darstellen, wo t die Gesamtheit der Zahlen mod m durchläuft, die zu m relativ prim sind. Offenbar sind diese Automorphismen mit der vollen multiplikativen Restgruppe $\mathfrak{B}$ mod m isomorph. Es entspricht also der Un-

tergruppe $\mathfrak{B}_1$ eine Untergruppe $\mathfrak{A}_1$ von $\mathfrak{A}$ deren Elemente die Gestalt $(\varepsilon, \varepsilon^{k_j})$ haben, wo k_j sämtliche Elemente von (1) durchläuft. Mit $A(\varepsilon)$ bezeichnen wir ein Element von $\mathfrak{K}(\varepsilon)$, das genau zu $\mathfrak{A}_1$ gehört, mit $f(x)$ das ganze ganzzahlige irreduzible Polynom, dessen Wurzel $A(\varepsilon)$ ist, und mit p einen rationalen Primteiler von $f(x)$, der in der Diskriminante von $\mathfrak{K}(\varepsilon)$ nicht aufgeht. Wenn wir nur zeigen, dass p mod m zur Gruppe $\mathfrak{B}_1$ gehört, so wird der Satz gänzlich bewiesen sein. Dies ergibt sich aber in der Tat folgendermassen: es sei $p/f(a)$, wo a eine entsprechende ganze rationale Zahl bezeichnet. Wir setzen

$$f(x) = (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_i),$$

$$x_j = A(\varepsilon^h) = A_1(\varepsilon) \equiv a \pmod{\mathfrak{p}_j}, \quad j = 1, 2, \ldots, i,$$

wo $\mathfrak{p}_j$ ein entsprechender Primidealteiler von p bezeichnet. Es ist also

$$a \equiv a^p \equiv A_1(\varepsilon)^p \equiv A_1(\varepsilon^p) \equiv a \equiv A_1(\varepsilon) \pmod{\mathfrak{p}_j}.$$

Wäre $A_1(\varepsilon^p) \neq A_1(\varepsilon)$, so würde eine der Differenzen

$$x_g - x_i = A(\varepsilon^u) - A(\varepsilon^w)$$

durch $\mathfrak{p}_j$ teilbar sein. Mithin würde die Diskriminante von $\mathfrak{K}(\varepsilon)$ durch p teilbar sein, was der Annahme in Bezug auf p widerspricht. Demnach muss

$$A_1(\varepsilon^p) = A_1(\varepsilon)$$

sein. Da $A(\varepsilon^h)$ zu $\mathfrak{A}_1$ gehört, so kann die letzte Gleichung dann und nur dann bestehen, wenn p mod m einer der Zahlen (1) mod m kongruent ist, womit der erste Teil des Satzes bewiesen erscheint.

Nun ist es leicht zu beweisen, dass auch die Umkehrung der letzten Tatsache gilt. Denn ist p einer der Zahlen (1) mod m kongruent, so ist $A(\varepsilon^p) = A(\varepsilon)$. Mithin ist

$$A(\varepsilon^p) \equiv A(\varepsilon)^p \equiv A(\varepsilon) \pmod{p}.$$

Also ist $A(\varepsilon)$ mod p einer gewissen ganzen rationalen Zahl b mod p kongruent, d. h. $f(b)$ durch p teilbar.

Als Folgerung des Satzes 4 erhalten wir eine Regel, mittels welcher man beantworten kann, wann ein normales Polynom dritten Grades mod p zerlegbar ist.

Folgerung 1. Voraussetzung: *$f(x)$ ist ein irreduzibles normales Polynom dritten Grades. D die Diskriminante des Körpers K, der durch die Wurzeln von $f(x)$ gebildet ist.*

Behauptung: *K ist Unterkörper eines von m-ten Einheitswurzeln gebildeten Körpers $K(\varepsilon)$. Ist $\mathfrak{A}_1$ die Untergruppe der Automorphismengruppe von $K(\varepsilon)$, zu der K gehört und $\mathfrak{B}_1$ die Untergruppe der vollen multiplikativen Restgruppe* mod m, *die zu $\mathfrak{A}_1$ isomorph ist, so ist $f(x)$* mod p, *wo $(p, D) = 1$, dann und nur dann linear zerlegbar, wenn p* mod m *zu $\mathfrak{B}_1$ gehört.*

Beweis. Nach dem wohlbekannten Kronecker-Weberschen Satze über die Einbettung der Abelschen Körper, muss K Unterkörper eines Kreisteilungskörpers sein. Demnach können wir den Satz 4 anwenden und mithin ist alles bewiesen.

Anmerkung. Dieser Satz gibt uns die Möglichkeit die Theorie des kubischen Körpers zu vervollständigen, da die bisherigen Betrachtungen dieser Theorie ausschliesslich den Fall eines nicht normalen kubischen Körpers behandelt haben (vgl. z. B. H. Hasse[6]). Den Fall eines kubischen Körpers K, der Unterkörper des Körpers der p-ten Einheitswurzel ist, p-prim, hat J. Westlund[7]) behandelt.

Der Beweis des Satzes 4 gibt uns auch die Möglichkeit in unmittelbarer Weise die folgende Verallgemeinerung eines Kummerschen Satzes[8]) zu geben.

Satz 5: *Ist $f(x)$ ein ganzes ganzzahliges Polynom vom Grade n, dessen Wurzeln zum Körper der m-ten Einheitswurzeln gehören, wobei*

$$m = P^t, \; 2P^t, \; P \neq 2,$$

wo P prim und t eine natürliche Zahl bezeichnet, so ist $f(x)$ dann und nur dann für primzahlige p, $(p, 2m) = 1$, mod p *linear zerlegbar, wenn p Wurzel der Kongruenz*

$$x^{\frac{\varphi(m)}{n}} - 1 \equiv 0 \pmod{m}$$

ist, wo $\varphi(m)$ die Eulersche Funktion bezeichnet.

Beweis. Es sei α Wurzel von $f(x)$ und $\alpha = A(\varepsilon)$, wo ε die m-te primitive Einheitswurzel und $A(\varepsilon)$ ein ganzzahliges Polynom von ε bezeichnet. Es sei ferner $\mathfrak{A}_1$ zu $A(\varepsilon)$ gehörende Untergruppe der Automorphismengruppe $\mathfrak{A}$ des m-ten Kreisteilungskörpers und $\mathfrak{B}_1$ die Unter-

[6]) H. Hasse: Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, Math. Zeitschr. 31 (1930), S. 565—582.

[7]) J. Westlund: On the factorisation of rational primes in cubic cyclotomic fields, Jahrbr. d. deutsch. Math. Ver. 22 (1913), S. 135—140.

gruppe von $\mathfrak{B}$, die zu $\mathfrak{A}$ isomorph ist. Nach dem Satze 4 beträgt die Ordnung von $\mathfrak{A}_1$ $\frac{\varphi(m)}{n}$, wo n der Grad von $f(x)$ ist. Mithin erfüllt jede ganze rationale Zahl, die mod m zu $\mathfrak{B}_1$ gehört, die Kongruenz

$$x^{\frac{\varphi(m)}{n}} \equiv 1 \pmod{m}. \tag{2}$$

Ist nun $m = P^l$, bzw. $= 2P^l$, wo P eine ungerade Primzahl bezeichnet, so ist $\mathfrak{B}$ zyklisch und demnach enthält $\mathfrak{B}$ nur eine zyklische Untergruppe von Ordnung $\frac{\varphi(m)}{n}$, d. h. sämtliche Lösungen von (2) mod m gehören zu einer entsprecheden Untergruppe (1). Nach Satz 4 ist also alles bewiesen.

Anmerkung. Kummer[8]) erhielt diesen Satz für ein primzahliges m, wobei die Wurzeln von $f(x)$ entsprechende Periodenzahlen der m-ten irreduziblen Kreisteilungsgleichung waren. Den ersten exakten Beweis des Kummerschen Satzes hat H. Smith[8]) gegeben; vgl. auch G. Rados[9]).

§ 5.

Wie wir bereits in der Einleitung erwähnt haben, ist das Schatunowskische Prinzip. ([1] S. 8) ein Sonderfall eines viel tieferliegenden Schurschen Prinzips[10]), das folgendermassen lautet:

Schursches Prinzip: Voraussetzung: *$f(x)$ ist ein ganzes ganzzahliges Polynom, dessen Wurzeln den Zahlen $w_1, w_2, \ldots, w_n$ gleich sind, Γ ist ein endlicher Kongruenzkörper* mod p, *wo p eine rationale Primzahl bezeichnet. In Γ ist*

$$f(x) \equiv (x-\eta_1)(x-\eta_2)\cdot\ldots\cdot(x-\eta_n) \pmod{p}.$$

$F_j(x_1, x_2, \ldots, x_n)$, $j = 1, 2, \ldots r$ sind irgendwelche ganze ganzzahlige Polynome, die für $x_i = w_i$, $i = 1, 2, \ldots, n$ verschwinden.

Behauptung: *Durch eine geeignete Anordnung der Elemente $\eta_{i_1}, \eta_{i_2}, \ldots, \eta_{i_n}$ kann man erreichen, dass*

$$F_j(\eta_{i_1}, \eta_{i_2}, \ldots, \eta_{i_n}) \equiv 0 \pmod{p}, \quad j = 1, 2, \ldots, r$$

sein wird.

[8]) H. J. Smith: Report of British Association, 1860, S. 128.

[9]) G. Rados: Bemerkungen und Ergänzungen zum Beweis eines Kummerschen Theorems. Journ. für Math. 152 (1923), S. 192—197.

[10]) I. Schur: Beispiele für Gleichungen ohne Affekt. Jahrbr. d. deutsch. Math. Ver. 29 (1920), S. 145—146.

Anmerkung. Für unsere Betrachtungen genügt der Fall, wenn $F_j(x_1, x_2, \ldots, x_n)$ symmetrische Polynome von $x_1, x_2, \ldots, x_n$ sind, Dann verläuft der Beweis sehr einfach.

Mittels des Schurschen Prinzips geben wir die folgende Verallgemeinerung eines wichtigen Nagellschen Satzes[4]).

Satz 6. Voraussetzung: *K ist ein algebraischer Körper. K_1 ein Unterkörper von K. p eine rationale Primzahl, die kein ausserwesentlicher Diskriminantenteiler von K und K_1 ist. $\mathfrak{p}$ ist ein Primidealteiler von p vom g-ten Grade.*

Behauptung: *p enthält in K_1 einen Primidealteiler $\mathfrak{P}$ vom Grade g', wo g' Teiler von g ist.*

Beweis. Ist p kein ausserwesentlicher Diskriminantenteiler von K, so existiert in K bzw. in K_1 ein primitives Element α bzw. β, für die $(\Delta, p) = (\Delta_1, p) = 1$, wo Δ bzw. Δ_1 den Index der Zahl α bzw. β bezeichnet. Ist $p = \mathfrak{p}_1 \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_t$, wo $\mathfrak{p}_i$, $i = 1, 2, \ldots, t$ Primideale des Körpers K vom Grade g_i sind, so folgt aus einem bekannten Dedekindschen Satze[11]), dass

$$f(x) \equiv f_1(x) f_2(x) \cdot \ldots \cdot f_t(x) \pmod{p}, \tag{1}$$

wo $f(x)$ das ganze ganzzahlige irreduzible Polynom bezeichnet, dessen Wurzel α ist und $f_i(x)$, $i = 1, 2, \ldots, t$, mod p irreduzibel und vom Grade g_i sind. Ist $F(x)$ das irreduzible ganzzahlige Polynom, dessen Wurzel β ist, so ist das ganzzahlige Polynom

$$\psi(x) = x^h - \sum \beta_h x^{n-1} + \sum_{i \neq j} \beta_i \beta_j x^{n-2} + \ldots \pm \beta_1 \beta_2 \ldots \beta_n, \tag{2}$$

wo n den Grad von K bezeichnet und β_h die verschiedenen Konjugierten von β in K bedeuten, eine Potenz von $F(x)$ (vgl. z. B.[13]) S. 69, Satz 54). Wir bezeichnen jetzt mit $\bar{K}$ den endlichen Körper, der aus sämtlichen Wurzeln von $f(x)$ mod p gebildet ist, und mit $\bar{x}$ das Element von $\bar{K}$, das dem Elemente x aus K entspricht. Nach dem Schurschen Prinzip können wir in (2) die Zahlen β_h durch die ihr entsprechenden Werte $\bar{\beta}_h$ ersetzen. Enthält also $f(x)$ mod p einen irreduziblen Faktor vom g-ten Grade, so enthält das Polynom $\psi(x)$ aus (2) mod p einen irreduziblen Faktor vom Grade g', wo g' Teiler von g ist (s. [18]) ibid.). Da $\psi(x)$ Potenz von $F(x)$ ist, so ist p in K_1, wieder nach dem Dedekindschen Satze[11]), durch ein Primideal vom Grade g' teilbar.

[11]) vgl. z. B. R. Dedekind: Werke I. Braunschweig 1930, S. 202—213; oder P. Bachmann: Allgemeine Arithmetik der Zahlenkörper. Leipzig 1905, Siebentes kapitel.

Als unmittelbare Folgerung dieses Satzes erhalten wir:

Folgerung 1: *Bei den Voraussetzungen des Satzes 6 ist p in K_1 durch ein Primideal ersten Grades teilbar, wenn nur p in K durch ein solches teilbar ist.*

Folgerung 2: *Sind $f_i(x)$, $i=1, 2, \ldots, n$, ganze ganzzahlige Polynome, so existieren unendlich viele natürliche Primzahlen p, für die $f_i(x)$, $i=1, 2, \ldots, n$, gleichzeitig mod p linear zerlegbar sind.*

Beweis. Ähnlich, wie im Beweise der Folgerung des Schatunowskischen Prinzips (s. [1]) S. 8) können wir $f_i(x)$ als normiert voraussetzen. Unter dieser Annahme konstruieren wir den kleinsten Körper $\Omega(\alpha)$, der die Wurzeln von $f_i(x)$, $i=1, 2, \ldots, n$ enthält. Ist nun $F(x)$ das normale ganzzahlige Polynom, für welches $F(\alpha)=0$, so enthält dieses bekanntlich unendlich viele Primteiler. Dieselbe Eigenschaft gilt auch für alle $f_i(x)$ zugleich, da nach Folgerung 1 alle $f_i(x)$ zugleich mod p zerlegbar sind, wenn dies für $F(x)$ zutrifft. w. z. b. w.

Anmerkung. Mit elementaren Mitteln hat T. Nagell[4]) gezeigt, dass zwei ganze ganzzahlige Polynome unendlich viele gemeinsame Primteiler haben.

Folgerung 3. *Bei den Voraussetzungen des Satzes 1 ist p in K_1 nur durch Primideale ersten Grades teilbar, wenn nur K_1 Galoissch ist und p in K mindestens durch ein Primideal ersten Grades teilbar ist.*

Die Folgerung 3 hat Bauer[12]) für gewisse Körper umgekehrt:

Satz 7. *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 $f_v(x)\equiv 0 \bmod p$ 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.*

Für diesen Kronecker-Bauerschen Einbettungssatz wollen wir unter Heranziehung der Kroneckerschen Dichtigkeitsformel einen sehr einfachen Beweis geben.

Beweis. Mit K bezeichnen wir den Durchschnitt von K_1 und K_2 und mit K_3 das Kompositum von K_1 und K_2. Es sei α bzw. β bzw. γ ein primitives Element von K_1 bzw. K_2 bzw. K_3. Bekanntlich kann man

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

$\gamma = t\alpha + t_1\beta$ setzen, wo t und t_1 gewisse ganze rationale Zahlen bezeichnen[13]). Ferner sei

$$F(x)=\prod_{i,j}(x - t\alpha_i - t_1\beta_j),$$

wo α_i und β_j unabhängig voneinander sämtliche Konjugierte von α bzw. von β durchlaufen. Hat also $f_1(x)$ mod p v_p' Linearfaktoren und $f_2(x)$ v_p'' Linearfaktoren, so hat $F(x)$ nach dem Schurschen Prinzip und Satz 6 $v_p'v_p''$ derartige Faktoren. Da man offenbar $f_2(x)$ als normales Polynom annehmen kann d. h. $G_2=K_2$, so ist, wenn $v_p''\neq 0$, $v_p''=n_2$, wo n_2 der Grad von $f_2(x)$ bezeichnet. Nach Voraussetzung des Satzes ist nun stets $v_p''\neq 0$, wenn nur $v_p'\neq 0$ ist. Wir erhalten also nach der Kroneckerschen Dichtigkeitsformel

$$r=\frac{\sum v_p p^{-s}}{\log\frac{1}{s-1}}=n_2\frac{\sum v_p' p^{-s}}{\log\frac{1}{s-1}}=n_2, \tag{1}$$

wo r die Anzahl der irreduziblen Faktoren von $F(x)$ im rationalen Körper und v_p die Anzahl der Linearfaktoren von $F(x)$ mod p bezeichnet. $F(x)$ enthält mithin einen irreduziblen Faktor, dessen Grad g nach (1) der Ungleichung

$$g\leqq\frac{n_1 n_2}{n_2}=n_1$$

genügt. Da der Grad eines Kompositums von Körpern nicht kleiner als der Grad eines der komponierten Körper ist, so muss $g=n_1$ sein, d. h. der Körper K_3 ist mit K_1 identisch und mithin ist K_2 Unterkörper von K_1. w. z. b. w.

Nun wollen wir zeigen, wie man mittels der obigen Betrachtungen die Arithmetisierung der Theorie der algebraisch auflösbaren Polynome vom Primzahlgrad durchführen kann. Dazu benötigen wir noch den folgenden Frobeniusschen[14]) Satz für den wir einen einfachen Beweis geben:

[13]) Vgl. z. B. E. Hecke: Vorlesungen über die Theorie der algebraischen Zahlen. Leipzig 1923. S. 67 — 68.

[14]) G. Frobenius: Gegenseitige Reduktion algebraischer Körper. Math. Annalen 70 (1911), S. 457 — 458.

Satz 8. Voraussetzung: *K_1 bzw. K_2 ist ein vollkommener algebraischer Körper vom Grade n_1 bzw. n_2. Der Grad des Durchschnittes K von K_1 und K_2 beträgt n. K_3 ist das Kompositum von K_1 und K_2 und n_3 sein Grad.*

Behauptung: *Ist K_2 Galoissch, so ist*

$$n_3 = \frac{n_1 n_2}{n}.$$

Beweis. Nehmen wir K als grundlegenden Körper an, so beträgt dann der Grad von K_1 bzw. von K_2 bzw. von K_3 in Bezug auf K $\frac{n_1}{n}$ bzw. $\frac{n_2}{n}$ bzw. $\frac{n_3}{n}$. Es bezeichne $\mathfrak{K}$ den kleinsten Galoisschen Körper der K_3 enthält und $\mathfrak{A}$ seine Automorphismengruppe in Bezug auf K. Ferner gehöre K_1 bzw. K_2 innerhalb $\mathfrak{K}$ in Bezug auf K zur Untergruppe $\mathfrak{A}_1$ bzw. $\mathfrak{A}_2$ von $\mathfrak{A}$. Da K_2 Galoissch ist, so ist $\mathfrak{A}_2$ Normalteiler von $\mathfrak{A}$. Mithin bildet das Produkt $\mathfrak{A}_1\mathfrak{A}_2$ eine Gruppe. Also gehört der Durchschnitt K von K_1 und K_2 zu $\mathfrak{A}_1\mathfrak{A}_2$. Da K den grundlegenden Körper bildet, so ist $\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2$. Mit $\mathfrak{A}_3$ bezeichnen wir jetzt die Gruppe zu der K_3 innerhalb $\mathfrak{K}$ in Bezug auf K gehört. Bekanntlich ist der Durchschnitt von $\mathfrak{A}_1$ und $\mathfrak{A}_2$ mit der Gruppe $\mathfrak{A}_3$ identisch (übrigens kann man dies leicht in unmittelbarer Weise zeigen). Es ist also, wenn $\delta(X)$ die Ordnung des Komplexes X bezeichnet,

$$\delta(\mathfrak{A}_1)\,\delta(\mathfrak{A}_2) = \delta(\mathfrak{A})\,\delta(\mathfrak{A}_3). \tag{1}$$

Andererseits ist

$$\delta(\mathfrak{A}_1) = \mathrm{Ind}(\mathfrak{A}_3, \mathfrak{A}_1)\,\delta(\mathfrak{A}_3); \quad \delta(\mathfrak{A}_2) = \mathrm{Ind}(\mathfrak{A}_3, \mathfrak{A}_2)\,\delta(\mathfrak{A}_3);$$

$$\delta(\mathfrak{A}) = \mathrm{Ind}(\mathfrak{A}_3, \mathfrak{A})\,\delta(\mathfrak{A}_3),$$

wo $\mathrm{Ind}(X, Y)$ den Index von X in Bezug auf Y bezeichnet. Da aus $\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2$ $\mathrm{Ind}(\mathfrak{A}_3, \mathfrak{A}_1) = \mathrm{Ind}(\mathfrak{A}_2, \mathfrak{A})$ folgt, so ist

$$\delta(\mathfrak{A}_1) = \frac{n_2}{n}\delta(\mathfrak{A}_3), \quad \delta(\mathfrak{A}_2) = \frac{n_1}{n}\delta(\mathfrak{A}_3), \quad \delta(\mathfrak{A}) = \frac{n_3}{n}\delta(\mathfrak{A}_3).$$

Setzen wir dies in (1) ein, so erhalten wir

$$\frac{n_1}{n}\frac{n_2}{n} = \frac{n_3}{n}; \qquad n_3 = \frac{n_1 n_2}{n}.$$

Die Arithmetisierung der genannten Theorie der algebraisch-auflösbaren Polynome ergibt sich mittels des folgenden Satzes.

Satz 9: *Damit das ganze ganzzahlige Polynom $f(x)$ vom Primzahlgrad n algebraisch-auflösbar sei, ist notwendig und hinreichend, dass*

1) *die Primzahlen p, für die $f(x)$ mod p linear zerlegbar ist, mit endlich vielen Ausnahmen, bezüglich einer gewissen natürlichen Zahl m, mod m einer Untergruppe $\mathfrak{B}_1$ der vollen multiplikativen Restgruppe $\mathfrak{B}$ von m gehören,*

2) *die Faktorgruppe $\mathfrak{B}/\mathfrak{B}_1$ zyklisch sei,*

3) *die Primzahlen p, die zu $\mathfrak{B}_1$ gehören und für die $f(x)$ mod p einen Linearfaktor hat, mit endlich vielen Ausnahmen die Eigenschaft haben, dass für sie $f(x)$ mod p linear zerlegbar ist.*

Beweis. Zunächst beweisen wir, dass die gennanten Bedingungen notwendig sind. Wir nehmen also an, dass $f(x)$ ein ganzzahliges algebraisch-auflösbares Polynom vom Primzahlgrad n ist und wir beweisen, dass mit endlich vielen Ausnahmen, diejenigen Primzahlen für die $f(x)$ mod p linear zerlegbar ist, nach einer gewissen Zahl m mod m, eine Untergruppe $\mathfrak{B}_1$ der mod m vollen multiplikativen Gruppe $\mathfrak{B}$ bilden, wo $\mathfrak{B}/\mathfrak{B}_1$ zyklisch ist. Dagegen gehören die Primzahlen, für die $f(x)$ linear nicht zerlegbar ist, doch Linearfaktoren enthält, mit endlich vielen Ausnahmen, nicht zu $\mathfrak{B}_1$. Dazu betrachten wir die Galoissche Gruppe $\mathfrak{A}$ von $f(x)$, die bekanntlich einen zyklischen Normalteiler $\mathfrak{N}$ von Ordnung n enthält, dabei lassen alle anderen, die zu $\mathfrak{N}$ nicht gehörigen Permutationen von $\mathfrak{A}$, ausser der Einheitspermutation, genau eine Ziffer unverändert. Die Gruppe $\mathfrak{A}$ können wir also als direktes Produkt

$$\mathfrak{A} = \mathfrak{L}\,\mathfrak{N} \tag{1}$$

darstellen, wo $\mathfrak{L}$ sämtliche Permutationen enthält, die eine feste Ziffer unverändert lassen. Mit $\mathfrak{K}$ bezeichnen wir den kleinsten Galoisschen Körper, der durch die Wurzeln von $f(x)$ gebildet ist. Ferner bezeichnen wir mit $\mathfrak{K}_1$ den Unterkörper von $\mathfrak{K}$, der zur Gruppe $\mathfrak{N}$ gehört. $\mathfrak{K}_1$ ist also Galoissch und ihre Automorphismengruppe ist mit der Faktorgruppe $\mathfrak{A}/\mathfrak{N}$, also mit der Gruppe $\mathfrak{L}$, isomorph[15]). Nun ist bekanntlich $\mathfrak{L}$ zyklisch[16]), also ist $\mathfrak{K}_1$ ebenfalls zyklisch. Nach einem wohlbekannten Kronecker-Weberschen Satze über die Einbettung Abelscher Körper[17]),

[15]) s. z. B. H. Weber: Kleines Lehrbuch der Algebra, Braunschweig 1921, S. 262.

[16]) vgl. z. B. [15]) S. 385 — 389, Besonders S. 389.

[17]) vgl. z. B. den Hilbertschen Beweis des gennanten Satzes: D. Hilbert. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. Werke I S. 53—62.

muss also $\mathfrak{K}_1$ Unterkörper des Körpers gewisser m-ter Einheitswurzeln sein. Jetzt bezeichnen wir mit $\varphi(x)$ das ganze ganzzahlige irreduzible Polynom, dessen Wurzeln $\mathfrak{K}_1$ bestimmen. Nach Satz 4 gehören die Primzahlen p, für die $\varphi(x)$ mod p linear zerlegbar ist, mit endlich vielen Ausnahmen, zu einer Untergruppe $\mathfrak{B}_1$ der vollen multiplikativen Restgruppe mod m. Ist $F(x)$ das normale irreduzible Polynom, das den Körper $\mathfrak{K}$ bestimmt, so gehören also nach dem (Kronecker-Bäuerschen Einbettugssatz) Satz 7 auch die Primzahlen p, für die $F(x)$ mod p linear zerlegbar ist, zur Gruppe $\mathfrak{B}_1$. Mithin haben auch die Primzahlen p, mit endlich vielen Ausnahmen, für die $f(x)$ mod p linear zerlegbar ist, dieselbe Eigenschaft. Da wegen (1) $\mathfrak{K}$ Produkt von $\mathfrak{K}_1$ und $\mathfrak{K}_2$ ist, so kann man annehmen, dass die Wurzeln von $F(x)$ die Gestalt $t\alpha_i + t_1\beta_j$ haben, wo α_i die von $f(x)$ und β_j die Wurzeln von $\varphi(x)$ bedeuten, und t und t_1 ganze rationale Zahlen bezeichnen [18]). Haben also $f(x)$ und $\varphi(x)$ mod p Linearfaktoren, so wird auch $F(x)$ nach dem Schurschen Prinzip einen solchen haben. Dann ist aber $F(x)$ als normales Polynom mod p linear zerlegbar. Demnach muss $f(x)$ mod p linear zerlegbar sein.

Umgehehrt wenn die Primzahlen p, nach denen $f(x)$ linear zerlegbar ist, mit endlich vielen Ausnahmen, zu der Untergruppe $\mathfrak{B}_1$ der vollen multiplikativen Restgruppe $\mathfrak{B}$ mod m gehören, so enthält der Galoissche Körper $\mathfrak{K}$ von $f(x)$, nach (dem Kronecker-Bauerschen Einbettungssatz) Satz 7 und Satz 4, einen Kreisteilungskörper K_2 vom Grade i, wo i der Index von $\mathfrak{B}_1$ in Bezug auf $\mathfrak{B}$ bezeichnet. Ist K_1 der durch die Wurzel α von $f(x)$ gebildete Körper, so beträgt der Grad des Kompositums K_3 von K_1 und K_2 nach Satz 8, da K_1 primitiv ist, in. Es sei γ ein primitives Element von K_3 und $\psi(x)$ das ganze ganzzahlige Polynom, dessen Wurzeln gleich $t\alpha_i + t_1\beta_j$ sind. (Bekanntlich kann man $\gamma = t\alpha + t_1\beta$ annehmen [13])). Da K_2 Unterkörper von K_3 ist, so enthält $\psi(x)$ nur nach solchen Primzahlen p Linearfaktoren, die mod m zu $\mathfrak{B}_1$ gehören: Ist $x - A$ ein Linearfaktor von $\psi(x)$ mod p, so ist $x - A$ ebenfalls Linearfaktor mod p eines gewissen im rationalen Körper irreduziblen Teilers $\psi_1(x)$ von $\psi(x)$. Bedeutet $t\alpha_i + t_1\beta_j$ eine Wurzel von $\psi_1(x)$, so ist offenbar $t\alpha_i + t_1\beta_j$ primitives Element des Kompositums $\mathfrak{K}_i$ der Körper K_i' und K_2, wo K_i' denjenigen konjugierten Körper von K_1 bezeichnet, dessen primitives Element α_i ist. Mithin haben nach Satz 6 auch $f(x)$ und $\Theta(x)$, wo $\Theta(x)$ das irreduzible gannzzahlige Polynom bezeichnet, dessen Wurzeln K_2 bestimmen, mit endlich vielen Ausnahmen, mod p zugleich Linearfaktoren, wenn nur $\psi_1(x)$, also wenn nur $\psi(x)$ einem solchen hat. Demnach kann, nach dem Schurschen Prinzip, $\psi(x)$ höchstens nur für endlich viele Primzahlen Linearfaktoren enthalten und dabei nach diesen Primzahlen linear nicht zerlegbar sein.

Aus der Kroneckerschen Dichtigkeitsformel (s. (1) des Beweises des Satzes 7; vgl. auch den Beweis der Folgerung 2 des Satzes IV [1])) erhält man unmittelbar, dass $\psi(x)$ ein normales Polynom ist. Mithin ist der Galoissche Körper $\mathfrak{K}$ von $f(x)$ mit K_3 identisch, d. h. der Grad von $\mathfrak{K}$ beträgt in. Die Automorphismengruppe von $\mathfrak{K}$ ist also dem Produkt $\mathfrak{A}_1\mathfrak{N}_1$ isomorph, wo $\mathfrak{N}_1$ eine zyklische Gruppe von der Ordnung n ist und $\mathfrak{A}_1$ der Automorphismengruppe von K_2 isomorph ist. Da $\mathfrak{A}_1$ Abelsch ist, so ist $\mathfrak{N}_1\mathfrak{A}_1$ auflösbar.

Anmerkung 1. Im zweiten Teile des Beweises des letzten Satzes haben wir nur die Tatsache ausgenützt, dass $\mathfrak{B}/\mathfrak{B}_1$ Abelsch ist, dagegen nicht, dass $\mathfrak{B}/\mathfrak{B}_1$ zyklisch ist. Das zweite folgt nämlich daraus, dass n prim ist.

Anmerkung 2. Den Fall, wo $\mathfrak{B}_1$ nur durch die Formen $nx \pm 1$ repraesentiert ist, hat U. Wegner [5]) bewiesen. Dann kann man, wie Wegner gezeigt hat, die Voraussetzung, dass „die Primzahlen für die $f(x)$ mod p Linearfaktoren hat, aber nicht linear zerlegbar ist, mit endlich vielen Ausnahmen zu $nx \pm 1$ nicht gehören" weglassen.

Endlich gehen wir zur Verallgemeinerung des Satzes V [1]) über. Dazu benötigen wir den folgenden Hilfssatz.

Hilfssatz. Voraussetzung: *$f(x)$ ist ein über dem Integritätsbereich I normiertes Polynom. $f(x) = f_1(x)f_2(x)$ ist im Quotientenkörper K von I Produkt zweier normierter Polynome $f_1(x)$, $f_2(x)$. Es existiert eine Erweiterung I_1 von I in dem jedes Element von I_1 durch Primelemente, von Einheiten abgesehen, eindeutig darstellbar ist. Gehören a und b zu I und ist b kein Teiler von a in I, so ist b auch kein Teiler von a in I_1.*

Behauptung: *Die Koeffizienten von $f_1(x)$ und $f_2(x)$ gehören zum Integritätsbereich I.*

Beweis. Mit $x_1, x_2, \ldots, x_m$ bezeichnen wir die Wurzeln von $f_1(x)$ (vgl. die Voraussetzung des Satzes). Aus $f_1(x) = (x - x_1) \ldots (x - x_m)$ erhält man, dass die Koeffizienten von $f_1(x)$, da sie durch Addition und Multiplikation ganzer über I algebraischer Elemente gebildet sind, ebenso ganz algebraisch sein müssen. Demgemäss ist jeder Koeffizient $\frac{a_i}{b_i}$ von $f_i(x)$, wo a_i, b_i zu I gehören, Wurzel eines normierten Polynoms. Nehmen wir an, dass $\frac{a_i}{b_i} = \frac{A_i}{B_i}$, wo A_i und B_i zu I_1 gehören und in I_1 keinen von Einheiten verschiedenen gemeinsamen Faktor haben, Wurzel eines Polynoms $F(x) = x^t + C_1 x^{t-1} + \ldots + C_t$ ist, wo C_j, $j = 1, 2, \ldots, t$, zu I_1 gehören, so folgt aus

$$B_i^t F\left(\frac{A_i}{B_i}\right) = A_i^t + C_1 A_i^{t-1} B_i + \cdot\ \cdot\ \cdot\ \cdot + C_t B_i^t = 0,$$

dass A_i^t und B_i in I_1 einen gemeisamen Teiler haben. Da in I_1 sämtliche Elemente durch Primelemente, von Einheiten abgesehen, darstellbar sind, so haben auch A_i und B_i einen gemeinsamen, von Einheiten verschiedenen, Faktor. Dies ist aber nur dann möglich, wenn B_i eine Einheit ist. Mithin ist b_i Teiler von a_i.

Anmerkung. Die Voraussetzungen des vorstehenden Hilfssatzes sind nicht nur hinreichend, sondern auch notwendig. Um dies einzusehen, geben wir eine Klasse von in I normierten Polynomen an, die im Quotientenkörper von I reduzibel, aber in I selbst irreduzibel sind. Es bestehe nämlich I aus $a+b\sqrt{D}$, wo a und b beliebige ganze rationale Zahlen sind und D eine ganze rationale quadratfreie Zahl bezeichnet. Es sei

I. $a+b\sqrt{D} = a_1+b_1\sqrt{D}$, für $a=a_1$, $b=b_1$;

II. $a+b\sqrt{D} \pm (a_1+b_1\sqrt{D}) = (a\pm a_1)+(b\pm b_1)\sqrt{D}$;

III. $(a+b\sqrt{D})(a_1+b\sqrt{D}) = a a_1 + D b b_1 + (a b_1 + b a_1)\sqrt{D}$.

Es ist klar, dass diese Elemente einen Integritätsbereich I bilden. Ist jetzt $0 > D = 1-4K$, so haben wir

$$x^2+x+K = \left(x+\frac{1+\sqrt{D}}{2}\right)\left(x-\frac{1-\sqrt{D}}{2}\right).$$

Satz 10: *Damit ein normiertes ganzes ganzzahliges Polynom $f(x)$ mit endlich vielen Ausnahmen nur Primteiler haben soll, die zugleich Primteiler der Form x^2-Dy^2 sind, D-quadratfrei, ist es notwendig und hinreichend, dass $4f(x)$ durch die Form $f(x)^2-Df_2(x)^2$ darstellbar sei, wo $f_1(x)$, $f_2(x)$ zugleich ganze ganzzahlige Polynome sind.*

Beweis. Nach der Eulerschen Identität genügt es den Satz für solche $f(x)$ zu beweisen, die im rationalen Körper irreduzibel sind. I. Zunächst zeigen wir, dass, wenn für gewisse ganze ganzzahlige Polynome $F_1(x)$, $F_2(x)$

$$F_1(x)^2 - D F_2(x)^2 \equiv 0 \pmod{f(x)},\quad (F_1(x), F_2(x), f(x)) = 1,$$

so existieren ganze ganzzahlige Polynome $f_1(x)$, $f_2(x)$, für die

$$4f(x) = f_1(x)^2 - D f_2(x)^2.$$

Ist nämlich $P(x)$ ein im absolut quadratischen Körper $K(\sqrt{D})$ normierter irreduzibler Teiler von $f(x)$, so muss $P(x)$ entweder in $F_1(x)+\sqrt{D}F_2(x)$ oder in $F_1(x)-\sqrt{D}F_2(x)$ aufgehen. Da $(F_1(x), F_2(x), f(x)) = 1$, so ist $\overline{P(x)} \neq P(x)$, wo $\overline{P(x)}$ konjugiert zu $P(x)$ ist, d. h. $\overline{P(x)}$ Koeffizienten hat, die zu den Koeffizienten von $P(x)$ konjugiert sind. Es existieren also solche in $K(\sqrt{D})$ irreduzible Teiler $P_i(x)$, $i=1, 2, \ldots g$, von $F_1(x)+\sqrt{D}F_2(x)$, für die

$$f(x) = \varepsilon P_1(x) P_1(x) \ \ldots\ . P_g(x)\overline{P_g(x)}, \tag{1}$$

wo ε eine Einheit von $K(\sqrt{D})$ bezeichnet. Da im absolut quadratischen Körper $K(\sqrt{D})$ eine Idealtheorie existiert, so können wir den vorstehenden Hilfssatz anwenden. Demnach sind die Koeffizienten von $P_i(x)$ ganze Zahlen des Körpers $K(\sqrt{D})$ und in

$$2P_1(x) \ \ldots\ . P_g(x) = U(x) + \sqrt{D}\, V(x)$$

sind $U(x)$ und $V(x)$ ganze ganzzahlige Polynome. Aus

$$2\overline{P_1(x)} \ \ldots\ . \overline{P_g(x)} = U(x) - \sqrt{D}\, V(x)$$

und (1) folgt also die Darstellbarkeit von $4f(x)$ durch $F_1(x)^2 - DF_2(x)^2$, mit ganzen ganzzahligen $F_1(x)$ und $F_2(x)$.

II. Wie im Beweise des Satzes V [1]) bleibt noch zu zeigen, dass die Bedingungen des Satzes hinreichend sind. Es habe also $f(x)$ mod p, mit endlich vielen Ausnahmen, dann und nur dann einen Linearfaktor, wenn die Kongruenz $x^2 \equiv D \pmod{p}$ in rationalen Zahlen lösbar ist. Nach dem (Kronecker-Bauerschen Einbettungssatz) Satz 7 enthält der Körper $K(\alpha)$, wo α eine Wurzel des Polynoms $f(x)$ ist, die Zahl $\sqrt{D}$. Es sei $\varphi(\alpha) = \sqrt{D}$, d. h. $\varphi^2(\alpha) - D = 0$, wo $\varphi(\alpha)$ ein rationalzahliges Polynom von α ist. Das Polynom $\varphi^2(x) - D$ hat also eine gemeinsame Wurzel mit dem irreduziblen Polynom $f(x)$ und demnach ist $\varphi^2(x) - D$ durch $f(x)$ teilbar. Nach I. ist also der Satz bewiesen.

Anmerkung. Der Sonderfall $D = -1$ ergibt den Satz V [1]). Nun bemerken wir, dass der Satz 10 als Ausgangspunkt eines neuen Zweiges der Zahlentheorie, namentlich der Polynomformentheorie angesehen werden kann. Dies werden wir in einer zukünftigen Arbeit ausführlicher betrachten.

(Eingegangen am 14. November 1935.)