$$\int^{*} d\alpha << X^{-m+3mc_{34}}.$$

Cette contribution est donc

$$<< X^{-m-\frac{1}{2}c_{33}} g_1 \dots g_n \sqrt{R} \sum_t w(t)$$

$$<< X^{-\frac{1}{2}c_{33}} (X^{-2m} g_1^2 \dots g_n^2 + R) \sum_t w(t).$$

Pour les autres points α et β il découle des conditions du théorème C, qu'on a

$$\sum_t w(t)\, e\Big(\sum_\mu (\beta_\mu - \alpha_\mu) t_\mu\Big) << X^{-c_{35}} \sum_t w(t),$$

où c_{35} est positif et fixe; la contribution de ces points est donc

$$<< X^{-c_{35}} I_{13} \sum_t w(t),$$

où I_{13} désigne l'intégrale qui est $\leqslant R$. Cette dernière contribution est donc $<< X^{-c_{35}} R \sum_t w(t)$.

De cette manière les trois théorèmes fondamentaux sont complètement démontrés.

(Reçu le 18 janvier 1939.)

Zur Arithmetisierung des Beweises des Minkowskischen Diskriminanten und Kronecker-Weberschen Einbettungssatzes.

Von

S. Lubelski (Warszawa).

E. Noether hat das Problem gestellt, einen arithmetischen Beweis für den Minkowskischen Diskriminantensatz (d. h. ohne Zuhilfenahme des Begriffes der reellen Zahl) zu finden*). In dieser Arbeit zeigen wir, wie sich der genannte Beweis für algebraisch auflösbare Polynome arithmetisieren lässt (vgl. Satz 5). Dieser Beweis ist von wesentlicher Bedeutung bei der Arithmetisierung des Beweises des Kronecker-Weberschen Einbettungssatzes,

die ebenfalls hier durchgeführt wird (vgl. Satz 9).

Als Anwendung hiervon geben wir einen arithmetischen Beweis des folgenden, auf algebraisch auflösbare Polynome beschränkten, Radosschen Satzes:

Ist $f(x)$ ein irreduzibles ganzzahliges algebraisch auflösbares Polynom vom Grade $n \geqq 2$, so gibt es unendlich viele Primzahlen p, für die $f(x)$ nicht in Linearfaktoren mod p *zerlegbar ist* (vgl. Satz 10).

§ 1. Arithmetischer Beweis des Minkowskischen Diskriminantensatzes für algebraisch auflösbare Polynome.

Wir benutzen oft die folgenden wohlbenkannten Sätze:

Hilfssatz 1. *Damit das Quadrat eines Ideals des algebraischen Körpers*

*) Auf diese Noethersche Fragestellung hat mich in liebenswürdiger Weise Herr N. Tschebotarëw aufmerksam gemacht.

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

K in einer rationalen Primzahl p aufgehe, ist notwendig und hinreichend, dass p Teiler der Diskriminante des Körpers K sei.

Anmerkung. Einen kurzen Beweis dieses Dedekindschen Diskriminantensatzes hat unlängst N. Tschebotarëw gegeben [2]).

Hilfssatz 2. Voraussetzung: *$\mathfrak{P}$ sei ein Primideal des Galoisschen Körpers K. p eine rationale Primzahl, die durch $\mathfrak{P}$ teilbar ist. Ferner bezeichne $\mathfrak{S}$ die Automorphismengruppe von K, g_z die Zerlegungsgruppe von $\mathfrak{P}$ und r_t die Ordnung der Trägheitsgruppe von $\mathfrak{P}$.*

Behauptung: *Ist* $\mathfrak{S} = g_z + s_1 g_z + \ldots + s_{n_3-1} g_z$, *so ist*

$$p = [\mathfrak{P}(s_1\mathfrak{P})(s_2\mathfrak{P})\ldots s_{n_3-1}\mathfrak{P})]^{r_t},$$

wo $s_i\mathfrak{P}$ von einander verschiedene Primideale bezeichnen.

Anmerkung. Wir bezeichnen immer mit $s_i\mathfrak{P}$ das Ideal, welches sich aus $\mathfrak{P}$ ergibt, wenn man in $\mathfrak{P}$ die Substitution s_i durchführt. Einen einfachen Beweis dieses Hilfssatzes findet man z. B. in [3]) S. 487 — 488.

Für unseren arithmetischen Beweis des Minkowskischen Diskriminantensatzes ist der folgende Kummersche Satz von fundamentaler Bedeutung:

Definition. *p und q seien ungerade ganze rationale Primzahlen und g eine feste primitive Wurzel* mod *q. Für eine ganze ratonale Zahl u,* $(u, q) = 1$, *bezeichnen wir mit* ind *u die kleinste natürliche Zahl, für die* $g^{ind\,u} \equiv u \bmod q$ *ist. Ist* $q \equiv 1 \bmod p$, *so sei* ε *bzw.* ρ *eine beliebige* (aber hier feste) *primitive p-te bzw. q-te Einheitswurzel. Ferner bedeute* $[1, \rho] = \sum_{n=1}^{q=1} \rho^n$ *und* $[\varepsilon, \rho]$ *die Lagrangesche Wurzelzahl*

$$[\varepsilon, \rho] = \sum_{n=1}^{q-1} \varepsilon^{ind\,n} \rho^n.$$

Hilfssatz 3 (Kummer[4])). *Die p-te Potenz der Lagrangeschen Wurzelzahl* $[\varepsilon, \rho]$ *ist im Körper K_ρ der p-ten Einheitswurzel ε folgendermassen in Primidealfaktoren $\mathfrak{P}_{n'}$ zerlegbar:*

[2]) N. Tschebotarëw: Kurzer Beweis des Diskriminantensatzes. Acta Arithmetica 1 (1936), S. 78 — 83.

[3]) P. Bachman: Allgemeine Arithmetik der Zahlkörper. Leipzig 1905.

[4]) für den Beweis dieses Satzes vgl. z. B. a) H. Weber: Lehrbuch der Algebra. II. (1896), S. 628—638; oder b) E. Landau: Vorlesungen über Zahlentheorie. III. (1927) S. 292—295.

$$[\varepsilon, \rho]^p = \prod_n \mathfrak{P}_{n'}^n, \qquad \mathfrak{P}_{n'} = (q, \varepsilon - g^{n\frac{q-1}{p}}),\ n < p,\ n\,n' \equiv 1 \pmod p,$$

wobei $\varepsilon, \rho, p, q, [\varepsilon, \rho]$ durch die vorstehende Definition bestimmt sind.

Satz 1. *Ist* $\psi_n = \psi(\varepsilon^n) \neq 0, n = 1, 2, \ldots, p-1$, *ein solches System ganzer konjugierter Idealzahlen des Körpers $K_\rho(\varepsilon)$ der p-ten Einheitswurzel ε, wo p eine ungerade Primzahl ist und ψ_n^ρ sowie $\psi_n^{-1}\psi_1^n$ zur Hauptklasse gehören, so gehören ψ_n ebenfalls zur Hauptklasse.*

Beweis. I. *Es sei*

$$\psi_n = \lambda^t \varphi_n, \quad \psi = \psi_1, \quad \varphi = \varphi_1, \quad \lambda = 1 - \varepsilon, \quad (\varphi, \lambda) = 1.$$

Mit ψ_n bzw. φ_n gehört auch φ_n bzw. ψ_n zur Hauptklasse. Offenbar erfüllen auch die φ_n die Bedingungen des Satzes und mithin können wir $(\psi_n, \lambda) = 1$ annehmen. Nun sei $P \neq p$ eine ungerade Primzahl, für welche

$$(1) \qquad P = \prod_i \mathfrak{p}_i'(\varepsilon^i), \quad \psi = \xi \prod_i \mathfrak{p}(\varepsilon^i)^{ki}, \quad (P, \xi) = 1,$$

wo $\mathfrak{p}(\varepsilon^i)$ Primideateiler von P in K_ρ sind. Da P in der Diskriminante von K_ρ nicht aufgeht, enthält P nach dem Dedekindschen Diskriminantensatz (vgl. Hilfssatz 1) keine Quadratteiler. Also enthält die Trägheitsgruppe von $\mathfrak{p}$ nach Hilfssatz 2, nur die Einheitssubstitution. Die Zerlegungsgruppe g_z von $\mathfrak{p}$ ist mithin nach einem Hilbertschen Satz[5]) zyklisch und von der Ordung f, wo f den Grad von $\mathfrak{p}$ bezeichnet. Ist g eine primitive Wurzel mod p, so ist die Automorphismengruppe von $K_\rho(\varepsilon)$ mit der zyklischen Gruppe

$$(2) \qquad g, g^2, \ldots, g^{p-1} \pmod p$$

isomorph. Die Zerlegungsgruppe g_z von $\mathfrak{p}$ ist also mit der Gruppe

$$(3) \qquad g^e, g^{2e}, \ldots, g^{fe} \pmod p, \quad e = \frac{p-1}{f},$$

isomorph. Bezeichnet R die Gruppe (2) und g_z' die Gruppe (3), so sind die Zahlen $t_1, t_2, \ldots, t_{e-1}$, die die Nebengruppen von g_z' in Bezug auf R bestimmen, dadurch gekennzeichnet, dass 1) ihre Anzahl $e-1$ beträgt, 2) zwei verschiedene Zahlen t_h, t_j aus dieser Menge untereinander und zugleich mit $\frac{t_h}{t_j}$ von den Zahlen (3) mod p verschieden sind. Nun haben

[5]) vgl. z. B. D. Hilbert: Werke I, 1932, S. 15.

die Zahlen $g, g^2, \ldots, g^{e-1}$ die genannten Eigenschaften. Demnach ist, für $T = \sum_{m=1}^{e} t_m$,

$$T = \sum_{m=1}^{e} t_m \equiv \frac{g^e - 1}{g - 1} \pmod{p}, \quad t_e = 1.$$

Wäre T durch p teilbar, so wäre $g^e \equiv 1 \bmod p$, d. h. $e = p-1$, $f = 1$. Mithin ist T für Primideale $\mathfrak{p}$, die nicht vom ersten Grade sind, durch p nicht teilbar.

Multiplizieren wir miteinander diejenigen Konjugierten der beiden Seiten der Gleichung (1), welche den Zahlen $u = t_j$, $j = 1, 2, \ldots, e$, entsprechen, so erhalten wir

$$\prod_u \psi_u = A \prod_u \xi_u, \quad \psi_u = \xi_u \prod \mathfrak{p}\,(\varepsilon^{iu})^{k_i},$$

wo A Potenz von P ist und $\prod \xi_u$ mit $\gamma = \prod \psi_u$ äquivalent ist. Nun ist γ nach Voraussetzung unseres Satzes mit ψ^T äquivalent. Mithin erhalten wir im Falle, wenn T durch p nicht teilbar ist, also, wenn die Gleichung $Tx + py = 1$ in ganzen rationalen Zahlen lösbar ist, da nach Voraussetzung ψ^p zur Hauptklasse gehört, dass mit γ auch

$$\psi = (\psi^T)^x (\psi^p)^y \tag{4}$$

zur Hauptklasse gehört. Es genügt also zu zeigen, dass γ zur Hauptklasse gehört. Da auch die Zahlen $\gamma_s = \prod \psi_{us}$, wegen $\psi_{us}^{-1} \psi_u^s = \psi_{us}^{-1} \psi^{us} b^s$, wo b zu $K_p(\varepsilon)$ gehört, die Voraussetzungen des Satzes erfüllen, so können wir nach iterierter Anwendung unseres Verfahrens annehmen, dass ψ nur Primidealteiler vom erstem Grade $\mathfrak{p}_\lambda = 1 - \varepsilon$ enthält.

II. Es sei ein System konjugierter Primideale $\mathfrak{p}_{an'}$ gegeben, wo a und n' ganze rationale Zahlen sind, für die $(an', p) = 1$ und an' ein volles multiplikatives Restsystem mod p durchläuft.

Aus Hilfssatz 3 erhält man

$$[\varepsilon^a, \rho]^p = \prod_n \mathfrak{p}_{an'}^n, \quad nn' \equiv 1 \pmod{p},$$

wo der Exponent n auf seinen kleinsten Rest mod p reduziert werden muss, und das Produkt des Exponenten mit dem Index eines Primidealfaktors mod p konstant und gleich a ist. Da nach I. die Zahlen ψ_t als Produkte von Primidealen ersten Grades angenommen werden können, kann man

$$\prod_n \psi_{an'}^a = \Phi_a = \eta_a \Theta_a^p, \quad nn' \equiv 1 \pmod{p}, \tag{5}$$

setzen, wo Θ_a Produkt Lagrangescher Wurzelzahlen ist und η_a eine Idealeinheit bezeichnet. Da nach einer wohlbekannten Relation (vgl. z. B. [4]) a) I. § 169, Relationen (14) und (16) oder II. S. 633 Relation (9)) das Produkt $[\varepsilon, \rho]^a [\varepsilon^a, \rho]^{-1}$ zum Körper $K_p(\varepsilon)$ gehört (was man übrigens unmittelbar verifiziert), so gehört auch $\Theta_1^a \Theta_a^{-1}$ zu $K_p(\varepsilon)$. Nun müssen auch im Produkte Φ_a aus (5) die Exponenten auf ihren kleinsten positiven Rest mod p reduziert werden. Dagegen sind die Indizes von ψ_t nur mod p bestimmt. Demgeäss ergibt sich nach Substitution von n' durch $a'n'$, $aa' \equiv 1 \bmod p$, dass $\Phi_a = \prod_n \psi_{n'}^{an - p\left[\frac{an}{p}\right]}$. Aus $\Phi_1 = \prod \psi_{n'}^n$ folgt

$$\Phi_1^a \Phi_a^{-1} = \prod_n \psi_{n'}^{p\left[\frac{an}{p}\right]} = \bar{\eta}_a \beta^p, \quad \left(\frac{\prod \psi_{n'}^{\left[\frac{an}{p}\right]}}{\beta}\right)^p = \eta_a'^p,$$

wo $\bar{\eta}_a = \eta_a'^p$ und η_a' Idealeinheiten von $K_p(\varepsilon)$ sind. Also ist

$$\prod \psi_{n'}^{\left[\frac{an}{p}\right]} = \eta_a' \beta.$$

Mithin ergibt sich aus der Äquivalenz von $\psi_{n'}$ mit $\psi^{n'}$, dass $\prod_n \psi_{n'}^{\left[\frac{an}{p}\right]}$ und $\psi_1^{\sum n'\left[\frac{an}{p}\right]}$ zugleich zur Einheitsklasse gehören.

III. Zeigen wir, dass für ein gewisses durch p nicht teilbares a, $\sum_n n' \left[\frac{an}{p}\right]$ durch p nicht teilbar ist, so sieht man, wie in (4), dass ψ mit einer ganzen Zahl a aus $K_p(\varepsilon)$ assoziiert ist. Die Existenz einer solchen Zahl n beweist man folgendermassen: Es sei $\{x\} = x - [x]$ also

$$\frac{an}{p} = \left[\frac{an}{p}\right] + \left\{\frac{an}{p}\right\}, \quad \frac{(p-a)n}{p} = \left[\frac{(p-a)n}{p}\right] + \left\{\frac{(p-a)n}{p}\right\}$$

und hieraus durch Addition

$$n = \left[\frac{an}{p}\right] + \left[\frac{(p-a)n}{p}\right] + \left\{\frac{an}{p}\right\} + \left\{\frac{(p-a)n}{p}\right\}.$$

Die Summe $\left\{\frac{an}{p}\right\}+\left\{\frac{(p-a)n}{p}\right\}$ ist also ganz rational und mithin gleich 1.

Folglich ist

$$\left[\frac{an}{p}\right]+\left[\frac{(p-a)n}{p}\right]=n-1;\quad \sum_n{}' \left[\frac{an}{p}\right]+\sum_n{}' \left[\frac{(p-a)n}{p}\right]\equiv -1 \pmod p.$$

Demnach können nicht beide Summen auf der linken Seite dieser Kongruenz durch p teilbar sein, womit der Satz bewiesen ist.

Anmerkung. Diesen Hilfssatz hat H. Weber [4] a), S. 651-665 für beliebige Primzahlpotenzen bewiesen. Da für primzahliges p der Beweis sehr gekürzt werden kann, haben wir den vorstehenden Beweis angeführt.

Satz 2. *Ist p eine ungerade Primzahl und $f(\varepsilon)$ eine Einheit des Körpers $K_{p^n}(\varepsilon)$ der p^n-ten Einheitswurzel ε, so ist für eine entsprechende Einheit $\psi(\varepsilon)$ von $K_{p^n}(\varepsilon)$, wo $\psi(\varepsilon)=\psi(\varepsilon^{-1})$, $f(\varepsilon)=\pm\varepsilon^t\psi(\varepsilon)$, wobei t eine ganze rationale Zahl ist.*

Beweis. Es sei $\Theta(\varepsilon)$ eine Einheit aus $K_{p^n}(\varepsilon)$, für die $\Theta(\varepsilon)\Theta(\varepsilon^{-1})=1$. Da

$$1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{m-1},\ m=p^{n-1}(p-1),$$

eine Basis von $K_{p^n}(\varepsilon)$ bilden (vgl. z. B. [14] S. 200), so existieren solche ganze rationale Zahlen $y_0, y_1, \ldots, y_{m-1}$, für die

$$\Theta(\varepsilon)=y_0+y_1\varepsilon+\ldots+y_{m-1}\varepsilon^{m-1}.$$

Also ist

$$\varepsilon^{m-1}=\Theta(\varepsilon)\varepsilon^{m-1}\Theta(\varepsilon^{-1})=\Theta(\varepsilon)(y_{m-1}+y_{m-2}\varepsilon+\ldots+y_0\varepsilon^{m-1}).$$

Der Koeffizient von ε^{m-1} der rechten Seite dieser Gleichung beträgt, da $2(m-1)-p^n<m-1$ ist, $\sum_{t=0}^{m-1} y_t^2$, d. h. $\sum_{t=1}^{m-1} y_t^2=1$. Demnach müssen alle y_t mit einer Ausnahme gleich 0 sein, d. h. $\Theta(\varepsilon)=\pm\varepsilon^g$, wo g eine ganze rationale Zahl ist. Nun ist jeder Bruch $\frac{f(\varepsilon)}{f(\varepsilon^{-1})}$, wo $f(\varepsilon)$ eine Einheit von $K_{p^n}(\varepsilon)$ ist, ein solches $\Theta(\varepsilon)$. Also ist $f(\varepsilon)=\pm\varepsilon^g f(\varepsilon^{-1})$. Da eine der Zahlen $g, g+p^n$ für ungerades p gerade ist, so kann man g als nicht negative gerade Zahl annehmen. Nehmen wir zunächst $f(\varepsilon)=-\varepsilon^g f(\varepsilon^{-1})$ an, so folgt aus $\varepsilon\equiv 1 \bmod (1-\varepsilon)$

$$f(\varepsilon)\equiv f(1)\equiv -f(1) \pmod{(1-\varepsilon)},\quad 2f(1)\equiv 2f(\varepsilon)\equiv 0 \pmod{(1-\varepsilon)}.$$

Die letztere Kongruenz ist für ungerades p unmöglich. Also ist $f(\varepsilon)=\varepsilon^g f(\varepsilon^{-1})$ und mithin

$$\varepsilon^{-\frac{1}{2}g} f(\varepsilon)=\varepsilon^{\frac{1}{2}g} f(\varepsilon^{-1}).$$

Setzen wir jetzt $\varepsilon^{-\frac{1}{2}g} f(\varepsilon)=\psi(\varepsilon)$, so ergibt sich $\psi(\varepsilon)=\varepsilon^{\frac{g}{2}}\psi(\varepsilon)$, wobei $\psi(\varepsilon)=\psi(\varepsilon^{-1})$.

Anmerkung. Dieser Satz bildet einen Sonderfall eines Kroneckerschen Satzes. Sein arithmetischer Beweis ist für die Arithmetisierung der Beweise des Minkowskischen, wie auch des Kronecker-Weberschen Satzes von wesentlicher Bedeutung. Der Kroneckersche Satz wurde bisher nur mittels des Begriffes der reelen Zahl bewiesen (vgl. z. B. [5] S. 225 — 227 oder [6]) bzw. [7]).

Hilfssatz 4. *Ist ein Körper K in Bezug auf einen vollkommenen Körper k vom Grade n und in Bezug auf seinen Unterkörper K_i vom Grade i, so ist $n=is$, wenn nur K, in Bezug auf k vom s-ten Grade ist,*

Anmerkung. Den Beweis dieses Satzes kann man in jeder Darstellung der Galoisschen Gleichungstheorie finden; vgl. z. B. [4] a) I. S. 483 — 487.

Hilfssatz 5. *Ist $\mathfrak{D}$ die Diskriminante und $\mathfrak{d}$ die Differente eines (absolut) Galoisschen Körpers K, so ist $\mathfrak{D}$ Potenz von $\mathfrak{d}$.*

Für den Beweis vgl. z. B. [5] S. 131.

Satz 3. *Damit der Unterkörper, bzw. Galoisscher Unterkörper K_1 des Galoisschen Körpers K, Unterkörper des zu dem Primideal $\mathfrak{P}$ gehörigen Trägheitskörpers k_t sei, ist notwendig und hinreichend, dass die Differente $\mathfrak{d}_1$ bzw. Diskriminante $\mathfrak{D}_1$ von K_1 durch $\mathfrak{P}$ bzw. p, wo p, die durch $\mathfrak{P}$ teilbare rationale Primzahl ist, nicht teilbar sei.*

Beweis. I. Mit sehr einfachen Mitteln (vgl. z. B. [5] S. 97 —98) kann man beweisen, dass die Differente eines Unterkörpers Teiler der Differente des entsprechenden Oberkörpers ist. Wollen wir also beweisen, dass die Differente $\mathfrak{d}_1$ von K_1 nicht durch das Primideal $\mathfrak{P}$ teilbar ist, so genügt es, wenn nur K_1 Unterkörper von K_t ist, das für den entsprechenden Trägheitskörper zu zeigen. Dies ist aber bekanntlich leicht zu beweisen (vgl. z. B. [3] S. 515).

II. Die Umkehrung von I. erhält man folgendemassen: Es bezeichne K_1 einen Unterkörper von K, dessen Differente $\mathfrak{d}_1$ durch das Primideal $\mathfrak{P}$ nicht teilbar ist. Ist also $(\xi_1, \xi_2, \ldots, \xi_i)$ eine Basis von K_1, so ist das in K befindliche Ideal

$$\eta_i=\{\xi_1-S\xi_1, \xi_2-S\xi_2, \ldots \xi_i-S\xi_i\},$$

wo S eine beliebige zu K_1 nicht gehörige Substitution der Automorphismengruppe von K bedeutet, durch $\mathfrak{P}$ nicht teilbar. Demnach ist für ein gewisses t $\xi_t-S\xi_t$ durch $\mathfrak{P}$ nicht teilbar, d. h. S gehört nicht zur Trägheitsgruppe g_t von $\mathfrak{P}$. Die Gruppe zu der K_1 gehört, enthält also g_t als Untergruppe. Also ist K_1 Unterkörper des Trägheitskörpers k_t.

III. Nach Hilfssatz 5 ist die Diskriminante $\mathfrak{D}_1$, wenn nur K_1 Galoissch ist, Potenz der Differente $\mathfrak{d}_1$. Ist also $\mathfrak{d}_1$ durch $\mathfrak{P}$ nicht teilbar,

so ist mithin die ganze rationale Zahl $\mathfrak{D}_1$ durch die rationale Primzahl p, wo $\mathfrak{P}|p$, nicht teilbar . Umgehehrt, wäre $\mathfrak{D}_1$ durch p nicht teilbar, so würde $\mathfrak{d}_1$ durch $\mathfrak{P}$ nicht teilbar sein.

Anmerkung. Der letzte Satz findet sich in der Hilbertschen Theorie der Galoisschen Körper in impliziter Form. Der Teil des Satzes, den wir in II. bewiesen haben, findet sich in [5]) S. 139 ausdrücklich formuliert. Doch ist er weder in [3]) noch in [5]) ausführlich bewiesen.

Folgerung: *Ist K Kompositum der Galoisschen Körper K_1 und K_2, so gehen in die Diskriminante $\mathfrak{D}$ von K sämtliche Primteiler von $\mathfrak{D}_1$ und $\mathfrak{D}_2$ auf, wo $\mathfrak{D}_1$ bzw. $\mathfrak{D}_2$ die Diskriminante von K_1 bzw. K_2 bezeichnet. Umgekehrt enthält $\mathfrak{D}$ nur solche Primteiler.*

Beweis. Nach Hilfssaatz 1 geht jeder rationale Primteiler p von $\mathfrak{D}_1$ bzw. von $\mathfrak{D}_2$ in $\mathfrak{D}$ auf. Ist umgekehrt $p|\mathfrak{D}$, $(p, \mathfrak{D}_1\mathfrak{D}_2)=1$, so sind nach Satz 2 K_1 und K_2 Unterkörper von k_t, wo k_t den Trägheitskörper eines beliebigen Primideals $\mathfrak{P}$ von p in K bedeutet. Also ist $K_t=K$ und mithin wäre nach Satz 3 $(p,\mathfrak{D})=1$.

Wir haben jetzt alles bei der Hand um einen arithmetischen Beweis des Kernes des Minkowskischen Diskriminantensatzes, beschränkt auf algebraisch auflösbare Polynome, wie auch des Kronecker-Weberschen Diskriminantensatzes, zu geben.

Satz 4. *Ein absolut zyklischer Körper Q vom Primzahlgrad p ist Unterkörper des Körpers K_{p^s}, bzw. des Körpers K_8 der p^2-ten, bzw. 8-ten Einheitswurzeln, wenn nur die Diskriminante von Q gleich $\pm p^m$ ist, wobei m nicht negativ und ganz rational ist.*

Beweis. I. Die Körper $k(\sqrt{-1})$, $k(\sqrt{-2})$, $k(\sqrt{-2})$ sind die einzigen quadratischen Körper, deren Diskriminanten Potenzen der Zahl 2 sind. Aus

$$x^4+1=(x^2)^2+1=(x^2-1)^2+2x^2=(x^2+1)^2-2x^2$$

folgt unmittelbar, dass diese Körper Unterkörper des Körpers der achten Einheitswurzeln sind. Wir könnnen also $p>2$ annehmen.

Es sei ε eine p-te Einheitswurzel, $\varphi(x)$ das ganze ganzzahlige irreduzible Polynom, dessen Wurzeln $x_1, x_2, \ldots, x_p$ Q bestimmen. Ausserdem seien

$$[\varepsilon^s, x_g]=x_g+\varepsilon^s x_{g+1}+\ldots+\varepsilon^{(p-1)s}x_{p+g-1},\ x_{p+l}=x_l,$$

die „Lagrangeschen Resolventen". Da die Gruppe $\mathfrak{G}$ von $\varphi(x)$ zyklisch ist, kann man die Indizes von x so ordnen, dass für ein bestimmtes ganzzahliges Polynom $\Phi(x)$

$$x_2=\Phi(x_1),\ x_3=\Phi(x_2)=\Phi(\Phi(x_1),\ldots,x_1=x_{p+1}=\Phi(x_p)=\Phi(\underbrace{\Phi\ldots\Phi}_{p\text{-Mal}}(x_1))$$

ist, usw. Es geht also $[\varepsilon^s, x_g]$ aus $[\varepsilon^s, x_1]$ durch die Substitution (x_1, x_g) hervor. Mithin bestehen, wegen $\varepsilon^{(g-1)s}[\varepsilon^s, x_g]=[\varepsilon^s, x_1]$, die Relationen

$$(1)\qquad [\varepsilon^s, x_1]^{-1}[\varepsilon, x_1]^s=\alpha_s,\quad [\varepsilon^s, x_1]^p=v_s,$$

wo α_s und ϑ_s, $s=1,2,\ldots,p-1$, zum Körper $K_p=K_p(\varepsilon)$ der p-ten Einheitswurzel ε gehören, da sie nach den Substitutionen der Automorphismengruppe $\mathfrak{G}$ von $K_p(\varepsilon)$ ihren Wert nicht ändern. Daraus ergibt sich unmittelbar die folgende wichtige Relation

$$\vartheta_s^{-1}\vartheta^s=\alpha_s^p,\quad \vartheta=\vartheta_1.$$

Nehmen wir hier die Normen beider Seiten, so finden wir $N(\vartheta)^{s-1}=a_s^p$, wo a_s eine ganze rationale Zahl bezeichnet. Da p ungerade ist, so kann man unter anderem $s=2$ setzen. Dann erhält man $N(\vartheta)=a_2^p$, d. h. die Norm von ϑ ist die p-te Potenz einer rationalen Zahl.

II. Wir wollen nun zeigen, dass ϑ selbst p-te Potenz eines Ideals ist. Dazu bemerken wir zunächst, dass der Exponent $e\geqq 0$, der in ϑ enthaltenen Primidealzahl $\lambda=1-\varepsilon$, durch p teilbar ist. Und zwar folgt aus $\vartheta=\lambda^e\vartheta'$, $(\lambda^{e+1}, \vartheta)=\lambda^e$, dass

$$N(\vartheta)=N(\lambda)^e N(\vartheta'),\quad a_2^p=p^e N(\vartheta'),\quad (N(\vartheta'), p)=1.$$

Mithin muss e durch p teilbar sein.

Es bezeichne jetzt $\mathfrak{p}\neq\lambda$ einen beliebigen Primidealteiler von ϑ in K_p, für den

$$(\mathfrak{p}^{i+1}, \vartheta)=\mathfrak{p}^i,\quad (i,p)=1.$$

Ferner sei: β eine ganze Zahl von K_p, die durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist; β_1 eine durch $\frac{\beta}{\mathfrak{p}}$, aber nicht durch $\mathfrak{p}$ teilbare ganze Zahl aus K_p; x, y seien natürliche Zahlen, die die Gleichung $ix-py=1$ erfüllen und schliesslich sei

$$V=\vartheta^x\beta^{-py},\quad \beta_1^{py}V=\vartheta^x\beta^{-py}\beta_1^{py}.$$

Nehmen wir an, dass $\sqrt[p]{\vartheta}$ keine Zahl aus K_p ist, so erhält man nach (1) und Hilfssatz 4 das Kompositum $\mathfrak{R}$ der Körper K_p und Q

durch Adjunktion von $\sqrt[p]{\vartheta}$ zu K_p. Demnach ergibt sich $\mathfrak{N}$ auch durch Adjunktion von $\sqrt[p]{\beta_1^{pu} V}$ zu K_p. Die Zahl $\beta_1^{pu} V$ ist durch $\mathfrak{p}$ aber nicht durch $\mathfrak{p}^2$ teilbar. Mithin ist in $\mathfrak{N}$ für das Ideal $\mathfrak{P} = (\mathfrak{p}, \sqrt[p]{\beta_1^{pu} V})$

$$\mathfrak{P}^p = (\mathfrak{p}^p, \mathfrak{p}^{p-1}\xi, \ldots, \mathfrak{p}^h \xi^{p-h}, \ldots, \xi^p), \quad \xi = \sqrt[p]{\beta_1^{pu} V}.$$

Also ist $\mathfrak{P}^p \mid \mathfrak{p}$. Wegen des Dedekindschen Diskriminantensatzes (Hilfssatz 1) muss also $\mathfrak{P}$ in der Diskriminante $\mathfrak{D}$ von $\mathfrak{N}$ aufgehen. Bezeichnet k_t den Trägheitskörper von $\mathfrak{P}$, so erhält k_t, nach Satz 3, den Körper Q, wie auch K_p, da $(\mathfrak{p}, \lambda) = 1$. Demnach ist $k_t = \mathfrak{N}$ Galoissch, und mithin folgt aus Satz 3, dass gleichzeitig $(\mathfrak{D}, \mathfrak{p}) = 1$ ist. Die Annahme $(i, p) = 1$ führt also zu einem Widerspruch.

III. Nach II können wir $\vartheta_s = \varepsilon_s' \varphi_s^p$ setzen, wo φ_s eine ganze Idealzahl und ε_s' eine Idealeinheit aus K_p bezeichnet. Nach Satz I gehören also φ_s zur Hauptklasse. Mithin können wir $\vartheta_s = e_s \xi_s^p$ setzen, wo ξ_s und e_s ganze Zahlen und e_s eine Einheit in K_p bedeutet. Demnach erhält man aus (1)

$$e_s^{-1} e_1^s (\xi_s^{-1} \xi_1^s)^p = \alpha_s^p.$$

Folgich ist $e_s e^{-s} = E_s^p$, wo E_s ebenfalls ganze Zahlen bezeichnen, die Einheiten in K_p sind. Aus diesen Gleichungen folgt jetzt leicht, dass auch e_s bis auf eine p-te Einheitswurzel, selbst Potenz einer Einheit ist, was wir folgendermassen zeigen: Wir wenden den Satz 2 an und erhalten für eine gewisse Einheit $\eta(\varepsilon)$ aus K_p, für die $\eta(\varepsilon) = \eta(\varepsilon^{-1})$ ist,

$$e_1 = \varepsilon^r \eta(\varepsilon), \quad e_s = \varepsilon^{rs} \eta(\varepsilon^s). \tag{2}$$

Also ist $e_1 e_{-1} = \eta(\varepsilon)^2$. Andererseits ist $e_1 e_{-1} = E_{-1}^p$, d. h. $\eta(\varepsilon)^2 = E_{-1}^p$. Ist für ein gewisses z $1 = 2z + p$, so folgt

$$\eta(\varepsilon) = \eta(\varepsilon)^{2z} \eta(\varepsilon)^p = (E_{-1}^z \eta(\varepsilon))^p.$$

Setzen wir $E_{-1}^z \eta(\varepsilon) = e(\varepsilon)$, so ergibt sich $\eta(\varepsilon) = (e(\varepsilon))^p$. Die Zahlen $[\varepsilon^s, x_k]$ sind also wegen (1) und (2) Elemente des p^2-ten Kreisteilungskörpers K_{p^2}. Demnach schliessen wir aus

$$p x_1 = \sum_{s=1}^{p} [\varepsilon^s, x_1], \quad p x_g = \sum_{s=1}^{p} \varepsilon^{-(g-1)s} [\varepsilon^s, x_1],$$

dass auch $x_1, x_2, \ldots, x_p$ zu K_{p^2} gehören, womit der Satz bewiesen ist.

Hilfssatz 6. *Die Diskriminante eines Unterkörpers des Körpers K_{p^n} der p^n-ten Einheitswurzel ε ist von ± 1 verschieden.*

Beweis. Das p^n-te Kreisteilungspolynom ist gleich dem Polynome

$$\frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \ldots + x^{p^{n-1}} + 1.$$

Mithin ist

$$p = \prod (1 - \varepsilon^m) = \prod \left(\frac{1 - \varepsilon^m}{1 - \varepsilon}\right) (1 - \varepsilon)^{p^{n-1}(p-1)},$$

wo ε^m sämtliche primitive p^n-te Einheitswurzeln durchläuft und

$$\frac{1 - \varepsilon^m}{1 - \varepsilon}, \quad \frac{1 - \varepsilon}{1 - \varepsilon^m} = \frac{1 - \varepsilon^{mm'}}{1 - \varepsilon^m}, \quad mm' \equiv 1 \pmod{p^2},$$

Einheiten des Körpers K_{p^n} der p^n-te Einheitswurzel ε sind. Also ist $p = [1 - \varepsilon]^{p^{n-1}(p-1)}$ und mithin beträgt nach Hilfssatz 2 die Ordnung der Trägheitsgruppe g_t von $[1 - \varepsilon]$ $p^{n-1}(p-1)$, d. h. sie ist mit der Automorphismengruppe von K_{p^n} identisch. Demnach ist der Trägheitskörper k_t von $[1 - \varepsilon]$ mit dem rationalen Körper identisch. Bezeichnet jetzt Q einen Unterkörper von K_{p^n} dessen Diskriminante ± 1 ist, so muss Q nach Satz 3 Unterkörper von k_t sein, d. h. Q ist mit dem rationalen Körper identisch, w. z. b. w.

Nun können wir jetzt einen verh. kurzen arithmetischen Beweis des auf algebraisch auflösbare Polynome beschränkten Minkowskischen Diskriminantensatzes geben.

Satz 5. *Die Diskriminante eines absolut algebraisch auflösbaren Körpers ist von ± 1 verschieden.*

Beweis. I. Es sei $K(\alpha)$ ein absolut-algebraisch auflösbarer Körper, $K(\alpha_i)$ ein zu $K(\alpha)$ konjugierter Körper, und $\mathfrak{N}$ der kleinste Galoissche Körper, der $K(\alpha)$ enthält. Ist die Diskriminante von $K(\alpha)$ gleich ± 1, so ist es auch die Diskriminante von $K(\alpha_i)$. Bezeichnet jetzt $\mathfrak{P}$ einen Primidealteiler der Diskriminante $\mathfrak{D}$ von $\mathfrak{N}$, so enthält nach Satz 3 der Trägheitskörper k_t von $\mathfrak{P}$ sämtliche $K(\alpha_i)$ als Unterkörper. Also ist k_t mit $\mathfrak{N}$ identisch. Die Differente von $\mathfrak{N}$ ist also nach Satz 3 durch $\mathfrak{P}$ nicht teilbar. Da $\mathfrak{N}$ Galoissch ist, so ist wieder nach Satz 3 auch $\mathfrak{D}$ durch p nicht teilbar, d. h. $\mathfrak{D} = \pm 1$. Demnach ist nach Hilfssatz 1 zugleich die Diskriminante eins beliebigen Unterkörpers von $\mathfrak{N}$ gleich ± 1.

II. Es bezeichnen $\mathfrak{G}$ die Automorphismengruppe von $\mathfrak{R}$ und $\mathfrak{N}$ einen grössten Normalteiler von $\mathfrak{G}$. Da $\mathfrak{G}$ auflösbar ist, so ist der Index p von $\mathfrak{N}$ in Bezug auf $\mathfrak{G}$ prim. Ist Q der Unterkörper von $\mathfrak{N}$, der der Gruppe $\mathfrak{N}$ entspricht, β ein primitives Element aus Q und $\varphi(x)$ das irreduzible ganzzahlige Polynom, dessen Wurzel β ist, so ist $\varphi(x)$ ein normales Polynom (eine Galoissche Resolvente) vom Grade p. Dies ist nur dann möglich, wenn die Automorphismengruppe $\mathfrak{G}_1$ von Q zyklisch und von der Ordnung p ist. Dabei ist nach I. und Hilfsatz 1 die Diskriminante d von Q gleich ± 1. Nach Satz 2 ist also Q Unterkörper der Körpers K_{p^2} der p^2-ten Einheitswurzeln. Nach Hilfssatz 6 ist dies aber unmöglich.

Als unmittelbare Folgerung der obigen Betrachtungen erhalten wir einen arithmetischen Beweis des auf algebraisch auflösbare Polynome beschränkten Tschebotaröwschen Monodromiesatzes [6]:

Satz 6. *Durch Komposition aller Trägheitsgruppen eines normalen absolut algebraisch auflösbaren Körpers $\mathfrak{R}$ entsteht die volle Galoissche Gruppe des Körpers.*

Beweis. Es sei K der Durchschnitt aller Trägheitskörper k_t von $\mathfrak{R}$ und $\mathfrak{d}$ die Differente von K. Da die Differente eines Unterkörpers Teiler der Differente des Oberkörpers ist, muss $\mathfrak{d}$ als Teiler der Differenten sämtlicher Trägheitskörper eine Einheit sein. Also ist die Diskriminante d von K, da $d = N(\mathfrak{d})$, gleich ± 1. Nach dem Minkowskischen Diskriminantensatz (vgl. Satz 5) ist also K mit dem rationalen Körper identisch, d. h. K gehört zur Automorphismengruppe von $\mathfrak{R}$. Andererseits gehört K innerhalb $\mathfrak{R}$, als Durchschnitt aller k_t, zum Kompositum aller Trägheitsgruppen; womit der Satz bewiesen ist.

Anmerkung. Wenden wir den Minkowskischen Diskriminantensatz in seinem vollen Umfang an, so erhalten wir einen Beweis des allgemeinen Tschebotaröwschen Monodromiesatzes.

§ 2. Arithmetischer Beweis des Kronecker-Weberschen Einbettungssatzes Abelscher Körper.

Zunächst verallgemeinern wir den Satz 4 auf beliebige zyklische Körper, deren Grade Primzahlpotenzen sind. Dazu bedürfen wir folgender Hilfssätze:

[6] N. Tschebotaröw. Beweis des Kronecker-Weberschen Satzes über Abelsche Körper. Recueil Math. Moscou, B. 31, 1922 (24), S. 302—309.

Hilfsatz 7. 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 beträg n, K_3 ist das Kompositum von K_1 und K_2 und n_3 sein Grad.*

Behauptung: *Ist K_2 Galoissch, so ist $n_3 = \frac{n_1 n_2}{n}$* [7].

Hilfssatz 8. Voraussetzung: *K_1 und K_2 seien über einem vollkommenen Körper K Galoissch. $\mathfrak{K}$ ist Kompositum von K_1 und K_2. $\mathfrak{G}$ sei die Automorphismengruppe von $\mathfrak{R}$ in Bezug auf K.*

Behauptung: *$\mathfrak{G}$ ist dem direkten Produkte der Automorphismengruppen von K_1 und K_2 isomorph.*

Beweis. Mit $\mathfrak{G}_1$ bzw. $\mathfrak{G}_2$ bezeichnen wir die Automorphismengruppe von K_1 bzw. von K_2. Mit $\mathfrak{U}_1$ bzw. $\mathfrak{U}_2$ bezeichnen wir die Gruppe zu der K_1 bzw. K_2 innerhalb ihres Kompositum $\mathfrak{K}$ gehört. Adjungieren wir K_2 bzw. K_1 zum Rationalitätsbereich K, so erhält man, dass die Gruppe $\mathfrak{G}$ von $\mathfrak{K}$ sich auf $\mathfrak{U}_2$ bzw. auf $\mathfrak{U}_1$ reduziert. Also muss $\mathfrak{U}_2$ bzw. $\mathfrak{U}_1$ einer Untergruppe von $\mathfrak{G}_1$ bzw. von $\mathfrak{G}_2$ isomorph sein. Bezeichnen wir jetzt mit n_1, n_2 bzw. n den Grad von K_1, K_2, bzw. von $\mathfrak{K}$ in Bezug auf K, so ergibt sich aus dem Hilfssatze 7

$$n = n_1 n_2 . \tag{1}$$

Das Kompositum $\mathfrak{K}$ von K_1 und K_2 gehört offenbar zum Durchschnitt von $\mathfrak{U}_1$ und $\mathfrak{U}_2$. Da $\mathfrak{K}$ zum Einheitselement $= E$ gehört, so haben $\mathfrak{U}_1$ und $\mathfrak{U}_2$ nur E als gemeinsames Element. Mithin folgt aus (1), dass $\mathfrak{G} = \mathfrak{U}_1 \mathfrak{U}_2$ ist. Demnach müssen sowohl $\mathfrak{U}_2$ mit $\mathfrak{G}_1$ als auch $\mathfrak{U}_1$ mit $\mathfrak{G}_2$ isomorph sein, d. h. $\mathfrak{G}$ ist dem direkten Produkte $\mathfrak{G}_1 \mathfrak{G}_2$ isomorph.

Hilfssatz 9. *Sind die Körper K_1 und K_2 über einem vollkommenen Körper K zyklisch, so enthält das Kompositium $\mathfrak{K}$ von K_1 und K_2 nur solche über K zyklische Unterkörper, deren Grade höchstens gleich den Graden von K_1 bzw. K_2 sind.*

Beweis. I. Bezeichnet K' den Durchschnitt von K_1 und K_2, so sind K_1 und K_2 in Bezug auf K' immer noch zyklisch. Nach Hilfssatz 8 ist die Automorphismengruppe von $\mathfrak{K}$ in Bezug auf K' dem direkten Produkte dieser zyklischen Gruppen isomorph.

[7] Für den Beweis diese Satzes vgl. S. Lubelski: Zur Reduzibilität von Polynomen in der Kongruenztheorie. II. Acta Arithmetica B. 2, 1937, S. 256.

II. Nach Hilfssatz 4 ist $\frac{n}{n'}, \frac{n_1}{n'}, \frac{n_2}{n'}$ der Grad von $\mathfrak{K}$, K_1, K_2 in Bezug auf K', wenn nur n, n_1, n_2, n' den Grad von $\mathfrak{K}$, K_1, K_2, K' in Bezug auf K bezeichnen. Enthält also $\mathfrak{K}$ in Bezug auf K einen zyklischen Unterkörper vom Grade N, wobei $N > n_1$ und $N > n_2$ ist, so enthält $\mathfrak{K}$ in Bezug auf K', wieder nach Hilfssatz 4, einen zyklischen Unterkörper vom Grade $\frac{N}{n'}$, wobei $\frac{N}{n'} > \frac{n_1}{n'}$, $\frac{N}{n'} > \frac{n_2}{n'}$. Dies ist aber unmöglich, weil es zu einem Widerspruch zu I. führt.

Hilfssatz 10. *Das Kompositum $\mathfrak{K}$ der in Bezug auf K Abelschen Körper $\mathfrak{K}_1$, $\mathfrak{K}_2$ ist ebenfalls in Bezug auf K Abelsch.*

Beweis. Ist nämlich α_1 bzw α_2 ein erzeugendes Element von $\mathfrak{K}_1$ bzw. von $\mathfrak{K}_2$, so kann man jedes Element von $\mathfrak{K}$ durch die Form $\xi(\alpha_1, \alpha_2)$ darstellen, wo $\xi(x, y)$ ein ganzes Polynom von x, y mit Koeffizienten aus dem zugrunde gelegten Körper K ist. Ist $S^{(i)}$ ein Element der Automorphismengruppe von $\mathfrak{K}$ dem das Element $S_1^{(i)}$ bzw $S_2^{(i)}$ der Automorphismengruppen von $\mathfrak{K}_1$ bzw. $\mathfrak{K}_2$ entspricht, so ist

$$S^{(i)}\,\xi(\alpha_1, \alpha_2) = \xi(S_1^{(i)}\,\alpha_1,\ S_2^{(i)}\,\alpha_2), \quad i = 1, 2;$$

$$S^{(1)}\,S^{(2)}\,\xi(\alpha_1, \alpha_2) = \xi(S_1^{(1)}\,S_1^{(2)}\alpha_1,\ S_2^{(1)}\,S_2^{(2)}\,\alpha_2) = \xi(S_1^{(2)}\,S_1^{(1)}\,\alpha_1,\ S_2^{(2)}\,S_2^{(1)}\alpha_2) = S^{(2)}\,S^{(1)}\,\xi(\alpha_1, \alpha_2).$$

Es ist also die Authomorphismengruppe von $\mathfrak{K}$ in Bezug auf K ebenfalls Abelsch.

Hilfssatz 11. *Ist $\mathfrak{G}$ eine Abelsche Gruppe von der Ordnung l^m, wo l prim ist so ist* 1) *$\mathfrak{G}$ direktes Produkt von $\mathfrak{A}$ und $\mathfrak{S}$, so $\mathfrak{A}$ eine zyklische Gruppe von möglichst grosser Ordnung ist.* 2) *$\mathfrak{G}$ zyklisch, wenn nur $\mathfrak{G}$ einen Normalteiler von der Ordnung l^{m-1} enthält.*

Beweis. 1) Bilden $A_1, A_2, \ldots, A_m$ eine Basis von $\mathfrak{G}$ und ist $\mathfrak{A}$ von der Ordnung l^a, so muss eines der Elemente $A_1, A_2, \ldots, A_m$ ebenfalls von der Ordnung a sein. Der Beweis von 2) ergibt sich unmittelbar aus dem von 1).

Satz 7. Voraussetzung: *K ist ein absolut zyklischer Körper vom Grade p^m, wo p prim und m eine natürliche Zahl ist. Die Diskriminante von K ist abgesehen vom Vorzeichen ebenfalls Potenz der Zahl p. Ferner bezeichnet K_s den Körper der s-ten Einheitswurzeln.*

Behauptung: *K ist Unterkörper von $K_{p^{m+1}}$ oder $K_{2^{m+2}}$, je nachdem $p > 2$ oder $p = 2$ ist.*

Beweis. I. Es sei $p > 2$ und Q sei das Kompositum von K mit dem zyklischen Unterkörper P vom Grade p^m des Körpers $K_{p^{m+1}}$. Wäre die Automorphismengruppe $\mathfrak{G}$ von Q nicht zyklisch, so würde $\mathfrak{G}$ nach

Hilfssatz 10 und 11 mindestens zwei verschiedene Normalteiler vom Index p enthalten. Demnach enthält Q zwei verschiedene Unterkörper von Grade p. Offenbar sind diese Unterkörper zyklisch. Da ihre Diskriminanten nach Hilfssatz 1 und der angegebenen Folgerung vom Satze 3, nur durch eine rationale Primzahl teilbar sind (und zwar durch p), so sind diese Unterkörper nach Satz 4 identisch. Demnach sind auch die Körper P_m und K identisch.

II. Es sei also $p = 2$. Die Körper $k(\sqrt{-1})$, $k(\sqrt{\pm 2})$ sind die einzigen quadratischen Körper, deren Diskriminanten, vom Vorzeichen abgesehen, Potenzen der Zahl 2 sind. Wir können also $m > 1$ annehmen.

Zunächst betrachten wir einen beliebigen Galoisschen Körper k' vom Grade 4, dessen Diskriminante gleich $\pm 2^t$ ist und der den Körper $k(\sqrt{-1})$ enthält. k' ist also in Bezug auf $k(\sqrt{-1})$ relativ quadratisch, d. h. k' ergibt sich durch Adjunktion einer Zahl $\sqrt{\delta}$, wo δ eine zu $k(\sqrt{-1})$ gehörige und dort quadratfreie Zahl ist. Ist λ ein Primteiler von δ in $k(\sqrt{-1})$, so schliesst man aus $(\lambda, \sqrt{\delta})^2 = \lambda$ nach Hilfssatz 1, dass λ Teiler der Zaht 2^t sein müss, was nur für $\delta = \pm(1+i)$, $\pm i$ möglich ist, d. h. k' ist durch die Wurzeln von $x^4 \pm 2x^2 + 2$ bzw. $x^4 + 1$ gebildet. Da

$$x^4 - 2x^2 + 2 \equiv (x^2 - 4)(x^2 + 2) \pmod 5, \quad x^4 + 2x^2 + 2 \equiv (x^2 - 1)(x^2 + 3) \pmod 5,$$

so ist $x^4 \pm 2x^2 + 2$ kein normales Polynom. Der Galoissche Körper k' ist also durch eine Wurzel von $x^4 + 1 = 0$ gebildet und mithin ist k' eindeutig bestimmt.

III. Es sei wieder $p = 2$ und K ein beliebiger zyklischer Körper vom Grade 2^m, $m > 2$. Die Diskriminante des Kompositums Q bzw. Q_1 von K und des Körpers $K_{2^{m+2}}$ bzw. $K_{2^{m+1}}$ der 2^{m+2}-ten, bzw. 2^{m+1}-ten Einheitswurzeln, ist ebenfalls nach Folgerung vom Satz 3, vom Vorzeichen abgesehen, Potenz der Zahl 2. Offenbar ist Q in Bezug auf $k(\sqrt{-1})$ Galoisch. Wäre Q in Bezug auf $k(\sqrt{-1})$ nicht zyklisch, so würde Q nach Hilfssatz 11 zwei verschiedene in Bezug auf $k(\sqrt{-1})$ relativ quadratische Körper enthalten, was nach II. unmöglich ist. Enthält K den Körper $k(\sqrt{-1})$ nicht, so ist das Kompositum K' von K und $k(\sqrt{-1})$ von Grade 2^{m+1}, d. h. K' muss mit $K_{2^{m+2}}$ identisch sein, da Q zyklisch ist. Ähnlich muss, wenn nur $k(\sqrt{-1})$ zu K gehört, Q_1 mit K, also mit $K_{2^{m+1}}$ identisch sein, womit der Satz bewiesen ist.

Satz 8. Voraussetzng: *$\mathfrak{P}$ sei ein Primideal des Galoisschen Körpers $\mathfrak{K}$, ferner seien g_z, g_t, bzw. g_v ihre Zerlegungs, - Trägheits, - bzw.*

Verzweigungsgruppe, und p sei die rationale Primzahl, die durch $\mathfrak{P}$ teilbar ist.

Behauptung: 1) *g_0 bzw. g_t ist Normalteiler von g_t bzw. von g_z. Dabei gehört g_0 zur p-Sylowgruppe der Automorphismengruppe von $\mathfrak{K}$ und die Faktorgruppen g_z/g_t, g_t/g_0 sind zyklisch, wobei g_z/g_t von der Ordnung f ist, wo f den Grad von $\mathfrak{P}$ bezeichnet.*

2) *Ist Z eine beliebige Substitution von g_z, die zum erzeugenden Element von g_z/g_t gehört, so ist $Z\tau Z^{-1} = \tau^p\sigma$, wo τ eine beliebige Substitution aus g_t und σ eine entsprechende Substitution aus g_0 bezeichnet.*[8])

Beweis. Der Beweis von 1) ist z. B. in 5) S. 132 und 135 durchgeführt. Wir beschäftigen uns also mit dem Beweise von 2).

Mit α und ξ bezeichnen wir ganze Zahlen aus dem Galoisschen Körper $\mathfrak{K}$, wo ξ durch das Primideal $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbar ist. Man kann also α durch die Form

$$\alpha \equiv \alpha_0 + \alpha_1\xi + \alpha_2\xi^2 + \ldots + \alpha_{i-1}\xi^{i-1} \pmod{\mathfrak{P}^i}$$

darstellen, wo $\alpha_0, \alpha_1, \ldots, \alpha_{i-1}$ mod $\mathfrak{P}$ zu einem festen Restsystem R mod $\mathfrak{P}$ gehören. Gehört δ zu g_z, so ist $\delta\xi \equiv 0$ mod $\mathfrak{P}$ und es wird also $\delta\xi \equiv d\xi$ mod $\mathfrak{P}^2$ seien. Wäre $\mathfrak{P}|d$, so würde $\mathfrak{P}^2|\xi$ sein. Es sei jetzt

$$g_z = g_t + Sg_t + \ldots + S^{h-1}g_t.$$

Z gehört also nach Voraussetzung zu Sg_t. Offenbar kann man.

$$Z^{-1}\xi \equiv a\xi \pmod{\mathfrak{P}^2}, \quad \tau\xi \equiv b\xi \pmod{\mathfrak{P}^2}$$

annehmen, wo $(a, \mathfrak{P}) = (b, \mathfrak{P}) = 1$, und a und b zu R gehören.

Man kann also $\tau\xi \equiv \rho^m\xi$ mod $\mathfrak{P}^2$ setzen, wo ρ eine primitive Wurzel mod $\mathfrak{P}$ bedeutet. Mithin ist

$$\tau Z^{-1}\xi \equiv (\tau a)(\tau\xi) \equiv a\tau\xi \equiv a\rho^m\xi \equiv \rho^m(Z^{-1}\xi) \pmod{\mathfrak{P}^2},$$

$$Z\tau Z^{-1}\xi \equiv (Z\rho^m)\xi \pmod{\mathfrak{P}^2}. \tag{1}$$

[8]) Der Teil 2) der Behauptung dieses Satzes ist aus der Speiserschen Methode des Beweises des Kronecker-Weberschen Satzes entnommen; vgl. A. Speiser. Die Zerlegungsgruppe. Journ. für Math. Bd. 149 (1919), S. 174-188.

II. Um die Zahl $Z\rho^m$ zu berechnen, bemerken wir folgendes; übt man eine Substitution von g_z auf das Restsystem R aus, so geht dieses System mod $\mathfrak{P}$ in sich über. Dabei folgt aus

$$\alpha + \beta \equiv \gamma \pmod{\mathfrak{P}}, \quad \alpha\beta \equiv \gamma \pmod{\mathfrak{P}},$$

dass

$$\alpha' + \beta' \equiv \gamma' \pmod{\mathfrak{P}}, \quad \alpha'\beta' \equiv \gamma' \pmod{\mathfrak{P}}$$

ist, wenn nur x' eine bestimmte Konjugierte von x bedeutet. Die Substitutionen der Zerlegungsgruppe g_z sind in R Automorphismen. Nun ist R ohne „0" zyklisch und mithin kann man die Automorphismen durch die Form (ρ, ρ^{p^i}) darstellen, wo $i = 0, 1, 2, \ldots f-1$, und f den Grad von $\mathfrak{P}$ bezeichnet. Demnach ist $Z\rho = \rho^p$, wenn Z zu Sg_t gehört. Aus (1) ergibt sich also

$$Z\tau Z^{-1}\xi \equiv \rho^{mp}\xi \pmod{\mathfrak{P}^2}.$$

Da

$$\tau^p\xi \equiv \rho^m\tau^{p-1}\xi \equiv \rho^{mp}\xi \pmod{\mathfrak{P}^2}$$

ist, gehört $Z\tau Z^{-1}\tau^{-p}$ zu g_0.

Satz 9. *Alle absolut Abelschen Körper K sind Kreisteilungskörper* (vgl. [4]) S. 648—669, [5]) S. 53—68).

Beweis. Wie nur leicht zu ersehen ist, kann man den Grad des Abelschen Körpers als Potenz l^m einer Primzahl l annehmen (vgl. z. B. [4]) S. 648—650).

Ist $p \neq l$, wo p eine rationale Primzahl bezeichnet, so muss die Verzweigungsgruppe g_0 eines Primidealteilers $\mathfrak{p}$ von p in K nach Satz 8) 1) mit der Einheitssubstitution identisch sein. Mithin ist die Trägheitsgruppe g_t von $\mathfrak{p}$ zyklisch.

Nehmen wir jetzt Z und τ wie im Satze 8 an, so ergibt sich aus diesem Satze, da die Zerlegungsgruppe g_z von $\mathfrak{p}$ Abelsch ist, dass

$$\tau = Z\tau Z^{-1} = \tau^p, \quad \tau^{p-1} = E \quad (E = \text{Einheitssubstitution}),$$

d. h. $p-1$ ist durch die Ordnung l^n der Trägheitsgruppe g_t teilbar, n eine natürliche Zahl. Demnach enthält der Körper K_p der p-ten Einheitswurzeln einen zyklischen Unterkörper P_n vom Grade l^n. Die Diskriminante von P_n ist nach Hilfssatz 1, ebenso wie die Diskriminante von K_p, Po-

tenz der Zahl p. Nach Satz 3 ist also die Diskriminante des Trägheitskörpers $\overline{k}_t$ eines Primidealteilers $\overline{\mathfrak{p}}$ von $p+l$ in P_n gleich ± 1. Nach Satz 5 ist $\overline{k}_t$ mit dem rationalen Körper identisch. Die Ordnung der Trägheitsgruppe von $\overline{\mathfrak{p}}$ in P_n beträgt also l^n. Mithin ist nach Hilfsatz 2

$$p = \overline{\mathfrak{p}}^{l^n}.$$

II. Wir betrachten jetzt das Kompositum K' von K und P_n, ferner den Trägheitskörper k'_t bzw. die Trägheitsgruppe g'_t eines Primidealteires $\mathfrak{P}$ von p in K'.

Nach Hilfssatz 4 und 7 ist auch der Grad von K' Potenz der Zahl l. Die Verzweigungsgruppe von $\mathfrak{P}$ in K' enthält also nach Satz 8 1) nur das Einheitselement, d. h. g'_t ist zyklisch. Nehmen wir k_t als grundlegenden Körper an, wo k_t den Trägheitskörper des Ideals $\mathfrak{P}$ bezeichnet, so sind auch dann K und P_n zugleich zyklisch, wobei K bzw. P_n in Bezug auf k_t vom Grade l^n, bzw. höchstens vom Grade l^n ist. Das Kompositum K' enthält also nach Hilfssatz 9 und 4, rel. k_t, keinen zyklischen Körper vom Grade $>l^n$. Da nach Satz 3 k_t Unterkörper von k'_t ist, so enthält K' auch in Bezug auf k'_t keinen zyklischen Unterkörper vom Grade $>l^n$. Nun ist nach (1) die Ordnung der zyklischen Gruppe g'_t, wegen Hilfssatz 2, $\geqq l^n$. Demnach ist der Grad vom K' in Bezug auf k'_t gleich l^n.

III. Nach Hilfssatz 10 ist k'_t als Unterkörper Abelscher Körper, Abelsch, und mithin auch Galoissch. Es bezeichne k' den Durchschnitt von P_n und k'_t, und d' seine Diskriminante. Ist δ ein rationaler Primteiler von d', so muss nach Hilfssatz 1 δ gemeinsamer Teiler der Diskriminanten von k'_t und P_n sein. Da nach Hilfssatz 1 die Diskriminante von P_n also auch von k' höchstens *einen* rationalen Primteiler (nämlich nur p) haben kann, so muss $d' = \pm 1$ sein. Nach Hilfssatz 6 (oder nach Satz 5) ist k' mit dem rationalen Körper identisch.

Es bezeichne jetzt $f(x)$ das ganze ganzzahlige irreduzible Polynom, dessen Wurzeln den Körper P_n bestimmen. Ist $f_1(x)$ ein in k'_t irreduzibler Faktor von $f(x)$, so gehören offenbar die Koeffizienten von $f_1(x)$ zugleich zu P_n. Da k' nur rationale Zahlen enthält, so muss $f_1(x) = f(x)$ sein. Adjungieren wir eine Wurzel von $f(x)$ zu k'_t, so erhalten wir nach Hilfssatz 4 den Körper K', d. h. K' ist das Kompositum von k'_t und P_n.

Demnach können wir nach Hilfssatz 10 sämtliche Betrachtungen dieses Beweises auch auf k'_t anwenden. Man erhält also schliesslich einen Abelschen Körper, dessen Grad und Diskriminante Potenz der Zahl l sind. Nach Satz 4 ist also der Kronecker-Webersche Satz bewiesen.

Anmerkung. Der Kronecker-Webersche Satz muss als Gipfelpunkt desjenigen Teiles der allgemeinen Zahlentheorie angesehen werden, den man mittels rein arithmetischer Methoden erreichen kann. Der obige Beweis dieses Satzes ist nämlich sowohl von transzendenten Hilfsmitteln (vgl. H. Weber [4]) a) S. 648—669), als auch vom Begriffe der reellen Zahl (die z. B. im Beweise des allgemeinen Minkowskischen Diskriminantensatzes oft benutzt wird, vgl. D. Hilbert [5]) S. 53—68, A. Speiser [6]) und N. Tschebotaröw [6])), unnabhängig. Ferner ist zu bemerken, da man den Satz 9 auch mittels des Tschebotaröwschen Monodromiesatzes und des Hilfsatzes 11, dagegen ohne Zuhilfenahme des Satzes 8, rein arithmetisch beweisen kann.

Als Anwedung des arithmetischen Beweises des Kronecker-Weberschen Einbettungssatzes wollen wir zeigen, dass ein interessanter, auf algebraisch auflösbare Polynome beschränkter Radosscher Satz, ebenfalls rein aritchmetisch bewiesen werden kann.

Satz 10. *Ist $f(x)$ ein ganzzahliges algebraisch auflösbares Polynom, vom Grade n, das mindestens einen ganzzahligen irreduziblen Faktor vom Grade $n \geqslant 2$ hat, so gibt es unendlich viele Primzahlen p, für die $f(x)$ nicht in Linearfaktoren* mod p *zerlegbar ist.*[9])

Beweis. Offenbar kann man $f(x)$ irreduzibel, normiert und vom Grade $n \geqslant 2$ annehmen. Bezeichnet $\mathfrak{N}$ einen grössten Normalteiler der Galoisschen Gruppe $\mathfrak{G}$ von $f(x)$, so ist der Index von $\mathfrak{N}$ in Bezug auf $\mathfrak{G}$ gleich einer Primzahl π, da $\mathfrak{G}$ auflösbar ist. Ist α ein Element des kleinsten Galoisschen Körpers von $f(x)$, das zum Normalteiler $\mathfrak{N}$ gehört, so ist α Wurzel eines zyklischen Polynoms $\varphi(x)$ vom π-ten Grade. Nach dem Kronecker-Weberschen Satze 9 gehören die Wurzeln von $\varphi(x)$ zu einem Kreisteilungskörper. Wir können also auf $\varphi(x)$ den folgenden Satz anwenden:

„Voraussetzung: m ist eine gewisse natürliche Zahl, $\mathfrak{H}_1$ eine gewisse Untergruppe der mod m vollen multiplikativen Restgruppe $\mathfrak{H}$".

„Behauptung: Es existiert ein ganzes ganzzahliges Kreisteilungspolynom $f(x)$, das mit endlich vielen Ausnahmen nur Primiteiler hat, die mod m zu $\mathfrak{H}_1$ gehören. Dabei ist der Grad von $f(x)$ dem Index von $\mathfrak{H}_1$ in Bezug auf $\mathfrak{H}$ gleich. Umgekehrt ist $\varphi(x)$ ein Kreisteilungpolynom, so entspricht $\varphi(x)$ eine gewisse Gruppe $\mathfrak{H}_1$ mit den genannten Eigenschaften." (vol. [7]) S. 249—250).

[9]) Eine ausführliche Beleuchtung des Falles $n=2$ findet sich in der Arbeit des Verf.: Zur Reduzibilität von Polynomen in der Kongruenztheorie. Acta Arithmetica B. I. (1936), S. 169 — 174.

Nach dem Schurschen Prinzip (vgl. [7]) S. 252—253)) kann $\varphi(x)$ mit endlich vielen Ausnahmen nur für diejenige Primzahlen p linear zerlegbar sein, für die $f(x)$ es ist. Wenden wir jetzt den folgenden Satz an:

„Bilden die Klassen die aus den ganzen Zahlen b_k, $k = 1, 2, \ldots, n$, entstehen, eine Untergruppe ($\mathfrak{H}_1$ der vollen multiplikativen Restgruppe ($\mathfrak{H}$ 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". (vgl [7]) S. 249),

so erhalten wir demnach den Beweis unseres Satzes.

(Eingegangen am 14. Juni 1937.)