Kurzer Beweis des Diskriminantensatzes.

Von

N. Tschebotarëw (Kasan).

Der Zweck der vorliegenden Note ist, einen neuen Beweis des Diskriminantensatzes darzulegen, der bekanntlich bei dem Auseinandersetzen der arithmetischen Idealtheorie besondere Schwierigkeiten bietet. Dieser Beweis hat bei seiner relativen Knappheit die Eigentümlichkeit, dass er ziemlich wenige Vorkenntnisse aus der Idealtheorie fordert (es ist z. B. der Begriff der Idealnorm als der Kongruenzklassenzahl nicht notwendig). Dagegen sind die Elemente der Galoisschen Theorie und der erste Sylowsche Satz als bekannt vorausgesetzt.

Wir formulieren den zu beweisenden Diskriminantensatz folgendermassen:

Es sei k ein algebraischer Zahlkörper, $\mathfrak{R}$ sein Ring, welcher alle ganzen rationalen Zahlen enthalten soll, $[\omega_1, \omega_2, \ldots, \omega_n]$ eine Basis von $\mathfrak{R}$. Die Diskriminante

$$\Delta = \begin{vmatrix} S(\omega_1\,\omega_1), & S(\omega_1\,\omega_2), \ldots, & S(\omega_1\,\omega_n) \\ S(\omega_2\,\omega_1), & S(\omega_2\,\omega_2), \ldots, & S(\omega_2\,\omega_n) \\ \cdot & \cdot \quad \cdot \quad \cdot & \cdot \\ S(\omega_n\,\omega_1), & S(\omega_n\,\omega_2), \ldots, & S(\omega_n\,\omega_n) \end{vmatrix} = \begin{vmatrix} \omega_1 & \omega_2 & \ldots, & \omega_n \\ \omega_1' & \omega_2' & \ldots, & \omega_n' \\ \cdot & \cdot & \cdot & \cdot \\ \omega_1^{(n-1)} & \omega_2^{(n-1)} & \ldots, & \omega_n^{(n-1)} \end{vmatrix}^2$$

ist durch eine rationale Primzahl p dann und nur dann teilbar, wenn p in bezug auf $\mathfrak{R}$ kritisch ist, d. h. wenn es in $\mathfrak{R}$ eine Zahl gibt, die nicht innerhalb $\mathfrak{R}$ durch p teilbar ist, während ihre gewisse Potenz innerhalb $\mathfrak{R}$ durch p teilbar ist. Dabei bedeuten $\omega, \omega', \ldots, \omega^{n-1}$ die zu ω algebraisch konjugierten Grössen und $S(\omega) = \omega + \omega' + \ldots + \omega^{(n-1)}$ die Spur von ω.

Es sei p kritisch und $\alpha = x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n$ eine Zahl von $\mathfrak{R}$, deren Potenz α^e durch p in $\mathfrak{R}$ teilbar ist, während nicht alle $x_i \equiv 0 \pmod p$ sind. Es sind $(\alpha')^e, (\alpha'')^e, \ldots, (\alpha^{(n-1)})^e$ durch p teilbar—zwar nicht notwendig in $\mathfrak{R}$, aber doch in den mit $\mathfrak{R}$ konjugierten Ringen $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(n-1)}$, also insbesondere im Normalkörper K, der alle mit k konjugierten Körper umfasst.

Sind Ω_{ij} die Komplemente von $\omega_i^{(j)}$ in der Determinante

$$\delta = \begin{vmatrix} \omega_1 & \omega_2 & \ldots, & \omega_n \\ \omega_1' & \omega_2' & \ldots, & \omega_n' \\ \cdot & \cdot & \cdot & \cdot \\ \omega_1^{(n-1)} & \omega_2^{(n-1)} & \ldots, & \omega_n^{(n-1)} \end{vmatrix}, \tag{1}$$

so gilt

$$\sum_j \Omega_{ij}\,\alpha^{(j)} = \sum_j \Omega_{ij} \sum_\mu \omega_\mu^{(j)}\,x_\mu = \sum_\mu x_\mu \sum_j \Omega_{ij}\,\omega_\mu^{(j)} = x_i \cdot \delta \quad (i = 1, 2, \ldots, n).$$

Ist $p^h \geqq e$, so sind in K

$$\Big\{\sum_j \Omega_{ij}\,\alpha^{(j)}\Big\}^{p^h} \equiv \sum_j \Omega_{ij}^{p^h}\,(\alpha^{(j)})^{p^h} \pmod p$$

durch p teilbar und da nicht alle $x_i \equiv 0 \pmod p$ sind, so gilt $\delta^{p^h} \equiv 0 \pmod p$. Da aber $\Delta = \delta^2$ ganz rational ist, so muss $\Delta \equiv 0 \pmod p$ sein, w. z. b. w.

Nun nehmen wir an, es sei Δ durch p teilbar. Die Zahl δ liegt in K. Aus $\delta^2 \equiv 0 \pmod p$ schliessen wir, dass δ durch das Produkt $\mathfrak{L} = \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_m$ aller voneinander verschiedenen Primidealteiler $\mathfrak{P}_i$ von p innerhalb K teilbar ist. Das Ideal $\mathfrak{L}$ ist gegenüber allen Substitutionen der Galoisschen Gruppe $\mathfrak{G}$ von K invariant. Die Primideale $\mathfrak{P}_i$ sind zueinander konjugiert, d. h. sie gehen ineinander mittels der Substitutionen von $\mathfrak{G}$ über.

Nun beweisen wir folgende drei Hilfssätze:

I. *Ist δ durch $\mathfrak{L}$ teilbar, so kann man das Kongruenzensystem*

$$\omega_1^{(i)}\xi_1 + \omega_2^{(i)}\xi_2 + \ldots + \omega_n^{(i)}\xi_n \equiv 0 \pmod{\mathfrak{L}} \quad (i = 0, 1, \ldots, n-1) \tag{2}$$

durch ganze Zahlen von K befriedigen, die nicht alle durch $\mathfrak{L}$ teilbar sind [1]).

Es sei

$$\begin{vmatrix} \omega_\alpha^{(i)}, \ldots, \omega_\beta^{(i)} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \omega_\alpha^{(j)}, \ldots, \omega_\beta^{(j)} \end{vmatrix}$$

ein durch $\mathfrak{L}$ nicht teilbarer Minor von (1), während alle Minoren von (1) höherer Ordnung durch $\mathfrak{L}$ teilbar sind. Führen wir die Bezeichnung

$$\begin{vmatrix} u_\alpha, \ldots, u_\beta, u_\gamma \\ \omega_\alpha^{(i)}, \ldots, \omega_\beta^{(i)}, \omega_\gamma^{(i)} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \omega_\alpha^{(j)}, \ldots, \omega_\beta^{(j)}, \omega_\gamma^{(j)} \end{vmatrix} = A_\alpha u_\alpha + \ldots + A_\beta u_\beta + A_\gamma u_\gamma$$

ein, so ist $\xi_\alpha = A_\alpha, \ldots, \xi_\beta = A_\beta, \xi_\gamma = A_\gamma$ (die übrigen $\xi = 0$) die gesuchte Lösung, für welche gilt: $\xi_\gamma \not\equiv 0 \pmod{\mathfrak{L}}$.

Wir wollen zeigen, dass man das System (2) durch ganze rationale, nicht alle durch p teilbare Zahlen befriedigen kann. Dazu beweisen wir:

II. *Ist $[\xi_1, \xi_2, \ldots, \xi_n]$ eine Lösung des Systems* (2), *so ist auch $[\xi_1 T, \xi_2 T, \ldots, \xi_n T]$ eine Lösung dieses Systems, wobei T eine beliebige Substitution von $\mathfrak{G}$* ist.

Wir fassen (2) als Relation zwischen den Körpergrössen von K auf und üben auf sie die Substitution T aus ($\mathfrak{L}$ ist gegenüber T invariant). Dadurch gehen die Formen $\omega_1^{(i)} u_1 + \omega_2^{(i)} u_2 + \ldots + \omega_n^{(i)} u_n$ ineinander über, so dass das System (2) dasselbe bleibt.

III. *Besitzt das System*

$$\omega_\alpha^{(i)} \xi_\alpha + \ldots + \omega_\beta^{(i)} \xi_\beta \equiv 0 \pmod{\mathfrak{L}} \qquad (i = 0, 1, \ldots, n-1) \tag{3}$$

eine Lösung $[\xi_\alpha, \ldots, \xi_\beta]$, in welcher ξ_α nicht durch $\mathfrak{L}$ teilbar ist, so besitzt es auch eine Lösung $[\eta_\alpha, \ldots, \eta_\beta]$, in welcher η_α zu p relativ prim ist.

[1] Vgl. hierzu E. Landau, Vorlesungen über Zahlentheorie, Bd. 3, Leipzig 1927, S. 129, Satz 822.

Es seien $\Pi_1, \Pi_2, \ldots, \Pi_m$ ganze Zahlen von K, die bzw. durch $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m$ und sonst durch keine Primidealfaktoren von p teilbar sind. Ist ξ_α etwa durch $\mathfrak{P}_{h+1}, \ldots, \mathfrak{P}_m$, aber nicht durch $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_h$ teilbar, und setzen wir $\tau_\nu = \Pi_2 \Pi_3 \ldots \Pi_h \xi_\nu$ ($= \xi_\nu$ für $h = 1$), so ist in der Lösung $[\tau_\alpha, \ldots, \tau_\beta]$ des Systems (3) τ_α durch $\mathfrak{P}_2, \mathfrak{P}_3, \ldots, \mathfrak{P}_m$, aber nicht durch $\mathfrak{P}_1$ teilbar. Sind $S_2, S_3, \ldots, S_m$ Substitutionen von $\mathfrak{G}$, die $\mathfrak{P}_1$ bzw. in $\mathfrak{P}_2, \mathfrak{P}_3, \ldots, \mathfrak{P}_m$ überführen, so ist $\tau_\alpha + \tau_\alpha S_2 + \ldots + \tau_\alpha S_m$ zu $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m$, also zu p relativ prim. Andererseits sind wegen II $[\tau_\alpha S_i, \ldots, \tau_\beta S_i]$ $(i = 2, 3, \ldots, m)$ und somit $[\tau_\alpha + \tau_\alpha S_2 + \ldots + \tau_\alpha S_m, \ldots, \tau_\beta + \tau_\beta S_2 + \ldots + \tau_\beta S_m]$ Lösungen des Systems (3). Die letztere Lösung genügt unserer Bedingung.

Es sei

$$\omega_1^{(i)} \xi_1 + \omega_2^{(i)} \xi_2 + \ldots + \omega_r^{(i)} \xi_r \equiv 0 \pmod{\mathfrak{L}} \quad (i = 0, 1, \ldots, n-1) \tag{4}$$

ein System, welches eine Lösung mit $\xi_1 \not\equiv 0 \pmod{\mathfrak{L}}$ besitzt, wobei r den kleinstmöglichen Wert habe. Wegen III können wir annehmen, ξ_1 sei in der Lösung $[\xi_1, \xi_2, \ldots, \xi_r]$ von (4) zu p relativ prim. Für $r > 1$ besitzt das System

$$\omega_2^{(i)} \xi_2 + \ldots + \omega_r^{(i)} \xi_r \equiv 0 \pmod{\mathfrak{L}} \qquad (i = 0, 1, \ldots, n-1) \tag{5}$$

keine Lösung, in welcher eine oder mehrere der Zahlen $\xi_\nu \not\equiv 0 \pmod{\mathfrak{L}}$ sind. Denn sonst könnte man (5) durch Umnumerieren in die Gestalt (4) mit kleinerem r setzen. Multiplizieren wir dann die ξ_ν mit $\frac{N(\xi_1)}{\xi_1}$, so erhalten wir eine Lösung $[\eta_{i1}, \eta_{i2}, \ldots, \eta_{ir}]$, in welcher $\eta_{i1} = N(\xi_1)$ ganz rational und zu p relativ prim ist. Diese Lösung ist eine einzige in dem Sinne, dass jede andere Lösung $[\eta_{i1}, \eta_{i2}^*, \ldots, \eta_{ir}^*]$ den Kongruenzen $\eta_{i\nu}^* \equiv \eta_{i\nu} \pmod{\mathfrak{L}}$ genügt. Denn sonst wäre $[\eta_{i2}^* - \eta_{i2}, \ldots, \eta_{ir}^* - \eta_{ir}]$ eine Lösung von (5), was unserer Voraussetzung zufolge unmöglich ist.

Es ist insbesondere $\eta_{i\nu} T \equiv \eta_{i\nu} \pmod{\mathfrak{L}}$ $(\nu = 1, 2, \ldots, r)$ (vgl. II), wobei T eine beliebige Substitution von $\mathfrak{G}$ ist. Nun sei $\mathfrak{H} = 1 + S_2 + \ldots + S_\pi$ die zu p gehörige Sylowgruppe von $\mathfrak{G}$, d. h. eine Untergruppe von $\mathfrak{G}$ von der Ordnung $\pi = p^s$ (es kann auch $s = 0$ sein), deren Index $a = (\mathfrak{G} : \mathfrak{H})$ zu p relativ prim ist (der erste Sylowsche Satz). Es gibt einen Exponenten f, für welchen

$$\eta_{i\nu}^{p^f} \equiv \eta_{i\nu} \pmod{\mathfrak{P}_i} \qquad (i = 1, 2, \ldots, m)$$

und somit

$$\eta_\nu^{p^f} \equiv \eta_\nu \pmod{\mathfrak{O}}$$

ist (verallgemeinerter Fermatscher Satz). Nehmen wir ein ganzes rationales q, so dass $l = qf - s$ positiv ist, so gilt:

$$(\eta_\nu \cdot \eta_\nu S_2 \ldots \eta_\nu S_\pi)^{p^l} \equiv \eta_\nu^{p^s \cdot p^{qf-s}} \equiv \eta_\nu^{p^{qf}} \equiv \eta_\nu \pmod{\mathfrak{O}}.$$

Die linke Seite dieser Kongruenz ist gegenüber $\mathfrak{H}$ invariant. Es ist also

$$\eta_\nu \equiv \tau_\nu \pmod{\mathfrak{O}},$$

wobei τ_ν gegenüber $\mathfrak{H}$ invariant ist.

Nun zerlegen wir $\mathfrak{G}$ nach $\mathfrak{H}$:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H} T_2 + \ldots + \mathfrak{H} T_a, \qquad (a, p) = 1.$$

Es ist

$$a \cdot \tau_\nu \equiv \tau_\nu + \tau_\nu T_2 + \ldots + \tau_\nu T_a \pmod{\mathfrak{O}},$$

wobei die rechte Seite dieser Kongruenz allen Substitutionen von $\mathfrak{O}$ gegenüber invariant, also ganz rational ist. Demnach können wir die Lösung $[a\eta_1, a\eta_2, \ldots, a\eta_r]$ des Systems (4) durch eine Lösung $[a\eta_1, x_2, \ldots, x_r]$ ersetzen, in welcher $a\eta_1, x_2, \ldots, x_r$ ganz rational sind und dabei $(a\eta_1, p) = 1$ gilt. [2])

Es sei $\mathfrak{O}^e$ durch p teilbar. Die Zahl

$$\alpha = a\eta_1 \omega_1 + x_2 \omega_2 + \ldots + x_r \omega_r$$

ist durch $\mathfrak{O}$, also α^e durch p teilbar. Andererseits ist α nicht in $\mathfrak{R}$ durch p teilbar, da sonst $\frac{\alpha}{p} = \frac{a\eta_1 \omega_1 + \ldots + x_r \omega_r}{p}$ in $\mathfrak{R}$ enthalten wäre, was der Annahme widerspricht, dass $[\omega_1, \omega_2, \ldots, \omega_n]$ eine Basis von $\mathfrak{R}$ ist. Denn die Koordinate $\frac{a\eta_1}{p}$ von $\frac{\alpha}{p}$ ist gebrochen. Damit ist gezeigt, dass p kritisch ist, w. z. b. w.

[2]) Diese Überlegung ist dem „*Zahlbericht*" von D. Hilbert entnommem. Vgl. *Gesammelte Abhandlungen*, Bd. I, Berlin 1932, S. 135, Satz 72.

(Eingegangen am 26. Oktober 1934.)

Über die Classenzahl quadratischer Zahlkörper.

Von

Carl Ludwig Siegel (Frankfurt a/M.).

Durch eine scharfsinnige Combination zweier Ansätze von Hecke und Deuring ist es Heilbronn gelungen, den lange vermuteten Satz zu beweisen, dass die Classenzahl $h(d)$ des imaginären quadratischen Zahlkörpers der Discriminante d mit $|d|$ unendlich wird. Es ist naheliegend, nach einer genaueren unteren Abschätzung von $h(d)$ zu fragen. Im folgenden soll die asymptotische Formel

$$\log h(d) \sim \log \sqrt{|d|} \tag{1}$$

bewiesen werden. Da nach Dirichlet

$$\pi |d|^{-\frac{1}{2}} h(d) = L_d(1) \qquad (d < -4)$$

gilt, wo

$$L_d(s) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-s}$$

gesetzt ist, so ist (1) mit der Aussage

$$\log L_d(1) = o(\log |d|) \tag{2}$$

gleichbedeutend. Man wird vermuten, dass (2) auch für positive Discriminanten d richtig ist; und dies wird ebenfalls bewiesen werden. Bedeutet ε_d die Grundeinheit, so ist nach Dirichlet

$$2 d^{-\frac{1}{2}} h(d) \log \varepsilon_d = L_d(1) \qquad (d > 0)$$

und folglich die Beziehung

$$\log (h(d) \log \varepsilon_d) \sim \log \sqrt{d}$$

das Analogon zu (1) für reelle quadratische Körper.