Über die Diskriminante auflösbarer Körper von Primzahlgrad.

Von *Helmut Hasse* in Göttingen.

Für die Diskriminante eines über dem rationalen Zahlkörper P kubischen Körpers K gilt bekanntlich [1]) die Formel

$$D = df^2,$$

wo d die Diskriminante des im galoisschen Körper N zu K enthaltenen quadratischen Teilkörpers Z ist (falls schon K = N galoissch ist, ist Z = P, $d = 1$ zu rechnen) und f der Führer des kubisch-zyklischen Relativkörpers N/Z. Dieser Tatbestand wurde von Wegner [2]) und Porusch [3]) auf beliebige auflösbare Körper K vom Primzahlgrad p über dem rationalen Zahlkörper verallgemeinert. Hier ist die Diskriminante (als Ideal, also abgesehen vom Vorzeichen) durch die Formel

$$\mathfrak{D}_{\mathsf{K/P}} = \mathfrak{D}_{\mathsf{Z/P}}^{\frac{p-1}{n}} \cdot \mathfrak{f}_{\mathsf{N/Z}}^{p-1}$$

gegeben, wo wieder N der galoissche Körper zu K ist, der dann zyklisch von einem Grade $n | p-1$ über K ist, und ferner zyklisch vom Grade p über einem über P vom Grade n zyklischen Teilkörper Z.

Diese für den Aufbau der Arithmetik in K wichtige Diskriminantenformel wurde von Wegner auf analytischem Wege, durch Vergleich von Zetafunktionalgleichungen, bewiesen. Porusch führt den Beweis in begrifflich nicht sehr befriedigender Weise folgendermaßen: Er stellt alle gruppentheoretisch möglichen Typen für die Hilbertsche Untergruppenreihe zu einer Primzahl q für N/P tabellarisch auf, gibt dabei jeweils die q-Beiträge zu den einzelnen Teilkörperdiskrimianten und Führern an, und liest so für die einzelnen q-Beiträge die Gültigkeit der fraglichen Formel ab.

Ich will hier zeigen, wie man diese Diskriminantenformel in einfacher Weise aus der von Artin [4]) entwickelten gruppentheoretischen Strukturtheorie der Diskriminante herleiten kann, die als formal-algebraisches Gerüst hinter der Wegnerschen analytischen Schlußweise steckt. Anschließend gebe ich noch einige Folgerungen, die im Zusammenhang mit der vorstehenden Arbeit von Wegner stehen.

1.

Sei Ω ein beliebiger algebraischer Zahlkörper, K ein über Ω auflösbarer Körper vom Primzahlgrad p, N der zugehörige galoissche Körper über Ω. Dann ist die Galois-

[1]) Siehe etwa H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, Math. Zeitschr. **31** (1930), 575, Satz 3 und 4.

[2]) U. Wegner, Zur Theorie der auflösbaren Gleichungen von Primzahlgrad. I, Journ. f. Math. **168** (1932), 183.

[3]) I. Porusch, Die Arithmetik in Zahlkörpern, deren zugehörige galoissche Körper spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage, Math. Zeitschr. **37** (1933), 149, Satz VII.

[4]) E. Artin, Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, Journ. f. Math. **164** (1931), 1—11. — Im folgenden zitiert mit „Artin".

gruppe $\mathfrak{G}$ von N/Ω bekanntlich von der Struktur:

$$S^p = 1, \quad T^n = 1, \quad TST^{-1} = S^r,$$

wobei n ein Teiler von $p-1$ und r eine Restklasse mod. p von der Ordnung n ist. K ist der Invariantenkörper etwa der Untergruppe $\{T\}$; der Invariantenkörper Z des Normalteilers $\{S\}$ ist zyklisch vom Grade n über Ω, sowie N zyklisch vom Grade p über Z.

Zur Anwendung der Artinschen Theorie haben wir zunächst die absolut-irreduziblen Darstellungen von $\mathfrak{G}$ aufzustellen. Wir geben die Darstellungsmatrizen selbst nur für die Erzeugenden S und T von $\mathfrak{G}$ an, und berechnen daraus die Charaktere der Darstellungen jeweils für die drei Typen von Elementen:

$$1, \quad S^i \quad (i = 1, \ldots, p-1), \quad S^i T^j \quad \begin{pmatrix} i = 0, 1, \ldots, p-1 \\ j = 1, 2, \ldots, n-1 \end{pmatrix}.$$

a) Die n Darstellungen ersten Grades der zyklischen Faktorgruppe $\mathfrak{G}/\{S\} \cong \{T\}$ liefern n Darstellungen ersten Grades auch für $\mathfrak{G}$:

$$S \to 1, \quad T \to \varepsilon^\nu \qquad (\nu = 0, 1, \ldots, n-1)$$

(ε primitive n-te Einheitswurzel),

mit den Charakteren

$$\psi_\nu(1) = 1, \quad \psi_\nu(S^i) = 1, \quad \psi_\nu(S^i T^j) = \varepsilon^{j\nu}.$$

b) Weitere Darstellungen ergeben sich, indem man von einer (nicht-identischen) Darstellung ersten Grades der Untergruppe $\{S\}$ ausgeht:

$$S \to \zeta^\mu \qquad (\mu \not\equiv 0 \text{ mod. } p)$$

(ζ primitive p-te Einheitswurzel),

mit dem Charakter

$$\varphi_\mu(1) = 1, \quad \varphi_\mu(S^i) = \zeta^{i\mu},$$

und die zugehörige induzierte Darstellung von $\mathfrak{G}$ bildet. Entsprechend den Relationen

$$T^\nu \cdot S = S^{r^\nu} T^\nu, \quad T^\nu \cdot T = T^{\nu+1} \qquad (\nu = 0, 1, \ldots, n-1)$$

ergibt sich als induzierte Darstellung

$$S \to \begin{pmatrix} \zeta^\mu & & & \\ & \zeta^{\mu r} & & \\ & & \ddots & \\ & & & \zeta^{\mu r^{n-1}} \end{pmatrix}, \quad T \to \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix},$$

mit dem Charakter

$$\chi_{\varphi_\mu}(1) = n, \qquad \chi_{\varphi_\mu}(S^i) = \sum_{\nu=0}^{n-1} \zeta^{i\mu r^\nu} = \eta_{i\mu}, \qquad \chi_{\varphi_\mu}(S^i T^j) = 0$$

(p-te Kreisteilungsperioden m-ten Grades).

Dabei kommt es auf μ nur mod. $\{r\}$, der durch r erzeugten Untergruppe der Ordnung n der primen Restklassengruppe mod. p, an; es genügt also, μ ein volles Repräsentantensystem von $m = \frac{p-1}{n}$ Resten mod. p nach dieser Untergruppe $\{r\}$ durchlaufen zu lassen. Im folgenden habe μ durchweg diese Bedeutung.

So entstehen m wegen der Verschiedenheit ihrer Charaktere nicht-äquivalente Darstellungen n-ten Grades von G. Der zugehörige Gruppenring über dem Körper $\mathsf{P}(\eta)$ des Charakters (Körper der p-ten Kreisteilungsperioden m-ten Grades) ist jedesmal das zyklische verschränkte Produkt des p-ten Kreiskörpers $\mathsf{P}(\xi)/\mathsf{P}(\eta)$ mit Faktorensystem 1, also eine einfache normale Algebra vom Grade n über $\mathsf{P}(\eta)$; daher sind die erhaltenen m Darstellungen n-ten Grades absolut-irreduzibel.

Die damit gewonnenen $n + m$ nicht-äquivalenten absolut-irreduziblen Darstellungen von G sind bereits ein vollständiges System. Denn die Quadratsumme ihrer Grade ergibt

$$n \cdot 1^2 + m \cdot n^2 = n + \frac{p-1}{n} n^2 = n + (p-1)n = pn,$$

also die Ordnung von $\mathfrak{G}$.

2.

Nach Artin (20) ist die Diskriminante von K/Ω gegeben durch

$$\mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{f}(\chi_{\psi_0^0}, \mathsf{N}/\Omega),$$

wo ψ_0^0 die identische Darstellung der K zugeordneten Untergruppe $\{T\}$ bezeichnet. Zur Berechnung des Führers rechts haben wir die durch ψ_0^0 induzierte Darstellung von $\mathfrak{G}$ in ihre absolut-irreduziblen Bestandteile zu zerlegen. Diese induzierte Darstellung ist nun, entsprechend den Relationen

$$S \cdot S^k = S^{k+1}, \qquad T \cdot S^k = S^{kr} T,$$

die bekannte Darstellung von $\mathfrak{G}$ als lineare Permutationsgruppe p-ten Grades mod. p, mit dem Charakter

$$\chi_{\psi_0^0}(1) = p, \qquad \chi_{\psi_0^0}(S^i) = 0, \qquad \chi_{\psi_0^0}(S^i T^j) = 1.$$

Andrerseits liefert auch die aus den oben bestimmten absolut-irreduziblen Charakteren gebildete Summe $\psi_0 + \sum\limits_{\mu} \chi_{\varphi_\mu}$ die Werte

$\psi_0(1) + \sum\limits_{\mu} \chi_{\varphi_\mu}(1) = 1 + mn$ $= p,$	$\psi_0(S^i) + \sum\limits_{\mu} \chi_{\varphi_\mu}(S^i) = 1 + \sum\limits_{\mu} \eta_{i\mu}$ $= 0,$	$\psi_0(S^i T^j) + \sum\limits_{\mu} \chi_{\varphi_\mu}(S^i T^j) = 1 + 0$ $= 1.$

Somit gilt

$$\chi_{\psi_0^0} = \psi_0 + \sum_{\mu} \chi_{\varphi_\mu}.$$

Daraus folgt nach Artin (18)

$$\begin{aligned}\mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{f}(\chi_{\psi_0^0}, \mathsf{N}/\Omega) &= \mathfrak{f}(\psi_0, \mathsf{N}/\Omega) \cdot \prod_{\mu} \mathfrak{f}(\chi_{\varphi_\mu}, \mathsf{N}/\Omega) \\ &= \prod_{\mu} \mathfrak{f}(\chi_{\varphi_\mu}, \mathsf{N}/\Omega),\end{aligned}$$

letzteres, da für den Hauptcharakter ψ_0 von $\mathfrak{G}$ gilt

$$\mathfrak{f}(\psi_0, \mathsf{N}/\Omega) = 1.$$

Ferner ist nach Artin (19)

$$\mathfrak{f}(\chi_{\varphi_\mu}, \mathsf{N}/\Omega) = \mathfrak{D}_{\mathsf{Z}/\Omega} \cdot N_{\mathsf{Z}/\Omega}(\mathfrak{f}(\varphi_\mu, \mathsf{N}/\mathsf{Z})),$$

also

$$\mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{D}_{\mathsf{Z}/\Omega}^m \cdot \prod_{\mu} N_{\mathsf{Z}/\Omega}(\mathfrak{f}(\varphi_\mu, \mathsf{N}/\mathsf{Z})).$$

Weil konjugiert-algebraische Charaktere denselben Führer haben, sind alle $\mathfrak{f}(\varphi_\mu, \mathsf{N}/\mathsf{Z})$ einander gleich, und ihr gemeinsamer Wert $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}}$ ist bei den Automorphismen von Z/Ω invariant. Wir haben somit schließlich

$$\mathfrak{D}_{\mathsf{K}/\Omega} = \mathfrak{D}_{\mathsf{Z}/\Omega}^m \cdot N_{\mathsf{Z}/\Omega}(\mathfrak{f}_{\mathsf{N}/\mathsf{Z}})^m = \mathfrak{D}_{\mathsf{Z}/\Omega}^{\frac{p-1}{n}} \cdot \mathfrak{f}_{\mathsf{N}/\mathsf{Z}}^{p-1}. \tag{1}$$

Damit ist die eingangs angeführte Wegner-Poruschsche Diskriminantenformel (für einen beliebigen Grundkörper Ω statt P) bewiesen, und zwar auf formal-gruppentheoretischem Wege, ohne die klassenkörpertheoretische Bedeutung von $f_{\mathsf{N}/\mathsf{Z}}$ als Führer der N in Z zugeordneten Idealgruppe $H_{\mathsf{N}/\mathsf{Z}}$ heranzuziehen.

Auch die aus der Klassenkörpertheorie bekannte Formel

$$\mathfrak{D}_{\mathsf{N}/\mathsf{Z}} = f_{\mathsf{N}/\mathsf{Z}}^{p-1} \tag{2}$$

ergibt sich ohne weiteres auf diesem formal-gruppentheoretischen Wege, ebenso die bekannte Relativdiskriminantenformel

$$\mathfrak{D}_{\mathsf{N}/\Omega} = \mathfrak{D}_{\mathsf{Z}/\Omega}^{p} \cdot N_{\mathsf{Z}/\Omega}(\mathfrak{D}_{\mathsf{N}/\mathsf{Z}}) = \mathfrak{D}_{\mathsf{Z}/\Omega}^{p} \cdot \mathfrak{f}_{\mathsf{N}/\mathsf{Z}}^{n(p-1)}. \tag{3}$$

Durch Kombination mit der obigen Diskriminantenformel (1) ergibt sich aus ihr die von Wegner in der vorstehenden Arbeit benutzte Formel

$$\mathfrak{D}_{\mathsf{N}/\Omega} = \mathfrak{D}_{\mathsf{Z}/\Omega} \cdot \mathfrak{D}_{\mathsf{K}/\Omega}^{n}. \tag{4}$$

3.

Porusch hat (im Spezialfall $\Omega = \mathsf{P}$) noch die folgende Tatsache aus seiner tabellarischen Zusammenstellung abgelesen (a. a. O. 149, Satz VI):

$\mathfrak{D}_{\mathsf{Z}/\Omega}$ *und* $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}}$ *haben höchstens Primteiler von p gemeinsam.*

Dies läßt sich ganz einfach mittels der Diskriminantenformeln (1) und (4) beweisen. Aus Teilbarkeitsgründen für die Verzweigungsordnungen ist ohne weiteres klar:

Ein Primideal $\mathfrak{q}_\Omega$ ist dann und nur dann voll-verzweigt in K ($\mathfrak{q}_\Omega = \mathfrak{q}_{\mathsf{K}}^{p}$), wenn einer (und damit jeder) seiner Primteiler $\mathfrak{q}_{\mathsf{Z}}$ verzweigt in N ist ($\mathfrak{q}_{\mathsf{Z}} = \mathfrak{q}_{\mathsf{N}}^{p}$).

Sei nun $\mathfrak{q}_{\mathsf{Z}} \mid \mathfrak{f}_{\mathsf{N}/\mathsf{Z}}$, also $\mathfrak{q}_{\mathsf{Z}} = \mathfrak{q}_{\mathsf{N}}^{p}$, und somit $\mathfrak{q}_\Omega = \mathfrak{q}_{\mathsf{K}}^{p}$, so ist für $\mathfrak{q}_\Omega \nmid p$ nach dem Dedekindschen Diskriminantensatz der Beitrag

$$\mathfrak{D}_{\mathsf{K}/\Omega}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{p-1}.$$

Da für $\mathfrak{q}_\Omega \nmid p$ in N/Z keine höhere Verzweigung vorliegt, ist ferner etwa nach Artin (17),

$$\mathfrak{f}_{\mathsf{N}/\mathsf{Z}}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{\frac{1}{e}},$$

wo e die Verzweigungsordnung für Z/Ω ist, also

$$\mathfrak{f}_{\mathsf{N}/\mathsf{Z}}(\mathfrak{q}_\Omega)^{p-1} = \mathfrak{q}_\Omega^{\frac{p-1}{e}}.$$

Nach der Diskriminantenformel (1) ist daher

$$\mathfrak{D}_{\mathsf{Z}/\Omega}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{n\left(1-\frac{1}{e}\right)},$$

und weiter nach (4)

$$\mathfrak{D}_{\mathsf{N}/\Omega}(\mathfrak{q}_\Omega) = \mathfrak{q}_\Omega^{n\left(1-\frac{1}{e}\right)+n(p-1)} = \mathfrak{q}_\Omega^{np\left(1-\frac{1}{ep}\right)}.$$

Da ep die Verzweigungsordnung für N/Ω ist, liegt also gemäß dem Dedekindschen Diskriminantensatz auch für Z/Ω und N/Ω keine höhere Verzweigung vor, d. h. die Trägheitsgruppe für N/Ω ist zyklisch von der Ordnung ep. Mit Hinblick auf die Struktur der Gruppe $\mathfrak{G}$ ist dies nur für $e = 1$ möglich, und das bedeutet $\mathfrak{q}_\Omega \nmid \mathfrak{D}_{\mathsf{Z}/\Omega}$.

4.

Sei von jetzt an der Grundkörper $\Omega = \mathsf{P}$. Spezielle Körper K der betrachteten Art sind die binomischen Körper

$$\mathsf{K} = \mathsf{P}(\sqrt[p]{a}),$$

wo a eine Zahl aus P ist, die keine p-te Potenz in P ist, und die ganz und p-te-potenzfrei angenommen werden kann. Für diese Körper K ist

$$\mathsf{N} = \mathsf{P}(\zeta, \sqrt[p]{a}), \quad \mathsf{Z} = \mathsf{P}(\zeta), \quad n = p - 1 .$$

Ferner ist

$$p = \mathfrak{p}^{p-1}, \quad \mathfrak{p} = (1 - \zeta)$$

in Z, und

$$\mathfrak{D}_{\mathsf{Z}/\mathsf{P}} = p^{p-2} .$$

Nach der Theorie der Kummerschen Körper ist, wenn a_0 das Produkt der von p und untereinander verschiedenen Primzahlen $q|a$ bezeichnet,

$$\mathfrak{f}_{\mathsf{N}/\mathsf{Z}} = \left\{ \begin{array}{lll} \mathfrak{p}^0 \, a_0, & \text{wenn} \;\; p \nmid a, & a^{p-1} \equiv 1 \bmod. p^2 \\ \mathfrak{p}^2 \, a_0, & \text{wenn} \;\; p \nmid a, & a^{p-1} \not\equiv 1 \bmod. p^2 \\ \mathfrak{p}^{p+1} a_0, & \text{wenn} \;\; p \mid a & \end{array} \right\} .$$

Nach (1) ist also entsprechend

$$\text{(5)} \qquad \mathfrak{D}_{\mathsf{K}/\mathsf{P}} = p^{p-2} \left\{ \begin{array}{ll} p^0 & a_0^{p-1} \\ p^2 & a_0^{p-1} \\ p^{p+1} & a_0^{p-1} \end{array} \right\},$$

wie es von Wegner a. a. O. 182 festgestellt wurde.

5.

Sei jetzt umgekehrt, wie in der vorstehenden Arbeit von Wegner, vorausgesetzt, daß K ein auflösbarer Körper vom Primzahlgrad p über P ist, dessen Diskriminante $\mathfrak{D}_{\mathsf{K}/\mathsf{P}}$ von einer der drei Formen (5) ist, wo jetzt $a_0 = q_1 \cdots q_s$ ein gegebenes Produkt untereinander und von p verschiedener Primzahlen ist.

Wegner findet dann die folgenden Bedingungen als hinreichend dafür, daß K binomisch über P ist:

Die Primzahl 2 kommt nicht unter den q_i vor.

Bei Vorliegen der ersten Form von $\mathfrak{D}_{\mathsf{K}/\mathsf{P}}$ in (5) ist $s \geqq 1$, und wenn f_i die Ordnungen der q_i mod. p sind, so sind die Zahlen

$$e_i = \frac{p-1}{f_i}$$

teilerfremd.

Ich will hier nur noch zeigen, wie man die folgenden drei vorbereitenden Feststellungen für Wegners Beweis unmittelbar aus der Diskriminnatenformel (1) ablesen kann:

a) Es ist $n = p - 1$.

b) Es ist $p = \mathfrak{p}^{p-1}$ in Z.

c) Es ist $\mathfrak{f}_{\mathsf{Z}/\mathsf{P}} = p$ oder $4p$, je nachdem $2 \nmid \mathfrak{D}_{\mathsf{Z}/\mathsf{P}}$ oder $2 \mid \mathfrak{D}_{\mathsf{Z}/\mathsf{P}}$.

Ad a). Vergleicht man die Voraussetzung (5) mit der Diskriminantenformel (1) (erste Form) und beachtet, daß p in (5) einen Exponenten $\equiv \pm 1$ mod. p hat, so ergibt sich $m \mid 1$, also $m = 1$, d. h. $n = p - 1$.

Ad b). Bezeichnet e die Verzweigungsordnung von p für Z/P, so ist nach dem Dedekindschen Diskriminantensatz

$$\mathfrak{D}_{\mathsf{Z}/\mathsf{P}}(p) = p^{(p-1)\left(1-\frac{1}{e}\right)} .$$

Ferner ist, etwa nach Artin (17),

$$\mathfrak{f}_{N/Z}(p) = p^{\frac{1}{e}(v+1)},$$

wo v die Anzahl der von 1 verschiedenen Verzweigungsgruppen für N/Z ist. Nach der Diskriminantenformel (1) ist also

$$\mathfrak{D}_{K/P}(p) = p^{(p-1)\left(1-\frac{1}{e}+\frac{v+1}{e}\right)} = p^{p-1+\frac{p-1}{e}v}.$$

Vergleicht man dies mit der Voraussetzung (5), so folgt

$$\frac{p-1}{e}\, v = \left\{\begin{matrix} -1 \\ 1 \\ p \end{matrix}\right\},$$

also notwendig $\frac{p-1}{e} = 1$, d. h. $e = p - 1$.

Ad c). Angenommen $\mathfrak{D}_{Z/P}$ enthält außer p noch eine andere Primzahl q. Nach dem oben Gezeigten gehen dann die $\mathfrak{q}_Z$ nicht in $\mathfrak{f}_{N/Z}$ auf, so daß also nach (1) und (5)

$$\mathfrak{D}_{Z/P}(q) = q^{p-1}$$

ist. Wie in der vorstehenden Arbeit von Wegner folgt daraus nach der allgemeinen Diskriminantenformel für Z/P, daß $q = 2$ ist, und daß in der zugehörigen Verzweigungsgruppenreihe nur die erste Verzweigungsgruppe von 1 verschieden ist, die Ordnung 2^1 hat und mit der Vielfachheit 1 auftritt. Insbesondere ist daher die Verzweigungsordnung von 2 in Z/P von der Form

$$e = 2e_0 \quad \text{mit} \quad (e_0, 2) = 1.$$

Hieraus kann nach Artin (17) der Beitrag von 2 zum Führer

$$\mathfrak{f}_{Z/P} = \mathfrak{f}(\psi_1^0, Z/P)$$

berechnet werden, wo ψ_1^0 ein erzeugender Charakter der Galoisgruppe $\{T\}$ von Z/P ist. Es ergibt sich

$$\mathfrak{f}_{Z/P}(2) = 2^{\frac{1}{e}[(e-0)+(2-0)]} = 2^{1+\frac{2}{e}}.$$

Hiernach ist notwendig $e \mid 2$, also $e = 2$, und somit

$$\mathfrak{f}_{Z/P}(2) = 2^2.$$

Daß $e = 2$, also $e_0 = 1$ sein muß, ist ein Spezialfall der allgemeinen Tatsache, daß die Vielfachheiten v_i der Verzweigungsgruppen abelscher Körper sämtlich durch den primen Bestandteil e_0 der Verzweigungsordnung teilbar sind [5]); diese Tatsache folgt allgemein aus der Identität der formalen Artinschen Führer mit den klassenkörpertheoretisch definierten Führern im abelschen Falle, denn danach sind die Exponenten der Artinschen Führer ganzzahlig.

---

[5]) Siehe H. Hasse, Führer, Diskriminante und Verzweigungskörper relativ-abelscher Zahlkörper, Journ. f. Math. **162** (1930), 171.

Eingegangen 5. Mai 1936.