Bestimmung eines auflösbaren Körpers von Primzahlgrad aus der Form seiner Diskriminante.

Von *Udo Wegner* in Darmstadt.

In einer früheren Arbeit [1]) habe ich unter anderem gezeigt, daß die Diskriminante $\vartheta_{\mathsf{K}/\mathsf{P}}$ eines binomischen Körpers $\mathsf{K} = \mathsf{P}(\sqrt[p]{a})$ vom Primzahlgrad p über dem Körper P der rationalen Zahlen, als Hauptideal in P geschrieben (also bis aufs Vorzeichen), die Form hat:

$$\vartheta_{\mathsf{K}/\mathsf{P}} = p^{p-2} p^m (p_1 \cdots p_n)^{p-1} = p^{p-2} p^m a_0^{p-1}, \qquad p_\mu \neq p_\nu, p,$$

wobei m einen der folgenden drei Werte hat:

$$\begin{aligned} &\alpha) \quad m = 0, \\ &\beta) \quad m = 2, \\ &\gamma) \quad m = p + 1. \end{aligned}$$

Hierbei ist im Falle α) und β)

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \qquad \text{mit} \quad \alpha_\nu \not\equiv 0 \bmod. p$$

[und zwar tritt Fall α) auf, wenn $a^p \equiv a \bmod. p^2$ ist, und Fall β), wenn $a^p \not\equiv a \bmod. p^2$ ist], und im Falle γ)

$$a = p^\alpha p_1^{\alpha_1} \cdots p_n^{\alpha_n} \qquad \text{mit} \quad \alpha, \alpha_\nu \not\equiv 0 \bmod. p.$$

Es erhebt sich nun die interessante Frage, ob umgekehrt jeder auflösbare algebraische Zahlkörper vom Primzahlgrad p ein binomischer Körper ist, wenn seine Diskriminante die Form $p^{p-2} p^m (p_1 \cdots p_n)^{p-1}$ hat, wo m eine der Zahlen $0, 2, p + 1$ bedeutet. Unter gewissen ziemlich einschränkenden Voraussetzungen bezüglich der p_ν konnte ich diese Frage in bejahendem Sinne beantworten [2]). Im folgenden will ich zeigen, daß diese Voraussetzungen wesentlich reduziert werden können. Es gilt nämlich der folgende

Satz. *Ist* K *ein auflösbarer Körper vom Primzahlgrad* p *über* P, *und ist die Diskriminante*

$$\vartheta_{\mathsf{K}/\mathsf{P}} = p^{p-2} \begin{Bmatrix} p^0 & a_0^{p-1} \\ p^2 & a_0^{p-1} \\ p^{p+1} & a_0^{p-1} \end{Bmatrix},$$

[1]) U. Wegner, Zur Theorie der auflösbaren Gleichungen von Primzahlgrad. I, Journal f. reine u. angew. Math. **168** (1932), S. 176—192.

[2]) Siehe [1]), S. 189. — Im Beweis des Satzes auf S. 190, Zeile 5, muß λ eine p-te Idealpotenzzahl und keine Einheit darstellen, worauf Herr A. Scholz freundlicherweise aufmerksam machte. Der Beweis bleibt dabei fast wörtlich bestehen. Ich führe ihn kurz an. Aus $\mu = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n} \lambda$ und $S(\mu) = \mu^\varkappa \alpha^p$ (in den dortigen Bezeichnungen) folgt dann durch Normbildung $\varkappa = 1$ und dann durch wiederholtes Anwenden von S auf $S(\lambda) = \lambda \alpha_1^p$ weiter $N(\lambda) = \lambda^{p-1} \beta^p$, d. h. $\lambda^{-1} = N(\lambda) \gamma^p$. Also darf μ rational angenommen werden.

wo a_0 *ein Produkt von verschiedenen Primzahlen* $p_\nu \neq p$, 2 *ist, deren Anzahl im ersten Falle mindestens* 1 *ist und für die in diesem ersten Falle die* $e_\nu = \frac{p-1}{f_\nu}$ (f_ν *der Exponent von* p_ν mod. p) *teilerfremd sind, so ist* $\mathsf{K} = \mathsf{P}(\sqrt[p]{a})$ *mit rationalem* a, *also* K *ein binomischer Körper* [3]).

Beweis. Sei K ein über dem rationalen Zahlkörper P auflösbarer Körper vom Primzahlgrad p und N der kleinste K enthaltende Normalkörper über P. Dann wird N gebildet als Produkt von K und einem zyklischen Körper Z vom Grade $\frac{p-1}{\varkappa}$, wo $\varkappa$ ein Teiler von $p-1$ ist. Denn die Galoissche Gruppe $\mathfrak{G}$ ist ein Teiler der vollen linearen Gruppe des Grades p und der Ordnung $p(p-1)$. $\mathfrak{G}$ wird erzeugt durch zwei Substitutionen S und $T^\varkappa$, wobei

$$S^p = T^{p-1} = E \quad \text{und} \quad ST = TS^r$$

ist (r eine Primitivwurzel mod. p). $\mathfrak{G}$ besitzt eine invariante Untergruppe der Ordnung p, nämlich den durch S erzeugten Zyklus [4]).

A. Wir behaupten, daß $\varkappa = 1$ ist.

Im Falle α) schließt man wie folgt: In K ist [5])

$$(p) = \bar{\mathfrak{q}}_1 (\mathfrak{q}_1 \cdots \mathfrak{q}_e)^b \left\{ \begin{array}{l} \bar{\mathfrak{q}}_1 \text{ vom Grade } 1 \\ \mathfrak{q}_\nu \text{ vom Grade } f = \frac{p-1}{eb} \end{array} \right\}.$$

Wegen $(b, p) = 1$ ist $\vartheta_{\mathsf{K}/\mathsf{P}}$ genau durch $p^{ef(b-1)}$ teilbar. Nach Voraussetzung ist demnach

$$ef(b-1) = p-2.$$

Da andrerseits

$$efb = p-1$$

ist, muß $ef = 1$, also $e = 1$, $f = 1$, $b = p-1$ sein. In Z ist nun [6])

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_a)^b, \quad \mathfrak{p}_\nu \text{ vom Grade } f = \frac{p-1}{\varkappa a b}, \quad \varkappa a = e.$$

Zusammengenommen ergibt sich also $\varkappa = 1$.

Für später vermerken wir noch, daß aus den erhaltenen Zerlegungen

$$(p) = \bar{\mathfrak{q}}_1 \mathfrak{q}_1^{p-1} \text{ in } \mathsf{K}, \qquad (p) = \mathfrak{p}^{p-1} \text{ in } \mathsf{Z}$$

die Unverzweigtheit von $\mathfrak{p}$ in N folgt, so daß also $\mathfrak{p}$ im Falle α) nicht in $\vartheta_{\mathsf{Z}/\mathsf{P}}$ vorkommt.

Im Falle β) und γ) ergibt sich unsere Behauptung durch Vergleich der allgemeinen Diskriminantenformel

$$\vartheta_{\mathsf{N}/\mathsf{P}} = \vartheta_{\mathsf{Z}/\mathsf{P}}^n \cdot N_{\mathsf{Z}/\mathsf{P}}(\vartheta_{\mathsf{N}/\mathsf{P}})$$

---

[3]) Schon an dieser Stelle möchte ich Herrn Hasse meinen besten Dank sagen für das große Interesse, das er dieser Arbeit entgegenbrachte, und für die vielen Ratschläge, die er mir erteilte. Insbesondere danke ich ihm für den Beweis, daß man die zum ersten Fall gemachten Voraussetzungen im zweiten und dritten Fall entbehren kann.

[4]) Siehe [1]), S. 177.

[5]) Siehe F. K. Schmidt, Zur Theorie der algebraisch auflösbaren Polynome und Zahlkörper von Primzahlgrad, Sitzungsber. d. Heidelberger Akad. 1929, Math.-nat. Kl., 2. Abhdl., S. 3—10; ferner [1]), S. 179; außerdem I. Porusch, Die Arithmetik in Zahlkörpern, deren zugehörige Galoissche Körper spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage, Math. Zeitschr. **37** (1933), S. 134—160. — Letztere Arbeit zitiere ich nachstehend mit P.

[6]) Siehe [1]), S. 179, und P, S. 140.

mit der in unserem Falle gültigen speziellen Diskriminantenformel [7])

$$\vartheta_{N/P} = \vartheta_{K/P}^{\frac{p-1}{\varkappa}} \cdot \vartheta_{Z/P}.$$

Da $\vartheta_{K/P}$ nach Voraussetzung genau durch p^{p+s} teilbar ist, mit $s = 0$ im Falle β), $s = p - 1$ im Falle γ), so ist jetzt p nach dem Dedekindschen Diskriminantensatz notwendig eine für K irreguläre Primzahl im Sinne dieses Satzes, und daher notwendig

$$(p) = \mathfrak{q}^p, \quad \mathfrak{q} \text{ vom Grade } 1$$

in K. Ist wieder

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_a)^b, \quad \mathfrak{p}_\nu \text{ vom Grade } f = \frac{p-1}{\varkappa a b}$$

in Z, so ist also notwendig jedes der Primideale $\mathfrak{p}_\nu$ in N verzweigt und somit in $\vartheta_{N/Z}$ enthalten. Nach einem bekannten Satz über relativ-zyklische Körper von Primzahlgrad ist $\vartheta_{N/Z}$ dann genau durch $(\mathfrak{p}_1 \cdots \mathfrak{p}_a)^{(p-1)(v+1)}$ teilbar (mit $1 \leqq v \leqq \frac{bp}{p-1}$ und $(v, p) = 1$ oder $v = \frac{bp}{p-1}$). Demnach ist $N_{Z/P}$ ($\vartheta_{N/Z}$) genau durch $p^{af(p-1)(v+1)}$ teilbar. Da $\vartheta_{Z/P}$ wegen $(b, p) = 1$ genau durch $p^{af(b-1)}$ teilbar ist, wird $\vartheta_{N/P}$ nach der ersten Diskriminantenformel genau durch p^E teilbar, wo

$$E = af(p-1)(v+1) + af(b-1)p$$

ist. Andrerseits ist nach der zweiten Diskriminantenformel

$$E = (p+s)\frac{p-1}{\varkappa} + af(b-1)$$

$$= afb(p+s) + af(b-1), \quad \text{wegen } f = \frac{p-1}{\varkappa a b}.$$

Der Vergleich ergibt nach Division mit af:

$$(p-1)(v+1) + (b-1)p = b(p+s) + (b-1)$$

oder also

$$(p-1)(v+b) = b(p+s).$$

$$v + b = \frac{b}{p-1}(p+s).$$

Wegen $s = 0$ oder $p - 1$ ist hiernach $p - 1 | b$, was mit $b | p - 1$ zusammen $b = p - 1$ ergibt. Dies hat $\varkappa = 1$ zur Folge.

Für später vermerken wir noch die sich weiter ergebenden Tatsachen $a = 1$, also $(p) = \mathfrak{p}^{p-1}$ in Z, sowie $v + 1 = s + 2 = 2$ oder $p + 1$, so daß also $\vartheta_{N/Z}$ genau durch $\mathfrak{p}^{2(p-1)}$ oder $\mathfrak{p}^{(p+1)(p-1)}$ teilbar ist, je nachdem Fall β) oder Fall γ) vorliegt.

B. In der Diskriminante von Z geht nur die Primzahl p auf. (Läßt man die gemachte Voraussetzung fallen, daß die $p_\nu \neq 2$ sein sollen, so geht unter Umständen auch noch die Primzahl 2 in der Diskriminante von Z auf.)

Da $\vartheta_{Z/P}$ Teiler von $\vartheta_{N/P}$ ist und $\vartheta_{N/P}$ bekanntlich aus genau denselben Primzahlen zusammengesetzt ist wie $\vartheta_{K/P}$, so gehen in $\vartheta_{Z/P}$ außer p höchstens die in der Voraussetzung genannten Primteiler p_ν von a_0 auf.

Wir zeigen zunächst, daß für diese p_ν die Zerlegung in K

$$(p_\nu) = \mathfrak{q}^p$$

---

[7]) Siehe [1]), S. 183, Zeile 2, und P, S. 150, sowie die nachstehende Arbeit von H. Hasse.

lautet. Falls p_ν eine für K reguläre Primzahl ist, ergibt sich dies wieder ohne weiteres aus dem Dedekindschen Diskriminantensatz und der Voraussetzung, daß $\vartheta_{K/P}$ genau durch p_ν^{p-1} teilbar ist.

Allgemein sei

$$(p_\nu) = (\mathfrak{p}_1 \cdots \mathfrak{p}_a)^b, \qquad \mathfrak{p}_i \text{ vom Grade } f = \frac{p-1}{ab}$$

in Z. Dann geht p_ν in $\vartheta_{Z/P}$ genau zum Exponenten $af(b - 1 + \varrho)$ auf, wo $\varrho \geqq 0$ die zugehörige Supplementzahl ist. Angenommen nun, die Primteiler $\mathfrak{p}_i$ gingen nicht in der Relativdiskriminante $\vartheta_{N/Z}$ auf. Dann wird

$$(p_\nu) = (\mathfrak{P}_1 \cdots \mathfrak{P}_c)^b$$

in N, und wegen

$$\vartheta_{N/P} = \vartheta_{Z/P}^{p} \cdot N_{Z/P}(\vartheta_{N/Z})$$

geht p_ν in $\vartheta_{N/P}$ genau zum Exponenten

$$E = paf(b - 1 + \varrho)$$

auf. Durch Vergleich mit

$$\vartheta_{N/P} = \vartheta_{K/P}^{p-1} \cdot \vartheta_{Z/P},$$

also

$$E = (p-1)(p-1) + af(b - 1 + \varrho),$$

folgt

$$af(b - 1 + \varrho) = p - 1,$$

was wegen

$$afb = p - 1$$

für die Supplementzahl ϱ den Wert

$$\varrho = 1$$

ergibt. Andrerseits ist nun nach der Diskriminantenformel der Hilbertschen Theorie des galoisschen Zahlkörpers für den zyklischen Körper Z die zu p_ν gehörige Supplementzahl ϱ gegeben durch

$$\varrho = (1 - p_\nu^l) + L(p_\nu^l - p_\nu^{l-1}) + \overline{L}(p_\nu^{l-1} - p_\nu^{l-2}) + \cdots + \overset{(l-1)}{\overline{L}}(p_\nu - 1),$$

wo p_ν^l die Ordnung der (ersten) Verzweigungsgruppe (also der Beitrag der Primzahl p_ν zu b) ist und $L, \overline{L}, \ldots, \overset{(l-1)}{\overline{L}}$ die zu den einzelnen Verzweigungsgruppen der Ordnungen $p_\nu^l, p_\nu^{l-1}, \ldots, p_\nu$ gehörigen Exponenten sind, die jedenfalls die Ungleichungen

$$1 < L < \overline{L} < \cdots < \overset{(l-1)}{\overline{L}}$$

erfüllen. Daraus und aus $\varrho = 1$ ergibt sich hier die Ungleichung

$$1 \geqq (1 - p_\nu^l) + L(p_\nu^l - 1) = (L-1)(p_\nu^l - 1),$$

die nur für $L = 1$, $p_\nu = 2$, $l = 1$ möglich ist. Da wir $p_\nu \neq 2$ vorausgesetzt hatten, ist also die Annahme $\mathfrak{p}_i \nmid \vartheta_{N/Z}$ unzutreffend, und somit ist $\mathfrak{p}_i \mid \vartheta_{N/Z}$. Daher zerfallen die $\mathfrak{p}_\nu$ in N nach dem Gesetz $\mathfrak{p}_i = \mathfrak{P}_i^p$, und daraus folgt ohne weiteres, daß p_ν in K nach dem Gesetz $(p_\nu) = \mathfrak{q}^p$ zerfällt.

Aus dieser nunmehr für jedes p_ν bewiesenen Tatsache ergibt sich bekanntlich weiter [8]), daß p_ν in N die Zerlegung

$$(p_\nu) = (\mathfrak{P}_1 \cdots \mathfrak{P}_a)^p$$

hat, während durch Eintragen von $\mathfrak{p}_i = \mathfrak{P}_i^p$ in obige Zerlegung von p_ν in Z die Zerlegung

$$(p_\nu) = (\mathfrak{P}_1 \cdots \mathfrak{P}_a)^{bp}$$

in N folgt. Demnach ergibt sich $b = 1$, und daher geht p_ν nicht in $\vartheta_{\mathsf{Z}/\mathsf{P}}$ auf, wie behauptet.

Für später vermerken wir noch, daß die $\mathfrak{p}_i$ als für N/Z reguläre Primideale in $\vartheta_{\mathsf{N}/\mathsf{Z}}$ genau zum Exponenten $p - 1$ aufgehen, so daß also mit Rücksicht auf $b = 1$ jedes p_ν zu $\vartheta_{\mathsf{N}/\mathsf{Z}}$ den Beitrag p_ν^{p-1} liefert.

Läßt man auch $p_\nu = 2$ zu und berechnet den Beitrag, den die Primzahl 2 in dem eben behandelten Falle $\mathfrak{p}_i \nmid \vartheta_{\mathsf{N}/\mathsf{Z}}$ zum Führer von Z liefert [9]), so ergibt sich 2^2. Allgemein gilt also:

Z/P *ist ein zyklischer Körper vom Grade* $p - 1$, *dessen Führer entweder* p *oder* $4p$ *ist.*

Nach der Theorie der alsolut-abelschen Körper besagt das:

Z *ist entweder der Körper der* p*-ten Einheitswurzeln oder ein im Körper der* $4p$*-ten* (*aber nicht schon der* p*-ten*) *Einheitswurzeln enthaltener zyklischer Körper vom Grade* $p - 1$.

Je nachdem $p \equiv 1$ oder -1 mod. 4 ist, gibt es nur einen solchen Körper vom Führer $4p$ oder zwei.

Unter unserer Voraussetzung, daß die Primzahl 2 *nicht in* a_0 *vorkommt, ist stets* $\mathsf{Z} = \mathsf{P}(\zeta)$ *der Körper der* p*-ten Einheitswurzeln.*

Ich möchte diese letztere Tatsache noch ganz elementar, ohne Benutzung der Theorie der absolut-abelschen Körper, aus der erhaltenen Feststellung folgern, daß $\vartheta_{\mathsf{Z}/\mathsf{P}}$ nur die Primzahl p enthält.

Z ist als Produkt zyklischer Körper Z_λ von Primzahlpotenzgraden $t_\lambda^{u_\lambda}$ darstellbar, mit $t_\lambda^{u_\lambda} | p - 1$. Zu einem dieser Körper Z_λ adjungieren wir den Teilkörper K_λ gleichen Grades des Körpers $\mathsf{P}(\zeta)$ der p-ten Einheitswurzeln. Der so entstehende zusammengesetzte Körper M_λ ist von einem Grade $t_\lambda^{u_\lambda + v_\lambda}$. Ein in p aufgehendes Primideal $\mathfrak{p}$ von M_λ geht mindestens zum Exponenten $t_\lambda^{u_\lambda}$ in p auf, da (p) in $\mathsf{P}(\zeta)$ die $(p - 1)$-te Potenz eines Primideals, in K_λ also die $t_\lambda^{u_\lambda}$-te Potenz eines Primideals ist. Wegen $(t_\lambda, u_\lambda) = 1$ ist M_λ selbst der Verzweigungskörper für $\mathfrak{p}$ in M_λ, und als solcher relativ-zyklisch über dem Trägheitskörper für $\mathfrak{p}$. Die Diskriminante dieses Trägheitskörpers enthält die Primzahl p nicht, und da auch keine anderen Primzahlen in der Diskriminante vorkommen, ist er gleich P. Somit ist M_λ zyklisch über P. Nun existieren aber in M_λ keine zyklischen Teilkörper von höherem Grade als $t_\lambda^{u_\lambda}$. Daher ist M_λ selbst vom Grade $t_\lambda^{u_\lambda}$ (obiges $v_\lambda = 0$), d. h. $\mathsf{Z}_\lambda = \mathsf{K}_\lambda$. Da hiernach alle $\mathsf{Z}_\lambda \leqq \mathsf{P}(\zeta)$ sind, folgt $\mathsf{Z} \leqq \mathsf{P}(\zeta)$, und dann wegen der Körpergrade $\mathsf{Z} = \mathsf{P}(\zeta)$, w. z. b. w.

C. Da N relativ-zyklisch vom Primzahlgrad p über $\mathsf{Z} = \mathsf{P}(\zeta)$ ist, so ist N/Z ein Kummerscher Körper:

$$\mathsf{N} = \mathsf{Z}(\sqrt[p]{\mu}) = \mathsf{P}(\zeta, \sqrt[p]{\mu}), \quad \mu \text{ in } \mathsf{Z}.$$

---

[8]) Siehe P, S. 140, und U. Wegner, Zur Theorie der affektlosen Gleichungen, Math. Ann. **111** (1935), S. 738, Hilfssatz.

[9]) Siehe dazu P, S. 140 und S. 149, Satz VII.

Dabei gilt als Ausdruck dafür, daß N/P galoissch ist,

$$\mu^T \underset{p}{=} \mu^k \quad \text{mit } (k, p) = 1 \text{ [10]}.$$

Wir betrachten den Führer $\mathfrak{f}_{N/Z}$ von N/Z; wir brauchen hier nur die durch den Zusammenhang mit der Relativdiskriminante von N/Z,

$$\vartheta_{N/Z} = \mathfrak{f}_{N/Z}^{p-1},$$

gegebene Bedeutung dieses Führers, nicht auch seine klassenkörpertheoretische Bedeutung. Aus der oben bereits gegebenen Bestimmung der Beiträge zu $\vartheta_{K/P}$ ergibt sich, daß entsprechend den drei Fällen α), β), γ), also entsprechend den drei Typen von $\vartheta_{K/P}$:

$$\vartheta_{K/P} = p^{p-2}\begin{Bmatrix} p^0 & a_0^{p-1} \\ p^2 & a_0^{p-1} \\ p^{p+1} & a_0^{p-1} \end{Bmatrix},$$

für $\mathfrak{f}_{N/Z}$ die folgenden drei Typen vorliegen [11]:

$$\mathfrak{f}_{N/Z} = \begin{Bmatrix} \mathfrak{p}^0 & (a_0) \\ \mathfrak{p}^2 & (a_0) \\ \mathfrak{p}^{p+1} & (a_0) \end{Bmatrix}, \qquad \text{wo } (p) = \mathfrak{p}^{p-1} \text{ in Z}.$$

Diese drei Typen haben wir jetzt näher zu diskutieren.

α) $\mathfrak{f}_{N/Z} = (a_0)$.

p_ν sei eine in a_0 vorkommende Primzahl und zuerst $p_\nu^{f_\nu} \equiv 1 \bmod. p$ mit $f_\nu e_\nu = p-1$. Dann erzeugt T^{e_ν} die Zerlegungsgruppe eines Primteilers $\mathfrak{q}$ von p_ν in Z, es ist also $\mathfrak{q}^{T^{e_\nu}} = \mathfrak{q}$. Ist dementsprechend $\mathfrak{q}^{g(T)}$ mit $g(T)$ vom Grade $\leqq e_\nu - 1$ der Beitrag von p_ν zu μ, so folgt aus $\mu^T \underset{p}{=} \mu^k$:

$$T\,g(T) \equiv k\,g(T) \bmod. (p, T^{e_\nu} - 1)$$

und daraus durch e_ν-malige Iteration

$$g(T) \equiv k^{e_\nu} g(T) \bmod. p.$$

Weil $g(T) \not\equiv 0 \bmod. p$ ist, wenn p_ν in a_0 vorkommt, ergibt sich also weiter

$$k^{e_\nu} \equiv 1 \bmod. p.$$

Daraus folgt:

Ist $a_0 = p_1 \cdots p_n$ mit $n \geqq 1$ und sind die zu den p_ν gehörigen e_ν untereinander teilerfremd, so ist $k \equiv 1 \bmod. p$, also

$$\mu^T \underset{p}{=} \mu.$$

β) $\mathfrak{f}_{N/Z} = \mathfrak{p}^2(a_0)$.

Hier kann ohne eine Zusatzvoraussetzung auf $k \equiv 1 \bmod. p$, also $\mu^T \underset{p}{=} \mu$ ge-

---

[10]) Wegen der Definition von T siehe S. 2. — Unter μ^T ist die Anwendung von T auf μ verstanden. — T stellt sich als Substitution von Z in der Form $\zeta^T = \zeta^g$ dar, wo g eine Primitivwurzel mod. p ist, die nicht notwendig mit der Primitivwurzel r in der Relation $ST = TS^r$ zusammenfällt (siehe dazu die Ausführungen im letzten Teil dieser Arbeit). — Mit $\underset{p}{=}$ wird die Gleichheit bis auf p-te Zahlpotenzen in Z bezeichnet; entsprechend ist nachher $\underset{p}{\equiv}$ verstanden.

[11]) Ohne die obigen Überlegungen heranzuziehen, kann das auch aus $\vartheta_{Z/P} = p^{p-2}$ und der Diskriminantenformel entnommen werden, die sich ohne weiteres durch Elimination von $\vartheta_{N/P}$ aus den beiden oben auf S. 3 angeführten Diskriminantenformeln ergibt; man beachte dabei die Invarianz des Ideals $\vartheta_{N/Z}$ bei den Substitutionen der Galoisgruppe von Z/P. Siehe dazu auch [1]), S. 183, sowie P, S. 149, Satz VII.

schlossen werden. Es gilt hier nämlich [12])

$$\mu \underset{p}{\equiv} 1 \bmod. p, \qquad \mu \underset{p}{\not\equiv} 1 \bmod. p\mathfrak{p},$$

also

$$\mu \underset{p}{\equiv} 1 + cp \bmod. p\mathfrak{p} \quad \text{mit rationalem } c \not\equiv 0 \bmod. p.$$

Dann ist auch

$$\mu^T \underset{p}{\equiv} 1 + cp \bmod. p\mathfrak{p},$$

während

$$\mu^k \underset{p}{\equiv} (1 + cp)^k \equiv 1 + kcp \bmod. p\mathfrak{p}$$

ist. Aus $\mu^T \underset{p}{=} \mu^k$ folgt also hier

$$kc \equiv c \bmod. p,$$

wegen $c \not\equiv 0 \bmod. p$ also

$$k \equiv 1 \bmod. p.$$

γ) $\mathfrak{f}_{N/Z} = \mathfrak{p}^{p+1}(a_0)$.

Auch hier kann ohne eine Zusatzvoraussetzung auf $k \equiv 1 \bmod. p$, also $\mu^T \underset{p}{=} \mu$ geschlossen werden. Es gilt hier nämlich [12])

$$\mu \underset{p}{\equiv} \pi^\nu \bmod. \mathfrak{p}^0 \quad \text{mit } \nu \not\equiv 0 \bmod. p,$$

wo $\pi = 1 - \zeta$ das Primelement zu $\mathfrak{p}$ in Z ist. Dann ist auch

$$\mu^T \underset{p}{\equiv} \pi^\nu \bmod. \mathfrak{p}^0,$$

da $\pi^T \underset{p}{\equiv} \pi \bmod. \mathfrak{p}^0$ (sogar mod. $\mathfrak{p}^1$) ist, während

$$\mu^k \underset{p}{\equiv} \pi^{k\nu} \bmod. \mathfrak{p}^0$$

ist. Aus $\mu^T \underset{p}{=} \mu^k$ folgt also hier

$$k\nu \equiv \nu \bmod. p,$$

wegen $\nu \not\equiv 0 \bmod. p$ also

$$k \equiv 1 \bmod. p \text{ [13])}.$$

Aus der damit in den drei Fällen α), β), γ) bestätigten Tatsache

$$\mu^T \underset{p}{=} \mu$$

folgt

$$N(\mu) = \mu^{1+T+\cdots+T^{p-2}} \underset{p}{=} \mu^{p-1} \underset{p}{=} \mu^{-1}.$$

Daher ist

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

mit rationalem $a = N(\mu)$, d. h. der Teilkörper p-ten Grades von N ist von der binomischen Form

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

Damit ist der eingangs ausgesprochene Satz bewiesen.

---

[12]) Siehe H. Hasse, Bericht Ia, § 11.

[13]) Den Beweis für die Fälle β) und γ) stellte mir liebenswürdigerweise Herr Hasse zur Verfügung, wie schon in der Einleitung erwähnt wurde.

Zum Schluß soll noch gezeigt werden, daß

1. auflösbare Körper K vom Grade p über P existieren, deren Diskriminanten die im Satz im ersten Falle angegebene Gestalt haben, die aber nicht binomisch sind,

2. die im ersten Falle des Satzes gemachte Zusatzvoraussetzung über die Teilerfremdheit der Zahlen e_ν nicht auch notwendig für die Gültigkeit des Satzes ist,

3. die Zahl k, die als Exponent von μ bei Anwendung der Substitution T auftritt ($\mu^T \underset{p}{=} \mu^k$), eine einfache Bedeutung bei der Darstellung der Galoisschen Gruppe von N als Permutationsgruppe der Konjugierten des Teilkörpers p-ten Grades K hat.

1. Damit ein Kummerscher Körper $\mathsf{N} = \mathsf{Z}(\sqrt[p]{\mu}) = \mathsf{P}(\zeta, \sqrt[p]{\mu})$ über $\mathsf{Z} = \mathsf{P}(\zeta)$ ein Normalkörper über P mit der vollen linearen Gruppe als Galoisscher Gruppe und mit einem Führer $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}} = a_0$ (erster der obigen drei Fälle) ist, sind insgesamt folgende Bedingungen notwendig und hinreichend:

a) $\mu^T \underset{p}{=} \mu^k$ mit $(k, p) = 1$; dies ist notwendig und hinreichend dafür, daß N/P galoissch ist.

b) gk^{-1} ist mod. p von der Ordnung $p - 1$, wo g die aus $\zeta^T = \zeta^g$ bestimmte Primitivwurzel mod. p ist; dies ist notwendig und hinreichend dafür, daß N/P die volle lineare Gruppe als Galoissche Gruppe hat.

c) $\mu \underset{p}{\equiv} 1$ mod. $p\mathfrak{p}$, wo $(p) = \mathfrak{p}^p$ in Z; dies ist notwendig und hinreichend dafür, daß $\mathfrak{p}$ nicht in $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}}$ vorkommt.

d) μ enthält nur Primteiler der $p_\nu \mid a_0$ zu durch p unteilbaren Exponenten, und für jedes p_ν wirklich mindestens einen solchen; dies ist notwendig und hinreichend dafür, daß $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}} = a_0$ ist.

Ist der in a) auftretende Exponent $k \equiv 1$ mod. p, so ist der in N enthaltene Teilkörper p-ten Grades K nach dem Schluß unseres obigen Beweises binomisch (und zwar fällt er unter den ersten Fall unseres Satzes, wegen $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}} = a_0$). Ist umgekehrt $\mathsf{K} = \mathsf{P}(\sqrt[p]{a})$ binomisch, so hat man

$$\mu \underset{p}{=} a^\varkappa \quad \text{mit } (\varkappa, p) = 1$$

und daher

$$\mu^T \underset{p}{=} \mu,$$

d. h. $k \equiv 1$ mod. p. Wir haben also in

e) $k \not\equiv 1$ mod. p

die notwendige und hinreichende Bedingung dafür, daß für einen Kummerschen Körper N mit den Eigenschaften a)—d) der Teilkörper p-ten Grades K nicht binomisch ist.

Ich gebe zunächst eine spezielle Realisierung der Bedingungen a)—e). Es sei $p = 5$, also etwa $g = 2$, $\zeta^T = \zeta^2$. Dann nehme ich

$$\mu = \alpha^{1+4T+T^2+4T^3} \quad \text{mit } \alpha = 5\zeta - 4,$$

also ausführlicher

$$\mu = (5\zeta - 4)\ (5\zeta^2 - 4)^4\ (5\zeta^4 - 4)\ (5\zeta^3 - 4)^4.$$

Ersichtlich ist

$$\mu^T \underset{p}{=} \mu^4,$$

d. h. a) und e) sind mit $k \equiv 4$ mod. 5 erfüllt. Da $gk^{-1} \equiv 3$ mod. 5 ist, ist auch b) erfüllt.

Ferner ist ersichtlich

$$\alpha = 5\zeta - 4 \equiv 5 \cdot 1 - 4 \equiv 1 \bmod. 5\mathfrak{p}$$

und dann auch $\alpha^{T^\nu} \equiv 1 \bmod. 5\mathfrak{p}$, also

$$\mu \equiv 1 \bmod. 5\mathfrak{p},$$

d. h. c) ist erfüllt. Schließlich hat man die Zerlegung

$$\alpha = 5\zeta - 4 = (\zeta^3 + 2\zeta)\,(4 + 2\zeta + \zeta^3)$$

mit

$$N(\zeta^3 + 2\zeta) = 11, \quad N(4 + 2\zeta + \zeta^3) = 191,$$

so daß also (α) Produkt zweier Primhauptideale ersten Grades

$$\mathfrak{p}_1 = (\zeta^3 + 2\zeta), \quad \mathfrak{p}_2 = (4 + 2\zeta + \zeta^3)$$

mit

$$N(\mathfrak{p}_1) = 11, \quad N(\mathfrak{p}_2) = 191$$

ist, und daher

$$(\mu) = (\mathfrak{p}_1\mathfrak{p}_2)^{1+4T+T^2+4T^3}.$$

Daher ist d) mit $p_1 = 11$, $p_2 = 191$ erfüllt.

Herr Hasse teilte mir freundlicherweise mit, wie man die obigen Bedingungen a)—e) in allgemeinerer Weise realisieren kann. Sei p eine solche Primzahl, daß der p-te Kreisteilungskörper Z eine genau durch p^1 teilbare Klassenanzahl hat, während jeder Teilkörper von Z eine durch p unteilbare Klassenzahl hat (z. B. $p = 59$). Dann hat der p-Klassenkörper N von Z die Eigenschaften a)—d). Denn N ist seiner invarianten Definition nach galoissch über P, ferner unter den gemachten Annahmen zyklisch vom Grade p über Z und besitzt keinen Teilkörper, der über einem Teilkörper von Z zyklisch vom Grade p ist, d. h. N hat die volle lineare Gruppe als Galoissche Gruppe, und schließlich ist N unverzweigt über Z, also $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}} = 1$. Wegen $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}} = 1$ hat der in N enthaltene Teilkörper p-ten Grades K die Diskriminante $\vartheta_{\mathsf{K}/\mathsf{P}} = \vartheta_{\mathsf{N}/\mathsf{Z}} = p^{p-2}$, ist also nach dem auf S. 2 Gesagten sicher nicht binomisch.

Ich will noch zeigen, daß sich die Bedingungen a)—e) auch mit $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}} \neq 1$ realisieren lassen, sogar mit beliebig vielen Primteilern p_ν von $\mathfrak{f}_{\mathsf{N}/\mathsf{Z}}$. Sei dazu $k \not\equiv 1 \bmod. p$ vorgegeben und e ein Exponent mit

$$k^e \equiv 1 \bmod. p, \quad ef = p - 1$$

(nicht notwendig der genaue Exponent von $k \bmod. p$). Ferner seien die p_ν irgendwelche Primzahlen ($\neq 2$), die mod. p vom genauen Exponenten f sind. Sei dann Z_e der Teilkörper e-ten Grades von Z, also der Zerlegungskörper für die Primzahlen p_ν im Körper Z, und sei jeweils $\mathfrak{p}_\nu$ ein Primteiler von p_ν in Z, der dann schon Primideal (ersten Grades) in Z_e ist. Wir wählen dann Zahlen γ_ν in Z_e mit den Eigenschaften:

γ_ν ist genau durch $\mathfrak{p}_\nu^1$ teilbar,

γ_ν ist prim zu den Konjugierten $\mathfrak{p}_\nu^T, \ldots, \mathfrak{p}_\nu^{T^{e-1}}$,

γ_ν ist prim zu den $p_{\nu'}\,(\nu' \neq \nu)$,

$\gamma_\nu \underset{p}{\equiv} 1 \bmod. p\mathfrak{p}$.

Solche γ_ν existieren bekanntlich stets. Damit bilden wir die symbolischen Potenzen

$$\eta_\nu \underset{p}{=} \gamma_\nu^{1+k^{-1}T+\cdots+k^{-(e-1)}T^{e-1}},$$

wo im Exponenten mod. p gerechnet sei, und damit das Produkt

$$\mu \underset{p}{=} \prod_{\nu} \eta_{\nu}.$$

Dieses μ hat dann, wie leicht aus der Konstruktion ersichtlich ist, die Eigenschaften a)—e), mit durch die gewählten p_ν teilbarem $\mathfrak{f}_{\mathsf{N/Z}}$.

2. Ich zeige, daß die im ersten der drei Fälle des Satzes gemachte Annahme, daß die Zahlen e_ν teilerfremd sind, nicht notwendig dafür ist, daß zu vorgegebener Diskriminante $\vartheta_{\mathsf{K/P}} = p^{p-2} a_0^{p-1}$ nur binomische Körper existieren, indem ich ein Beispiel mit $a_0 = p_1$, $e_1 = 2$ konstruiere, in dem zur Diskriminante $\vartheta_{\mathsf{K/P}} = p^{p-2} p_1^{p-1}$ nur der binomische Körper $\mathsf{K} = \mathsf{P}(\sqrt[p]{p_1})$ gehört.

Sei dazu $p = 7$, also etwa $g = 3$, und ferner $p_1 = 67$, also $f_1 = 3$, $e_1 = 2$, wegen $67^3 \equiv 1 \bmod. 7$. Der binomische Körper $\mathsf{K} = \mathsf{P}(\sqrt[7]{67})$ fällt wegen $67 \equiv 18 \bmod. 7^2$ und $18^6 \equiv 1 \bmod. 7^2$ (Jacobi!), also $67^6 \equiv 1 \bmod. 7^2$ unter den ersten Fall des Satzes, hat also die Diskriminante $\vartheta_{\mathsf{K/P}} = 7^5 \cdot 67^6$. Andrerseits ergeben die obigen Bedingungen b) und e) für einen nicht binomischen auflösbaren Körper 7-ten Grades dieser Diskriminante notwendig $k \equiv 2 \bmod. 7$, so daß also $k^{e_1} \equiv 2^2 \not\equiv 1 \bmod. 7$ wäre, während doch im Beweis auf S. 8 allgemein $k^{e_\nu} \equiv 1 \bmod. p$ festgestellt wurde. Daher gibt es außer $\mathsf{K} = \mathsf{P}(\sqrt[7]{67})$ keinen auflösbaren Körper 7-ten Grades mit der Diskriminante $7^5 \cdot 67^6$.

3. Ich will noch eine einfache gruppentheoretische Bestimmung der Zahl k geben, die einem über P galoisschen Körper $\mathsf{N} = \mathsf{P}(\zeta, \sqrt[p]{\mu})$ mit der vollen linearen Gruppe als Galoisscher Gruppe $\mathfrak{G}$ durch die Relation $\mu^T \underset{p}{=} \mu^k$ invariant zugeordnet ist. $\mathfrak{G}$ wird erzeugt durch

$$S = \begin{pmatrix} \zeta & : & \zeta \\ \sqrt[p]{\mu} & : & \zeta\sqrt[p]{\mu} \end{pmatrix} \quad \text{und} \quad T = \begin{pmatrix} \zeta & : & \zeta \\ \sqrt[p]{\mu} & : & \sqrt[p]{\mu^k \gamma} \end{pmatrix},$$

mit den Relationen

$$S^p = T^{p-1} = E \quad \text{und} \quad ST = TS^r.$$

Dabei sind g und r Primitivwurzeln mod. p, und γ ist die in der Relation $\mu^T = \mu^k \gamma^p$ auftretende Zahl aus Z. Durch Anwendung von $ST = TS^r$ auf die Zahl $\sqrt[p]{\mu}$ ergibt sich

$$g \equiv kr \bmod. p,$$

also insbesondere die oben angeführte Bedingung b), daß gk^{-1} mod. p von der Ordnung $p - 1$ ist. Sei nun der Teilkörper p-ten Grades K unter seinen Konjugierten als der Invariantenkörper von T festgelegt, ferner sei $\mathsf{K} = \mathsf{P}(\alpha)$ irgendeine Erzeugung von K, und seien die Konjugierten $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ von α gruppentheoretisch durch $\alpha_\nu = \alpha^{S^\nu}$ (ν mod. p) festgelegt. Dann stellt sich $\mathfrak{G}$ als die volle lineare Permutationsgruppe der p Konjugierten α_ν dar, und zwar

$$S \text{ als der } p\text{-gliedrige Zyklus } \begin{pmatrix} \alpha_\nu \\ \alpha_{\nu+1} \end{pmatrix},$$

$$T \text{ als der } (p-1)\text{-gliedrige Zyklus } \begin{pmatrix} \alpha_\nu \\ \alpha_{\nu r} \end{pmatrix}.$$

Geht man von $\mathsf{K} = \mathsf{P}(\alpha)$ aus, und sind $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ die Konjugierten zu α in solcher Reihenfolge, daß die eben genannten beiden zyklischen Permutationen die

Galoissche Gruppe $\mathfrak{G}$ erzeugen, so bestimmt sich die zu der hierbei willkürlich gewählten Primitivwurzel r im Sinne des Vorhergehenden gehörige Primitivwurzel g auf Grund der Tatsache

$$\mathsf{N} = \mathsf{P}(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) \geqq \mathsf{Z} = \mathsf{P}(\zeta),$$

indem man eine rationale Darstellung von ζ durch die α_ν aufsucht:

$$f(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}) = \zeta^g,$$

und darin die Permutation $\begin{pmatrix}\alpha_\nu \\ \alpha_{\nu r}\end{pmatrix}$ anwendet:

$$f(\alpha_0, \alpha_r, \ldots, \alpha_{(p-1)r}) = \zeta^g.$$

Daraus bestimmt sich dann die Invariante k gemäß der obigen Relation

$$g \equiv kr \text{ mod. } p.$$

Eingegangen 23. April 1936.