Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 55 (1980)

Artikel: Über schwache quadratische Zerlegungssätze.
Autor: Klingen, Norbert
DOI: https://doi.org/10.5169/seals-42401

Comment. Math. Helvetici **55** (1980) 645–651 Birkhäuser Verlag, Basel

Über schwache quadratische Zerlegungsgesetze

Norbert Klingen

Das Zerlegungsverhalten von Primidealen in abelschen Zahlkörpererweiterungen $L \mid k$ ist aufgrund des Zerlegungsgesetzes der Klassenkörpertheorie bekannt: Bis auf endlich viele Ausnahmen ist der Restklassengrad eines Primideals $\mathfrak{p}$ von k als Ordnung von $\mathfrak{p}$ modulo der L zugeordneten Kongruenzgruppe (nach einem geeigneten Erklärungsmodul) gegeben ("starkes Zerlegungsgesetz"). Insbesondere sind die Primideale von k, die in L Primteiler ersten Grades haben, gerade die Primideale in dieser Kongruenzuntergruppe ("schwaches Zerlegungsgesetz"). Das schwache Zerlegungsgesetz impliziert das starke und charakterisiert bereits die abelsche Körpererweiterung. Während allerdings durch das starke Zerlegungsgesetz die Körpererweiterung $L \mid k$ unter *allen* Erweiterungen von k eindeutig bestimmt ist, legt das schwache Zerlegungsgesetz L nur unter allen *galoisschen* Erweiterungen eindeutig fest.

Erstmalig hat V. Schulze [9] nicht-abelsche Zahlkörper angegeben, die ein schwaches abelsches Zerlegungsgesetz haben, d.h. in denen genau die Primzahlen einen Primteiler ersten Grades haben, die in einer bestimmten Kongruenzidealgruppe liegen. Die Schulze'schen Beispiele sind quadratische Erweiterungen abelscher Zahlkörper vom Grade 3, 5, 6 mit demselben schwachen Zerlegungsgesetz wie diese abelschen Körper. Resultate von W. Jehne ([4], §9) zeigen, daß dies sehr spezielle Fälle einer allgemeinen Tatsache sind: Zu allen abelschen Körpererweiterungen $L \mid k$, die keine 2-Erweiterungen sind, gibt es unendlich viele quadratische Erweiterungen K von L mit demselben schwachen Zerlegungsverhalten bzgl. k wie L. Für 2-Erweiterungen kann es solche quadratischen Erweiterungen nicht geben (Klingen [5], Satz 9). Hat die abelsche 2-Erweiterung $L \mid k$ jedoch mindestens den Exponenten 8, so gibt es unendlich viele kubisch-zyklische Erweiterungen K von L mit gleichem schwachem Zerlegungsgesetz wie L (Jehne [4], Satz 3').

Diese Ergebnisse zeigen, daß im allgemeinen ein abelscher Zahlkörper in der Gesamtheit aller Zahlkörper nicht durch sein schwaches Zerlegungsgesetz charakterisiert ist. Nach den oben erwähnten Ergebnissen ist dies allenfalls für abelsche 2-Erweiterungen vom Exponenten 2 oder 4 denkbar. Daß dies für quadratische Erweiterungskörper tatsächlich zutreffen könnte, lassen neben Resultaten von W. Jehne ([4], §6) die nachfolgenden Ergebnisse vermuten.

Sei $K \mid k$ ein minimales Gegenbeispiel zu dieser Vermutung, d.h. eine nichtquadratische Erweiterung mit schwachem quadratischem Zerlegungsgesetz (siehe Def.). Dann ist dadurch eine nicht-abelsche einfache Gruppe bestimmt, der sog. "simple type" von $K \mid k$ (Jehne [4]). Es wird gezeigt, daß als simple type die klassischen Gruppen $\mathrm{PSL}(2, p^\nu)$ (p beliebige Primzahl, $\nu \in \mathbf{N}$) nicht auftreten können; dies erweitert ein Resultat von Jehne. Darüber hinaus wird gezeigt, daß auch keine der einfachen Gruppen einer Ordnung unter 10^6 "simple type" einer Körpererweiterung $K \mid k$ sein kann.

Zusammen mit der Tatsache, daß auch die alternierenden Gruppen $\mathfrak{A}_n$ kein "simple type" sein können (Klingen [6], Satz 3), ergeben sich hieraus Konsequenzen für den Körpergrad $(K:k)$ eines Körpers K mit schwachem quadratischem Zerlegungsgesetz. So folgt unter anderem: Ist $K \mid k$ eine Zahlkörpererweiterung mit schwachem quadratischem Zerlegungsgesetz und $(K:k)<72$, so ist $K \mid k$ bereits eine quadratische Erweiterung.

Bezeichnungen: Es bezeichne im folgenden

k	einen endlich-algebraischen Zahlkörper,
P_k	die Menge der Primideale von k,
$\mathfrak{m}$	einen Zykel (Erklärungsmodul) von k,
$\mathfrak{J}_k^{(\mathfrak{m})}$	die Gruppe der zu $\mathfrak{m}$ primen Ideale von k,
$S_k(\mathfrak{m})$	den Strahl modulo $\mathfrak{m}$ in $\mathfrak{J}_k^{(\mathfrak{m})}$,
$D(K \mid k)$	die Menge der Primideale von k, die im Erweiterungskörper K einen Primteiler ersten Grades haben,
$='$	die Gleichheit (von Mengen) bis auf endlich viele Ausnahmen,
$\exp G$	den Exponenten und
1_G	den Einscharakter einer Gruppe G.

DEFINITION. Eine endliche Zahlkörpererweiterung $K \mid k$ hat ein *schwaches quadratisches Zerlegungsgesetz*, wenn eine Kongruenzuntergruppe $H \subset \mathfrak{J}_k^{(\mathfrak{m})}$ zu einem Zykel $\mathfrak{m}$ von k existiert, so daß H in $\mathfrak{J}_k^{(\mathfrak{m})}$ den Index 2 hat und genau die Primideale von k enthält, die in K einen Primteiler ersten Grades besitzen und $\mathfrak{m}$ nicht teilen.

Hat $K \mid k$ ein schwaches quadratisches Zerlegungsgesetz, so ist die Idealgruppe H mit den oben genannten Eigenschaften eindeutig bestimmt (im Sinne der "Gleichheit" von Idealgruppen, Hasse [2]). Es gilt genauer:

Bemerkung 1. Hat $K \mid k$ ein schwaches quadratisches Zerlegungsgesetz mit Idealgruppe H, so enthält K genau einen über k galoisschen Teilkörper $L \neq k$; dieser ist eine quadratische Erweiterung von k, und zwar der Klassenkörper zu H über k.

Beweis. Der Klassenkörper L zu H ist eine quadratische Erweiterung von k und es gilt nach dem Zerlegungsgesetz der Klassenkörpertheorie

$$D(L \mid k) =' \{\mathfrak{p} \in P_k \mid \mathfrak{p} \in H\}.$$

Nach Voraussetzung ergibt sich daher

$$D(L \mid k) =' D(K \mid k). \tag{1}$$

Mit anderen Worten:

K und L sind über k Kronecker-äquivalent (im Sinne von Jehne [4]). (2)

Nach dem Satz von Bauer [1] folgt aus (1), daß L ein Teilkörper von K ist.

Ist nun $L' \mid k$ galoissch mit $L' \subseteq K$, so hat LL' wegen $L \subseteq LL' \subseteq K$ dasselbe schwache Zerlegungsgesetz wie L und K:

$$D(L \mid k) =' D(LL' \mid k) =' D(K \mid k) \tag{3}$$

Da L und LL' aber galoissche Erweiterungen von k sind, müssen sie nach dem schon erwähnten Satz von Bauer übereinstimmen. Es gilt daher $L' \subseteq L$, also $L' = k$ oder $L' = L$.

Damit ist Bemerkung 1 bewiesen, und die eingangs erwähnte Vermutung besagt nun:

Es ist K gleich dem quadratischen Zahlkörper L, der zur Kongruenzuntergruppe H gehört.

Für die folgenden Untersuchungen sei nun $K \mid k$ ein minimales Gegenbeispiel zu dieser Vermutung, es gelte also

(V) *$K \mid k$ ist eine minimale, nicht quadratische Erweiterung mit schwachem quadratischem Zerlegungsgesetz und L der quadratische Teilkörper* (siehe Bem. 1).

Dann gilt

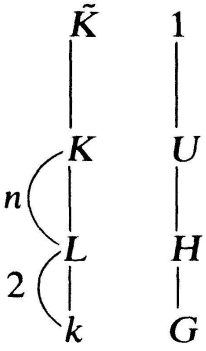
$K \mid L$ ist eine echte Erweiterung ohne Zwischenkörper. (4)

Es gilt sogar schärfer

Bemerkung 2. Unter der Voraussetzung (V) ist L der einzige echte Zwischenkörper der Erweiterung $K \mid k$.

Beweis. Sei $k \subseteq L' \subseteq K$, also $L \subseteq LL' \subseteq K$. Nach (4) folgt $L = LL'$ oder $K = LL'$. $L = LL'$ bedeutet $L = k$ oder $L' = L$. Ist nun $LL' = K$ und wäre $L' \neq K$, so wäre $K \mid L'$ eine quadratische Erweiterung, K besäße also einen nicht-trivialen k-Automorphismus im Widerspruch zu Klingen [5], Satz 7.

Es sei im folgenden $\tilde{K}$ die galoissche Hülle von $K \mid L$. Diese ist dann sogar über k galoissch (Jehne [4], Th. 5).



(B) Mit U, H, G seien die entsprechenden Galoisgruppen von $\tilde{K}$ über K, L, k bezeichnet. Weiter sei N der eindeutig bestimmte minimale Normalteiler von H; dieser ist nicht-abelsch einfach, der sog. "simple type" von $K \mid k$ (Jehne [4]).

Es ist bekannt, daß als simple type nicht auftreten $\mathfrak{A}_n$ (Klingen [6]) und $\mathrm{PSL}(2, p^\nu)$ ($p \neq 2$ Primzahl, $\nu \in \mathbf{N}$, Jehne [4]). Das letztgenannte Resultat wird hier mit einfachen charaktertheoretischen Mitteln bewiesen und erweitert zu

SATZ 1. *Der "simple type" N einer Körpererweiterung $K \mid k$ mit schwachem quadratischem Zerlegungsgesetz kann*

(a) *keine der klassischen Gruppen* $\mathrm{PSL}(2, p^\nu)$ (p *beliebige Primzahl,* $\nu \in \mathbf{N}$) *sein, und*

(b) *keine Ordnung* $\leq 10^6$ *haben.*

Beweis. Sei $n = (K:L)$ und $P: H \to \mathfrak{S}_n$ die Permutationsdarstellung von H bzgl. U, also die natürliche Darstellung als Galoisgruppe einer erzeugenden Gleichung für $K \mid L$.

Die Darstellung P ist nach den gemachten Voraussetzungen treu und primitiv. Da die Körper K und L k-Kroneckeräquivalent sind, folgt aus der gruppentheoretischen Beschreibung dieser Äquivalenz (siehe etwa Jehne [4], §1)

$$H = \bigcup_{\rho \in G} H^\rho = \bigcup_{\rho \in G} U^\rho = \bigcup_{\tau \in H} U^\tau \cup \bigcup_{\tau \in H} U'^\tau, \tag{5}$$

wobei $U' := U^\sigma$ mit $\sigma \in G \backslash H$ gesetzt sei. Wegen der Primitivität von P sind $P \mid N$ und $P' \mid N$ ($P' = P^\sigma = P(\sigma \cdots \sigma^{-1})$) transitive Permutationsdarstellungen von N desselben Grades n, also

$$N = \bigcup_{\tau \in N} (U \cap N)^\tau \cup \bigcup_{\tau \in N} (U' \cap N)^\tau. \tag{6}$$

Wegen $\exp U = \exp H$ ist der Grad $(K:L) = n$ ein Teiler von $\#H/\exp H$. Da N als einziger minimaler Normalteiler von H auch Normalteiler in G ist, sind $U \cap N$

und $U' \cap N$ isomorph, also gilt auch $\exp(U \cap N) = \exp N$ und n teilt $\#N/\exp N$. Für $N = \mathrm{PSL}(2, p^\nu)$ bedeutet dies, daß n ein Teiler von $2p^{\nu-1}$ ist. Nach dem "Satz von Galois" (Huppert [3], Th. 8,28) ist dies nur für $p^\nu = 9$, $n = 6$ möglich, aber $\mathrm{PSL}(2, 9)$ ist als alternierende Gruppe $\mathfrak{A}_6$ kein simple type. Im Falle $p = 2$ benötigt man den "Satz von Galois" nicht, weil dann $K \mid k$ eine 2-Potenzerweiterung wäre, die zu $L \subsetneqq K$ Kronecker-äquivalent wäre, im Widerspruch zu Klingen [5], Satz 9.

Zum Beweis von (b) betrachtet man die Charaktere θ, θ' der transitiven Permutationsdarstellungen $P \mid N$, $P' \mid N$ von N vom Grade n. Diese sind unter $\mathrm{Aut}(N)$ konjugiert und es gilt für jedes $\rho \in N$: $\theta(\rho) > 0$ oder $\theta'(\rho) > 0$ (siehe (6)). Hieraus ergibt sich insbesondere $\theta \neq \theta'$. Damit besitzt N mit $\psi = \theta - 1_N$, $\psi' = \theta' - 1_N$ zwei verschiedene, rationalwertige Charaktere, die den Einscharakter nicht enthalten, unter der Automorphismengruppe $\mathrm{Aut}(N)$ von N konjugiert sind und die Eigenschaft $\psi(\rho) \geq 0$ oder $\psi'(\rho) \geq 0$ für alle $\rho \in N$ haben. Da rationalwertige Charaktere Funktionen der Abteilungen sind, bedeutet $\psi(\rho) \neq \psi'(\rho) = \psi(\sigma\rho\sigma^{-1})$, daß die Konjugationsklassen von ρ und $\sigma\rho\sigma^{-1}$ nicht zur gleichen Abteilung gehören, wohl aber unter $\mathrm{Aut}(N)$ konjugiert sind (also z.B. gleiche Ordnung und Mächtigkeit haben). In den einfachen Gruppen N verschieden von $\mathrm{PSL}(2, p^\nu)$ und $\mathfrak{A}_n$ mit $\#N \leq 10^6$ gibt es solche Konjugationsklassen höchstens in den Gruppen $\mathrm{PSL}(3, 4)$, M_{12}, $\mathrm{U}(3, 5)$, $\mathrm{Sp}(4, 4)$ (McKay [7]). Für diese Gruppen N betragen die Quotienten $\#N/\exp N$ beziehungsweise $2^4 \cdot 3$, $2^3 \cdot 3^2$, $2 \cdot 3 \cdot 5^2$ und $2^6 \cdot 3 \cdot 5$. Da der Grad von ψ durch $1 + \psi(1) = n \mid \#N/\exp N$ beschränkt ist, schließt man sofort, daß $\mathrm{PSL}(3, 4)$, M_{12} und $\mathrm{U}(3, 5)$ keinen rationalwertigen Charakter ψ mit $(\psi, 1_N) = 0$ und diesem Grad besitzen. Für $N = \mathrm{Sp}(4, 4)$ gibt es zwar verschiedene rationalwertige Charaktere ψ mit $(\psi, 1_N) = 0$ und gleichem Grad $n \mid 960$, diese erfüllen aber nicht die übrigen Bedingungen $\psi(\rho) \geq 0$ oder $\psi'(\rho) \geq 0$ für alle $\rho \in N$. Damit ist Satz 1 bewiesen.

Aus Satz 1 folgert man durch Untersuchung primitiver Permutationsgruppen den folgenden

SATZ 2. *Ist $K \mid k$ eine Zahlkörpererweiterung mit schwachem quadratischem Zerlegungsgesetz und $(K : k) < 72$, so ist $K \mid k$ quadratisch.*

Beweis. Unter den Voraussetzungen (V) und mit den Bezeichnungen (B) ist H eine primitive Permutationsgruppe vom Grade $n = \frac{1}{2}(K : k)$, deren minimaler Normalteiler N keine alternierende Gruppe $\mathfrak{A}_m$ ist und den in Satz 1 genannten Einschränkungen unterliegt. Aufgrund der Kenntnis aller primitiven Permutationsgruppen vom Grade ≤ 20 (Sims [10]) ergibt sich hieraus unmittelbar: $(K : k) > 40$. Mit einer umfassenden Übersicht über alle primitiven Permutationsgruppen läßt sich diese Schranke leicht vergrößern. Man kann aber auch

zunächst die möglichen Grade n stark einschränken:

LEMMA.[1] *Unter den Voraussetzungen* (V) *und mit den Bezeichnungen* (B) *gilt für* $n=(K:L)=\frac{1}{2}(K:k)$, p *ein Primteiler von* n:

$$n=mp^{\nu} \Rightarrow p<2m$$
$$n=mp \Rightarrow p<m.$$

Beweis. Sei $n=mp^{\nu}$ und H_p eine p-Sylowgruppe in H, t die Zahl der H_p-Bahnen in der Permutationsdarstellung $\hat{P}$ von G bzgl. U vom Grade $(G:U)=2mp^{\nu}$. Da die H_p-Bahnen mindestens die Mächtigkeit p^{ν} haben (Wielandt [11], 3.4), ist $t\leq 2m$. Andererseits gilt nach (5)

$$H_p=\bigcup_{i=1}^{t}\bigcup_{\rho\in H_p} U_i^{\rho}$$

mit U_i Fixgruppe in H_p eines Elementes der i-ten Bahn $(i=1,\ldots,t)$. In der p-Gruppe H_p erzeugt U_i einen echten Normalteiler Q_i, also folgt

$$\#H_p<t\cdot\frac{\#H_p}{p},$$

d.h.

$$p<t\leq 2m.$$

Sei nun $n=mp$ und $p\geq m$, d.h. $p^2\geq n$. Wegen $\exp U=\exp H$ und $(H:U)=n$ gilt $p^2\mid \#H$ und U enthält ein Element σ mit $\operatorname{ord}\sigma=p$. Es ist dann $P(\sigma)$ eine Permutation vom Grad $d<n\leq p^2$. Nach einem Satz von Praeger [9] folgt daraus $H\supseteq \mathfrak{A}_n$ oder $n=p^2$. Beides ist aber unmöglich; letzteres nach dem bereits bewiesenen Teil des Lemmas, das erstere, da $\mathfrak{A}_n$ kein "simple type" ist.

Von den Graden $n<36$ verbleiben also nur 24 und 30. Durch Diskussion der Zyklentypen von Elementen von Primzahlordnung in H folgert man mit Resultaten von Jordan, Manning und Weiss (vgl. Wielandt [11], §§13, 17), daß H 2-fach transitiv, U also eine Permutationsgruppe von Primzahlgrad 23 bzw. 29 ist. Ist U auflösbar, so folgt $\#H<10^6$ im Widerspruch zu Satz 1. Im nichtauflösbaren Fall verbleibt nur $n=24$, $U=M_{23}$, also $H=M_{24}$ (Neumann [8]). Aber diese

[1] Ich danke dem Referenten für dieses Lemma, das die ursprünglichen Resultate verbessert.

Mathieugruppe besitzt keinen äußeren Automorphismus im Widerspruch zum Beweis von Satz 1(b).

LITERATUR

[1] BAUER, M., *Zur Theorie der algebraischen Zahlkörper.* Math. Ann. 77 (1916), 353–356.
[2] HASSE, H., *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper* ("*Zahlbericht*"). Würzburg 1965.
[3] HUPPERT, B., *Endliche Gruppen I.* Springer: Berlin-Heidelberg-New York 1967.
[4] JEHNE, W., *Kronecker classes of algebraic number fields.* J. Number Theory *9* (1977), 279–320.
[5] KLINGEN, N., *Zahlkörper mit gleicher Primzerlegung.* J. reine angew. Math. *299/300* (1978), 342–384.
[6] ——, *Atomare Kroneckerklassen mit speziellen Galoisgruppen.* Abh. Math. Sem. Hamburg *48* (1979), 42–53.
[7] MCKAY, J., *The non-abelian simple groups G, $|G|<10^6$-Character tables,* Comm. Alg. *7* (1979), 1407–1445.
[8] NEUMANN, PETER M. *Permutationsgruppen von Primzahlgrad und verwandte Themen.* Vorlesungsausarbeitung Univ. Gießen 1977.
[9] PRAEGER, C. E. *Primitive permutation groups containing an element of order p of small degree, p a prime.* J. Alg. *34* (1975), 540–546.
[10] SCHULZE, V., *Die Verteilung der Primteiler von Polynomen auf Restklassen I, II.* J. reine angew. Math. *280* (1976), 122–133; *281* (1976), 126–148.
[11] SIMS, C. C., *Computational methods in the study of permutation groups.* In: Computational problems in abstract algebra. (Proc. Conf. Oxford 1967), Oxford 1970, p. 169–183.
[12] WIELANDT, H., *Finite permutation groups.* Academic Press: New York-London 1964.

Mathematisches Institut
Wegertal 86–90
D-5000 Köln

Eingegangen den 19 Juni 1980