ACTA ARITHMETICA
XXXVI (1980)

Über Radikalerweiterungen *

von

FRANZ HALTER-KOCH (Essen)

1. Sei L/K eine endlich-separable Körpererweiterung, $n \in \boldsymbol{N}$ teilerfremd zur Charakteristik von K und $C \subseteq L^\times$ eine Untergruppe mit $L = K(C)$ und $C^n \subseteq K$; da es im folgenden stets auf die Gruppe $\langle K^\times, C\rangle$(1) und nicht auf C ankommt, setze ich $K^\times \subseteq C$ voraus.

Enthält K die n-ten Einheitswurzeln, so ist L/K eine Kummererweiterung, und es gilt:

$$[L:K] = (C:K^\times) = (C^n : K^{\times n}).$$

Enthält K die n-ten Einheitswurzeln nicht, so gilt im allgemeinen keine der obigen Gleichungen; M. Kneser [2] und A. Schinzel [4] gaben notwendige und hinreichende Bedingungen für das Bestehen des ersten Gleichheitszeichens an. In der vorliegenden Arbeit untersuche ich den Zusammenhang zwischen $[L:K]$ und $(C^n : K^{\times n})$; ich zeige, daß $(C^n : K^{\times n})$ stets ein Teiler von $[L:K]$ ist (Satz 2), gebe notwendige und hinreichende Bedingungen für Gleichheit an (Satz 5) und untersuche die Struktur einiger speziellen Radikalerweiterungen genauer (Sätze 3 und 4).

Für $q \in \boldsymbol{N}$ sei W_q die Gruppe der q-ten Einheitswurzeln (in einer festen algebraischen Hülle) und $\zeta_q \in W_q$ eine primitive q-te Einheitswurzel; die Normierung sei so, daß

$$\zeta_q = \zeta_{q'}^{q'/q} \quad \text{für} \quad q \mid q'.$$

Nach [2] gilt:

SATZ 1. *Sei L/K eine endlich-separable Körpererweiterung, $n \in \boldsymbol{N}$ teilerfremd zur Charakteristik von K und $K^\times \subseteq C \subseteq L^\times$ eine Untergruppe*

* Diese Arbeit entstand im Rahmen eines durch das Land Nordrhein-Westfalen geförderten Forschungsvorhabens. Herrn E. Becker (Köln) danke ich für viele interessante Diskussionen und wertvolle Hinweise zu dieser Arbeit.

(1) $\langle M\rangle$ ist die von M erzeugte Gruppe.

mit $L = K(C)$ und $C^n \subset K$. Dann ist

$$[L:K] \leqslant (C:K^\times),$$

und das Gleichheitszeichen gilt genau dann, wenn die beiden folgenden Bedingungen erfüllt sind:

A. *Für jede Primzahl p ist $W_p \cap C \subset K$.*

B. *Ist $1+\zeta_4 \in C$, so ist $\zeta_4 \in K$.*

SATZ 2. *Sei L/K eine endlich-separable Körpererweiterung, $n \in \mathbf{N}$ teilerfremd zur Charakteristik von K und $K^\times \subseteq C \subseteq L^\times$ eine Untergruppe mit $C^n \subset K$; dann ist*

$$(C^n : K^{\times n}) \mid [L:K].$$

Insbesondere sind die Gruppen $C/K^\times$ und $C^n/K^{\times n}$ endlich.

2. Für den Beweis von Satz 2 benötige ich eine Reihe von Hilfssätzen; die Voraussetzungen seien stets dieselben wie in Satz 2. Es sei

$$C_n(L/K) = \{x \in L^\times \mid x^n \in K\},$$

also stets $K^\times \subseteq C \subseteq C_n(L/K)$.

LEMMA 1. *Sei $x \in C_n(L/K) \setminus K$ und $m \mid n$ minimal mit $x^m \in K$. Dann gilt:*

(a) *Für jeden Primteiler $q \mid m$ mit $W_q \subset K$ ist $x^m \notin K^q$.*

(b) *Falls $x^m \notin K^q$ für alle Primzahlen $q \mid m$, so gilt entweder*

$$[K(x):K] = m$$

oder

$$4 \mid m, \quad \zeta_4 \notin K \quad \text{und} \quad x^{m/4} = (1 \pm \zeta_4) z \quad \text{mit } z \in K.$$

Beweis. (a) Wäre $x^m = z^q$ mit $z \in K$, $q \mid m$ und $W_q \subset K$, so wäre $x^{m/q} = \zeta z$ mit $\zeta \in W_q \subset K$ im Widerspruch zur Minimalität von m.

(b) Ist $[K(x):K] < m$, so ist entweder $x^m \in K^q$ für eine Primzahl $q \mid m$ oder $4 \mid m$ und $x^m \in -4K^4$ ([4], Chap, VIII, Theorem 16); im letzteren Falle folgt $x^{m/4} \in (1 \pm \zeta_4) \cdot K^\times$, und wegen der Minimalität von m ist $\zeta_4 \notin K$.

LEMMA 2. *Seien p und q Primzahlen, $p \neq q$, $a \geqslant 1$, $n = q^a$ und $[L:K] = p$. Dann gilt:*

$$C_{q^a}(L/K) = \langle K^\times, W_{q^a} \cap L \rangle,$$

also insbesondere $C_{q^a}(L/K)^{q^a} = K^{\times q^a}$.

Beweis. Trivialerweise ist $W_{q^a} \cap L \subseteq C_{q^a}(L/K)$. Sei nun $x \in C_{q^a}(L/K) \setminus K$ und $c \geqslant 1$ minimal mit $x^{q^c} \in K$. Wäre $x^{q^c} \notin K^q$, so wäre nach Lemma 1 entweder $[K(x):K] = q^c$ oder $q = 2$ und $K \subsetneq K(\zeta_4) \subseteq L$, also in jedem Falle $q \mid [K(x):K] \mid p$, ein Widerspruch. Daher ist $x^{q^c} \in K^q$, und es genügt, $x^{q^c} \in K^{q^c}$ nachzuweisen, denn dann ist $x \in (W_{q^c} \cap L) \cdot K^\times \subseteq (W_{q^a} \cap L) \cdot K^\times$.

Ich nehme an, es sei $x^{q^c} \notin K^{q^c}$ und $1 \leqslant l < c$ maximal mit $x^{q^c} \in K^{q^l}$; dann ist $x^{q^c} = z^{q^l}$ mit $z \in K \setminus K^q$, also $x^{q^{c-l}} = \zeta \cdot z$ mit einer primitiven q^l-ten Einheitswurzel ζ. Wegen der Minimalität von c ist $\zeta \notin K$, also $L = K(\zeta)$, und wegen $q \nmid [L:K]$ ist auch $\zeta_q \notin K$ und daher $L = K(\zeta_q)$. Aus $z \notin K^q$ folgt $[K(\sqrt[q]{z}) : K] = q$, also $W_q \not\subset K(\sqrt[q]{z})$; $K(\sqrt[q]{z})/K$ ist nicht galoissch, und daher kann $L(\sqrt[q]{z})/K$ nicht abelsch sein. Anderseits ist aber $\zeta z \in L^q$, also $L(\sqrt[q]{z}) = L(\sqrt[q]{\zeta})$ der Körper der q^{l+1}-ten Einheitswurzeln über K und damit $L(\sqrt[q]{z})/K$ abelsch, womit ein Widerspruch erreicht ist. □

LEMMA 3. *Sei q eine Primzahl, $a \geqslant 1$, $n = q^a$, $[L:K] = q$, $L \neq K(\zeta_4)$ und $C \neq K^\times$. Dann gilt:*

(a) $C_{q^a}(L/K) = C_q(L/K) = \langle K^\times, x \rangle$ *für jedes $x \in C_q(L/K) \setminus K$.*

(b) $\left(C_{q^a}(L/K)^{q^a} : K^{\times q^a}\right) = \begin{cases} 1, & \text{falls } L = K(\zeta_{q^e}) \text{ mit } 2 \leqslant e \leqslant a, \\ q & \text{sonst.} \end{cases}$

Beweis. (a) Sei $x \in C_{q^a}(L/K) \setminus K$ und $c \geqslant 1$ minimal mit $x^{q^c} \in K$. Wäre $x^{q^c} \in K^q$, so wäre $x x^{q^{c-1}} = \zeta z$ mit $z \in K$, $\zeta \in W_q \setminus K$, also $q \neq 2$ und $K \subsetneq K(\zeta) \subseteq K(x) \subseteq L$; das ergibt wegen $[L:K] = q$ und $[K(\zeta):K] \mid q-1$ einen Widerspruch. Also ist $x^{q^c} \notin K^q$, und aus Lemma 1 folgt $c = 1$, also $x \in C_q(L/K)$; damit ist $C_{q^a}(L/K) = C_q(L/K)$ bewiesen. Sind $x, y \in C_q(L/K) \setminus K$, so ist $L = K(x) = K(y)$, also $\langle K^\times, x \rangle = \langle K^\times, y \rangle$ nach [4] (Korollar zu Theorem 3) und damit $C_q(L/K) = \langle K^\times, x \rangle$ für jedes $x \in C_q(L/K) \setminus K$.

(b) Wegen $[L:K] = q$ ist $W_q \cap L \subset K$, also $W_p \cap C_{q^a}(L/K) \subset K$ für jede Primzahl p; nach Satz 1 ist daher $\left(C_{q^a}(L/K) : K^\times\right) = q$, woraus wegen

$$\left(C_{q^a}(L/K) : K^\times\right) = \left(C_{q^a}(L/K)^{q^a} : K^{\times q^a}\right) \cdot \left(W_{q^a} \cap C_{q^a}(L/K) : W_{q^a} \cap K\right)$$

die Behauptung folgt. □

Das folgende Lemma stellt eine leichte Verschärfung von [5], Lemma 2 dar (siehe auch [1], Satz 2).

LEMMA 4. *Sei $L = K(\zeta_4) \neq K$, $a \geqslant 1$, $n = 2^a$ und*

$$c = \sup\{t \in \mathbf{N} \mid \zeta_{2^t} + \zeta_{2^t}^{-1} \in K\} \quad (2 \leqslant c \leqslant \infty);$$

sei $K^\times \subset C \subset C_{2^a}(L/K)$ eine Untergruppe und

$$\omega = \omega(a, K) = \begin{cases} \zeta_{2^{a+1}}, & \text{falls } a < c, \\ 1 + \zeta_{2^c}, & \text{falls } a \geqslant c. \end{cases}$$

Dann gilt:

(a) $C_{2^a}(L/K) = \langle K^\times, \omega \rangle$.

(b) $\quad (C^{2^a} : K^{\times 2^a}) = \begin{cases} 2, & \text{falls } \omega \in C, \\ 1, & \text{falls } \omega \notin C. \end{cases}$

Beweis. Sei σ die erzeugende Substitution von L/K; ist $t \geqslant 1$ mit $\zeta_{2^t} + \zeta_{2^t}^{-1} \in K$, so ist $\zeta_{2^t} \in L$ und $\zeta_{2^t}^{\sigma} = \zeta_{2^t}^{-1}$. Ein $x \in K^\times$ liegt genau dann in $C_{2^a}(L/K)$, wenn $1 = (x^{2^a})^{\sigma-1} = (x^{\sigma-1})^{2^a}$, d.h., wenn $x^{\sigma-1} \in W_{2^a} \cap L$. Damit erhält man einen Monomorphismus

$$1-\sigma\colon C_{2^a}(L/K)/K^\times \to W_{2^a} \cap L,$$

und nach Hilbert's Satz 90 ist

$$\mathrm{Bild}(1-\sigma) = \{\xi \in W^{2^a} \cap L \mid \xi^{1+\sigma} = 1\},$$

also $\mathrm{Bild}(1-\sigma) = \langle \xi_0 \rangle$ mit

$$\xi_0 = \begin{cases} \zeta_{2^a}, & \text{falls } a < c, \\ \zeta_{2^c}, & \text{falls } a \geqslant c, \end{cases}$$

und man rechnet sofort $\omega^{1-\sigma} = \xi_0$ nach. Daher bleibt zu zeigen:

$$\omega^{2^{a+1}} \in K^{\times 2^a}, \quad \omega^{2^a} \notin K^{\times 2^a};$$

beide Beziehungen sind unmittelbar nachzurechnen.

Lemma 5. *Sei $n = n_1 n_2$ mit $(n_1, n_2) = 1$ und*

$$C_{(n_i)} = \{x \in C \mid x^{n_i} \in K\}.$$

Dann gilt:

$$C^n \subseteq C^{n_i}_{(n_i)} \quad (i = 1, 2),$$

und die Diagonaleinbettung

$$C^n \hookrightarrow C^{n_1}_{(n_1)} \times C^{n_2}_{(n_2)}$$

induziert einen Gruppenisomorphismus

$$f\colon C^n/K^{\times n} \to C^{n_1}_{(n_1)}/K^{\times n_1} \times C^{n_2}_{(n_2)}/K^{\times n_2}.$$

Insbesondere gilt:

$$(C^n : K^{\times n}) = (C^{n_1}_{(n_1)} : K^{\times n_1}) \cdot (C^{n_2}_{(n_2)} : K^{\times n_2}).$$

Beweis. Wegen $K^{\times n_1} \cap K^{\times n_2} = K^{\times n}$ ist f injektiv. Sind $x_1 \in C_{(n_1)}$, $x_2 \in C_{(n_2)}$, so wähle man $a, b \in \mathbf{Z}$ mit $an_2 \equiv 1 \bmod n_1$, $bn_1 \equiv 1 \bmod n_2$ und erhält mit $x_1^a x_2^b \cdot K^{\times n}$ ein Urbild von $(x_1 K^{\times n_1}, x_2 K^{\times n_2})$; also ist f auch surjektiv. □

Lemma 6. *L/K habe keine echten Zwischenkörper. Dann ist entweder*

$$C_n(L/K) = K^\times$$

oder

$$[L : K] \text{ ist eine Primzahl.}$$

Beweis. Sei $C_n(L/K) \neq K^\times$; dann existiert eine Primzahl $q \mid n$ und ein $x \in C_n(L/K) \setminus K$ mit $x^q \in K$, und nach Voraussetzung ist $L = K(x)$.

Im Falle $x^q \notin K^q$ ist nach Lemma 1 $[L : K] = q$; im Falle $x^q \in K^q$ ist $L = K(x) = K(\zeta_q)$, also L/K zyklisch und ohne echte Zwischenkörper, folglich vom Primzahlgrad. □

Beweis von Satz 2. Nach Lemma 5 genügt es, den Beweis für Primzahlpotenzen $n = q^a$ (q prim, $a \geqslant 1$) zu führen. Ich bediene mich vollständiger Induktion nach $[L : K]$ und nehme zunächst an, daß L/K keine echten Zwischenkörper enthält. Ist $C_n(L/K) \neq K^\times$, so ist nach Lemma 6 $[L : K]$ eine Primzahl, und mit den Lemmata 2, 3 und 4 folgt in diesem Falle die Behauptung des Satzes.

Sei nun $K \subsetneq K_1 \subsetneq L$ ein echter Zwischenkörper und Satz 2 für L/K_1 und K_1/K bewiesen. Dann gilt:

$$(C^n : K^{\times n}) = (C^n : C^n \cap K_1^{\times n}) \cdot (C^n \cap K_1^{\times n} : K^{\times n});$$

$(C^n : C^n \cap K_1^{\times n}) = (\langle K_1^\times, C \rangle^n : K_1^{\times n})$ teilt $[L : K_1]$, und wegen $C^n \cap K_1^{\times n} \subseteq C_n(K_1/K)^n$ ist $(C^n \cap K_1^{\times n} : K^{\times n})$ ein Teiler von $\left(C_n(K_1/K)^n : K^{\times n}\right)$, also auch von $[K_1 : K]$, woraus die Behauptung folgt. □

Aus obigem Beweis kann man leicht ablesen:

Lemma 7. *Sei L/K eine endlich-separable Körpererweiterung, $K \subseteq K_1 \subseteq L$ ein Zwischenkörper, $n \in \mathbf{N}$ teilerfremd zur Charakteristik von K und $K^\times \subseteq C \subseteq L^\times$ eine Untergruppe mit $C^n \subset K$ und $(C^n : K^{\times n}) = [L : K]$. Dann gilt:*

(a) $L = K(C)$;

(b) $[L : K_1] = (\langle K_1^\times, C \rangle^n : K_1^{\times n}) = \left(C_n(L/K_1)^n : K_1^{\times n}\right)$,
$[K_1 : K] = (C^n \cap K_1^{\times n} : K^{\times n}) = \left(C_n(K_1/K)^n : K^{\times n}\right)$.

3. Bevor ich notwendige und hinreichende Kriterien für das Bestehen der Gleichheit $[L : K] = (C^n : K^{\times n})$ angebe, untersuche ich die Struktur einiger spezieller Radikalerweiterungen genauer.

Ein Spezialfall des folgenden Lemmas findet sich bereits in [5], Lemma 6 (siehe auch [1], Satz 2):

Lemma 8. *Sei K ein Körper und p eine von der Charakteristik von K verschiedene Primzahl; im Falle $p = 2$ sei $\zeta_4 \in K$. Sei $0 \leqslant a < \infty$ maximal mit $\zeta_{p^\mu} \in K$, $\mu \geqslant 1$, $L = K(\zeta_{p^\mu})$ und $s \geqslant 1$. Dann gilt:*

$$C_{p^s}(L/K) = \langle K^\times, W_{p^{s+a}} \cap L \rangle.$$

Beweis. Es genügt, $C_{p^s}(L/K) \subseteq \langle K^\times, W_{p^{s+a}} \cap L \rangle$ zu zeigen, und ich führe den Beweis durch Induktion über μ. Im Falle $\mu = 1$ ist $[L : K] \mid p-1$, also nach Satz 2 $\left(C_{p^s}(L/K)^{p^s} : K^{\times p^s}\right) \mid p-1$ und damit $C_{p^s}(L/K)^{p^s} = K^{\times p^s}$; ist nun $x \in C_{p^s}(L/K)$, so ist $x^{p^s} = z^{p^s}$ mit $z \in K$, also $x = \zeta z \in \langle K^\times, W_{p^s} \cap L \rangle$.

Sei nun die Behauptung für ein $\mu \geqslant 1$ bewiesen, $L = K(\zeta_{p^{\mu+1}})$ und $x \in C_{p^s}(L/K)$; falls $x \in K(\zeta_{p^\mu})$, ist nach Induktionsvoraussetzung $x \in \langle K^\times, W_{p^{s+a}} \cap K(\zeta_{p^\mu}) \rangle \subseteq \langle K^\times, W_{p^{s+a}} \cap L \rangle$. Sei also $x \notin K(\zeta_{p^\mu})$; dann ist $K(\zeta_{p^\mu})$

$\subsetneq L$, also $[L:K(\zeta_{p^\mu})]=p$ und daher $L=K(x)$; wegen $x^{p^s}\in K\subseteq K(\zeta_{p^\mu})$ folgt aus Lemma 1 $x^n\in K(\zeta_{p^\mu})$, und nach Lemma 3 gilt $x=\zeta y$ mit $y\in K(\zeta_{p^\mu})$ und einer primitiven $p^{\mu+1}$-ten Einheitswurzel ζ. Ist $t=\max(\mu+1,s)$, so ist $y^{p^t}\in K$, also $y\in C_{p^t}(K(\zeta_{p^\mu})/K)$, woraus nach Induktionsvoraussetzung $y=\zeta' z$ mit $\zeta'\in W_{p^{t+a}}\cap L$ und $z\in K$ folgt. Damit gilt

$$x=\zeta\zeta' z;$$

$\zeta\zeta'\in L$ ist eine Einheitswurzel von p-Potenzordnung mit $(\zeta\zeta')^{p^s}\in K$, also $(\zeta\zeta')^{p^s}\in W_{p^a}$, woraus $\zeta\zeta'\in W_{p^{a+s}}\cap L$ folgt. □

Die folgenden Sätze liefern in einer Reihe von Fällen eine gute Übersicht über den Zwischenkörperverband einer Radikalerweiterung.

LEMMA 9. *Sei L/K eine Körpererweiterung, $x\in L$ und $n\geqslant 1$ mit $L=K(x)$ und $x^n\in K$; n sei minimal mit dieser Eigenschaft und teilerfremd zur Charakteristik von K. Ferner sei $W_n\cap K=1$ (also insbesondere $2\nmid n$) und $m|n$ maximal mit $x^n\in K^m$. Dann gilt:*

(a) $\zeta_m\in L$, $[L:K(\zeta_m)]=(\langle K^\times,x\rangle^n:K^{\times n})=n/m$.

(b) *$K(\zeta_m)$ ist der größte über K abelsche Zwischenkörper von L/K.*

(c) *Ist $k\in\mathbf{N}$ mit $(C_k(L/K)^k:K^{\times k})=[L:K]$, so folgt:*

(c_1) $([K(\zeta_m):K],n)=1$;

(c_2) *Ist $K\subseteq K_1\subseteq L$ ein Zwischenkörper mit $[K_1:K]=[K(\zeta_m):K]$, so ist $K_1=K(\zeta_m)$.*

Beweis. (a) Sei $z\in K$ mit $x^n=z^m$; dann ist $z\notin K^p$ für alle $p|n/m$ und $x^{n/m}=z\zeta$ mit einer primitiven m-ten Einheitswurzel ζ, also $K(\zeta)=K(\zeta_m)\subseteq L$. Wegen $L=K(\zeta_m)(x)$ und $x^{n/m}\in K(\zeta_m)$ folgt $[L:K(\zeta_m)]\leqslant n/m$; wäre $[L:K(\zeta_m)]<n/m$, so gäbe es nach Lemma 1 eine Primzahl $p|n/m$ und ein $a\in K(\zeta_m)$ mit $x^{n/m}=z\zeta=a^p$, und damit wäre $\sqrt[p]{z}\in K(\zeta_m)(\sqrt[p]{\zeta})=K(\zeta_{mp})$; nun ist aber $K(\zeta_{mp})/K$ abelsch und $K(\sqrt[p]{z})/K$ wegen $\zeta_p\notin K$ nicht einmal normal: das ist ein Widerspruch, es gilt $[L:K(\zeta_m)]=n/m$.

Sei $d=(\langle K^\times,x\rangle^n:K^{\times n})$; wegen $(x^n)^{n/m}=z^n\in K^{\times n}$ gilt $d|n/m$; aus $x^{nd}=z^{md}\in K^{\times n}$ folgt wegen $W_n\cap K=1$, aber $z\notin K^{\times n/md}$, also $n/md=1$, $d=n/m$.

(b) Wäre $K(\zeta_m)$ nicht der größte über K abelsche Zwischenkörper, so gäbe es einen Körper K_1 mit $K(\zeta_m)\subsetneq K_1\subseteq L$ derart, daß K_1/K abelsch ist. Wegen $L=K_1(x)$, $x^{n/m}=z\zeta\in K_1$ und $[L:K_1]<n/m$ folgte nach Lemma 1 die Existenz einer Primzahl $p|n/m$ und eines $a\in K_1$ mit $z\zeta=a^p$, also $\sqrt[p]{z}\in K_1(\sqrt[p]{\zeta})=K_1\cdot K(\zeta_{pm})$; das kann aber wieder nicht sein, da $K_1\cdot K(\zeta_{pm})/K$ abelsch, jedoch $K(\sqrt[p]{z})/K$ nicht normal ist.

(c_1) Sei p ein Primteiler von $[K(\zeta_m):K]$; dann gibt es einen über K abelschen Zwischenkörper $K\subsetneq K_1\subseteq K(\zeta_m)$ mit $[K_1:K]=p$. Nach Lemma 7 ist dann $p=(C_k(K_1/K)^k:K^{\times k})$, woraus mit den Lemmata 2, 3 und 5

$$p=(C_p(K_1/K)^p:K^{\times p})$$

folgt, also (wiederum mit Lemma 3 und 7) $K_1=K(x)$ mit $x^p\in K$. Aber K_1/K ist abelsch, also folgt $\zeta_p\in K$ und damit $p\nmid n$, da $W_n\cap K=1$.

(c_2) Sei $[K_1:K]=[K(\zeta_m):K]$; dann ist

$$[K_1\cdot K(\zeta_m):K_1]=[K(\zeta_m):K_1\cap K(\zeta_m)]$$

Teiler von $[L:K_1]=[L:K(\zeta_m)]$ und auch von $[K(\zeta_m):K]$, also einerseits Teiler von n und anderseits prim zu n, woraus $[K_1\cdot K(\zeta_m):K_1]=1$ und damit $K_1=K(\zeta_m)$ folgt. □

KOROLLAR. *L/K sei eine endliche abelsche Erweiterung, $n\in\mathbf{N}$ teilerfremd zur Charakteristik von K und $W_n\cap K=1$. Dann gilt*

$$C_n(L/K)=\langle K^\times,W_n\cap L\rangle.$$

Beweis. Es genügt, Lemma 9 auf $x\in C_n(L/K)$ anzuwenden. Das Korollar folgt auch unmittelbar aus [5], Theorem 2, das im Falle $W_n\cap K=1$ einen Spezialfall von Lemma 9 darstellt.

Die Aussagen (a) und (b) von Lemma 9 sind die entscheidenden Spezialfälle des folgenden Satzes:

SATZ 3. *Sei L/K eine endlich-separable Körpererweiterung, $n\in\mathbf{N}$ teilerfremd zur Charakteristik von K, $W_n\cap K=1$ (also insbesondere $2\nmid n$) und $K^\times\subseteq C\subseteq L^\times$ eine Untergruppe mit $C^n\subset K$ und $L=K(C)$; sei $\overline{K}=K(C\cap W_n)$. Dann gilt:*

(a) $[L:\overline{K}]=(\langle\overline{K}^\times,C\rangle:\overline{K}^\times)=(C:C\cap\langle K^\times,W_n\rangle)=(C^n:K^{\times n})$.

(b) *$\overline{K}$ ist der größte über K abelsche Zwischenkörper von L/K.*

(c) *Jeder Zwischenkörper $\overline{K}\subseteq K_1\subseteq L$ ist von der Form $K_1=K(C_1)$ mit einer Untergruppe $C_1\subseteq C$.*

Beweis. Ich zeige zunächst:

$$(*)\qquad W_n\cap\langle\overline{K}^\times,C\rangle\subset\overline{K}.$$

Sei $\zeta\in W_n\cap\langle\overline{K}^\times,C\rangle$, $\zeta=yx$ mit $y\in\overline{K}$, $x\in C$; dann ist $1=\zeta^n=y^nx^n$, $x^n\in C^n\subset K$, also $y\in C_n(\overline{K}/K)$ und damit $y=\xi x_0$ mit $\xi\in W_n\cap L$, $x_0\in K$ nach dem Korollar zu Lemma 9. Es folgt $\zeta\xi^{-1}=xx_0\in C\cap W_n\subset\overline{K}$, also $x\in\overline{K}$ und damit $\zeta\in\overline{K}$.

(a) $L=\overline{K}(C)$ erfüllt nach (*) die Voraussetzungen von Satz 1 (n ist ungerade!), also gilt $[L:\overline{K}]=(\langle\overline{K}^\times,C\rangle:\overline{K}^\times)$. Nach dem Korollar zu Lemma 9 ist $C\cap\overline{K}^\times\subseteq\langle K^\times,W_n\rangle$ und daher $C\cap\overline{K}^\times=C\cap\langle K^\times,W_n\rangle$,

woraus $(\langle \bar{K}^\times, C\rangle : \bar{K}^\times) = (C : C\cap\langle K^\times, W_n\rangle)$ folgt, aber $(C : C\cap\langle K^\times, W_n\rangle) = (C^n : K^{\times n})$, da $W_n\cap C = W_n\cap C\cap\langle K^\times, W_n\rangle$.

(b) Ich nehme an, $\bar{K}$ sei nicht der größte über K abelsche Teilkörper von L; dann gibt es einen über K abelschen Körper K_1 mit $\bar{K}\subsetneq K_1\subseteq L$, so daß $K_1/\bar{K}$ keine echten Zwischenkörper besitzt. Seien $x_1, \dots, x_k \in C$ derart, daß die Restklassen $\bar{x}_1, \dots, \bar{x}_k \in \langle \bar{K}^\times, C\rangle/\bar{K}^\times$ eine Basis von $\langle \bar{K}^\times, C\rangle/\bar{K}^\times$ bilden, und sei $n_i \in \boldsymbol{N}$ die Ordnung von $\bar{x}_i$; dann ist

$$L = \bar{K}(x_1, \dots, x_k) = K_1(x_1, \dots, x_k),$$

$$[L : \bar{K}] = (\langle \bar{K}^\times, C\rangle : \bar{K}^\times) = \prod_{i=1}^{k} n_i > [L : K_1],$$

und daher folgt nach [4], Theorem 1 die Existenz einer Relation der Form

$$\prod_{\substack{i=1\\ p\mid n_i}}^{k} x_i^{n_i c_i} = y^p \tag{0}$$

mit $y \in K_1$, $c_i \in \boldsymbol{Z}$ und mindestens einem $c_j \not\equiv 0 \bmod p$, es kann jedoch (0) nicht mit einem $y \in \bar{K}$ statthaben. Es ist $y^p \in \bar{K}$, $y^p \notin \bar{K}^p$ und daher $K_1 = \bar{K}(y)$; setzt man

$$y_1 = \prod_{\substack{i=1\\ p\mid n_i}}^{k} x_i^{\frac{n_i}{p} c_i} \in C,$$

so ist $y_1^p = y^p$, also $\bar{K}(y_1)$ konjugiert zu K_1 und damit $\bar{K}(y_1) = K_1$, da ja K_1/K abelsch ist. Nun ist aber auch $K(y_1)/K$ abelsch und $y_1^n \in K$, woraus nach dem Korollar zu Lemma 9 $y_1 = z\xi$ mit $z \in K$ und $\xi \in W_n$ folgt; wegen $y_1 \in C$ ist $\xi \in C$, also $\xi \in \bar{K}$, und das hat den Widerspruch $y_1 \in \bar{K}$, $K_1 = \bar{K}$, zur Folge.

(c) Sei $\bar{K}\subseteq K_1\subseteq L$ ein Zwischenkörper. Nach (a) ist

$$[L : \bar{K}] = (\langle \bar{K}^\times, C\rangle : \bar{K}^\times) = (\langle \bar{K}^\times, C\rangle^n : \bar{K}^{\times n}),$$

da $W_n\cap\langle \bar{K}^\times, C\rangle \subset \bar{K}$, und daraus folgt nach Lemma 7

$$[K_1 : \bar{K}] = (C^n\cap K_1^{\times n} : \bar{K}^{\times n}).$$

Sei $C_1 = \{x \in C \mid x^n \in K_1^{\times n}\}$; dann ist $C_1 \subset K_1$, da $W_n\cap L \subset \bar{K}\subseteq K_1$, also $\bar{K}(C_1)\subseteq K_1$. Unter Verwendung von Satz 2 folgt

$$\begin{aligned}[\bar{K}(C_1) : \bar{K}] &\geqslant (\langle \bar{K}^\times, C_1\rangle^n : \bar{K}^{\times n}) = (C^n\cap K_1^{\times n} : \bar{K}^{\times n})\\ &= [K_1 : \bar{K}] \geqslant [\bar{K}(C_1) : \bar{K}]\end{aligned}$$

und damit $\bar{K}(C_1) = K_1$. □

Im Gegensatz zu dem in Lemma 9(c) behandelten Spezialfall kann im allgemeinen der volle Zwischenkörperverband von $K(C)/K$ auch schon

im Falle zyklischer Faktorgruppe $C/K^\times$ recht kompliziert werden. Wie das Beispiel $\boldsymbol{Q}(\sqrt[21]{2\zeta_{21}})/\boldsymbol{Q}$ zeigt; Einheitswurzeln von 2-Potenzordnung bringen noch einmal zusätzliche Schwierigkeiten. Ist aber $C/K^\times$ zyklisch von ungerader Primzahlpotenzordnung, so kann man den Zwischenkörperverband von $K(C)/K$ gut überschauen:

Satz 4. *Sei $p \neq 2$ eine Primzahl, K ein Körper mit $\mathrm{char}(K) \neq p$, $s \geqslant 1$ und $L = K(x)$ mit $x^{p^s} \in K$, $x^{p^{s-1}} \notin K$.*

(a) *Genau dann ist $\zeta_p \in L\setminus K$, wenn $x^{p^s} \in K^p$.*

(b) *Ist $\zeta_p \notin L\setminus K$ (also entweder $\zeta_p \in K$ oder $\zeta_p \notin L$), so sind die Körper $K(x^{p^j})$ $(0 \leqslant j \leqslant s)$ genau die sämtlichen Zwischenkörper von L/K.*

(c) *Ist $\zeta_p \in L\setminus K$, $\bar{K} = K(W_{p^s}\cap L)$ und $\mu \leqslant s$ maximal mit $x^{p^s} \in K^{p^\mu}$ so ist $\bar{K} = K(\zeta_{p^\mu})$, und im Falle $\zeta_{p^{\mu+1}} \notin L$ gilt für jeden Zwischenkörper $K \subseteq K_1 \subseteq L$ entweder $K_1 \subseteq \bar{K}$ oder $\bar{K} \subseteq K_1$.*

Beweis. (a) Falls $\zeta_p \in K$, folgt $x^{p^s} \notin K^p$ nach Lemma 1; ist aber $\zeta_p \notin K$, so ist nach Lemma 9 $K(\zeta_{p^\mu})$ ($\mu \leqslant s$ maximal mit $x^{p^s} \in K^{p^\mu}$) der größte über K abelsche Zwischenkörper von L/K, also $K(\zeta_{p^\mu}) = K(W_{p^s}\cap L)$; daraus folgt nun (a) und auch bereits der erste Teil von (c).

(b) Sei $K \subseteq K_1 \subseteq L$ ein Zwischenkörper und $k \geqslant 0$ minimal mit $x^{p^k} \in K_1$; wegen $\zeta_p \notin L\setminus K_1$ ist nach (a) $x^{p^k} \notin K_1^p$, also $[L : K_1] = p^k$. Anderseits folgt aber $K(x^{p^k}) \subseteq K_1$ und $p^k \geqslant [L : K(x^{p^k})] \geqslant [L : K_1] = p^k$, also insgesamt $K_1 = K(x^{p^k})$.

(c) In (a) wurde bereits $\bar{K} = K(\zeta_{p^\mu})$ bewiesen. Im Falle $\mu = s$ ist $\bar{K} = L$ und nichts mehr zu zeigen; sei also $1 \leqslant \mu < s$, $t = s-\mu \geqslant 1$ und $z \in K$ mit $x^{p^s} = z^{p^\mu}$, also $x^{p^t} = \zeta_0 z$ mit einer primitiven p^μ-ten Einheitswurzel ζ_0. Sei ζ eine primitive p^s-te Einheitswurzel mit $\zeta^{p^t} = \zeta_0$ und $\tilde{L} = L(\zeta) = L(\zeta_{p^s})$. Ich setze

$$y = \zeta^{-1}x$$

und habe $y \in L$, $y^{p^t} = \zeta_0^{-1}x^{p^t} = z \in K\setminus K^p$, also $[K(y) : K] = p^t$, und nach (a) gilt $K(y)\cap K(\zeta) = K$, woraus wegen $\tilde{L} = K(\zeta, y)$ auch $[\tilde{L} : K(\zeta)] = [K(y) : K] = p^t$ folgt. Die Galoisgruppe von $\tilde{L}/K(y)$ ist isomorph zu einer Untergruppe der primen Restklassengruppe mod p^s, also zyklisch, und ich setze

$$\mathrm{Gal}(\tilde{L}/K(y)) = \langle\sigma\rangle$$

mit $\zeta^\sigma = \zeta^r$, $r \in \boldsymbol{Z}$, $r \not\equiv 0 \bmod p$. Sei $\tau = (y \mapsto \zeta^{p^\mu}y)$ die erzeugende Substitution von $\tilde{L}/K(\zeta)$; dann ist $\tau^{p^t} = 1$ und

$$G = \mathrm{Gal}(\tilde{L}/K) = \langle\sigma, \tau\rangle.$$

Für $\nu \in \boldsymbol{Z}$ ist

$$y^{\tau\sigma} = \zeta^{p^\mu r}\cdot y, \qquad \zeta^{\tau\sigma} = \zeta^r,$$

$$y^{\sigma\tau^\nu} = \zeta^{p^{\mu_\nu}}\cdot y, \qquad \zeta^{\sigma\tau^\nu} = \zeta^r,$$

also genau dann $\tau\sigma = \sigma\tau^r$, wenn $p^\mu r \equiv p^\mu \nu \bmod p^s$, also $r \equiv \nu \bmod p^t$, woraus $\tau\sigma = \sigma\tau^r$ folgt.

Als nächstes bestimme ich die Fixgruppe G_0 von L; es ist

$$G = \{\sigma^k\tau^l \mid 0 \leqslant k < [K(\zeta):K],\ 0 \leqslant l < p^t\},$$

und genau dann ist $\sigma^k\tau^l \in G_0$, wenn $x^{\sigma^k\tau^l} = x$, woraus wegen $x^{\sigma^k\tau^l} = \zeta^{lp^\mu + r^k - 1} \cdot x$

$$G_0 = \{\sigma^k\tau^l \mid lp^\mu + r^k - 1 \equiv 0 \bmod p^s\}$$

folgt. Sei k_0 die Ordnung von $r \bmod p^\mu$ und $l_0 = -\dfrac{r^{k_0}-1}{p^\mu}$; beachtet man

$$(0) \qquad (\sigma^k\tau^l)^n = \sigma^{nk} \cdot \tau^{l\cdot\frac{r^{nk}-1}{r^k-1}} \quad \text{für} \quad n \geqslant 1,$$

so folgt

$$G_0 = \langle \sigma^{k_0}\tau^{l_0} \rangle = \mathrm{Gal}(\tilde{L}/L).$$

Wegen $\zeta_{p^{\mu+1}} \notin L$ ist

$$\zeta_{p^{\mu+1}}^{\sigma^{k_0}\tau^{l_0}} = \zeta_{p^{\mu+1}}^{r^{k_0}} \neq \zeta_{p^{\mu+1}},$$

also $r^{k_0} \not\equiv 1 \bmod p^{\mu+1}$ und damit $l_0 \not\equiv 0 \bmod p$. Aus demselben Grunde ist $\langle \sigma^{k_0} \rangle$ die Fixgruppe von $K(y, \zeta_{p^\mu})$, also $\langle \sigma^{k_0}, \tau \rangle$ die Fixgruppe von $K(y, \zeta_{p^\mu}) \cap K(\zeta)$; nun ist einerseits

$$\bar{K} = K(\zeta_{p^\mu}) \subseteq K(y, \zeta_{p^\mu}) \cap K(\zeta),$$

anderseits aber $\langle \sigma^{k_0}, \tau \rangle \supseteq \langle \sigma^{k_0}\tau^{l_0} \rangle$ und damit $K(y, \zeta_{p^\mu}) \cap K(\zeta) \subseteq L$, also $K(y, \zeta_{p^\mu}) \cap K(\zeta) = \bar{K}$; folglich gilt

$$\langle \sigma^{k_0}, \tau \rangle = \mathrm{Gal}(\tilde{L}/\bar{K}).$$

Für den Beweis von (c) genügt es nun, die folgende rein gruppentheoretische Behauptung zu zeigen:

$$(*) \quad \begin{cases} \text{Für jede Untergruppe } G_0 \leqslant H \leqslant G \text{ gilt entweder} \\ H \subseteq \langle \sigma^{k_0}, \tau \rangle \text{ oder } \langle \sigma^{k_0}, \tau \rangle \subseteq H. \end{cases}$$

Fall 1: H ist zyklisch. Sei $H = \langle \sigma^k\tau^l \rangle$ mit $0 \leqslant k < [K(\zeta):K]$, $0 \leqslant l < p^t$; nach Voraussetzung ist $\sigma^{k_0}\tau^{l_0} \in H$, also nach (0) $k \mid k_0$, $k_0 = nk$ mit $n \geqslant 1$ und $\sigma^{k_0}\tau^{l_0} = (\sigma^k\tau^l)^n$; daraus folgt

$$l \cdot \frac{r^{nk}-1}{r^k-1} \equiv l_0 \bmod p$$

unter Beachtung von (0) und der Tatsache, daß p die Ordnung von τ teilt. Wäre nun $k < k_0$, so wäre $r^k \not\equiv 1 \bmod p^\mu$, also $l_0 \equiv 0 \bmod p$; oben hatte ich aber $l_0 \not\equiv 0 \bmod p$ nachgewiesen. Daher ist $k = k_0$ und $H = \langle \sigma^{k_0}\tau^l \rangle \subseteq \langle \sigma^{k_0}, \tau \rangle$.

Fall 2: H ist nicht zyklisch. Dann enthält H mindestens ein Element der Form $\sigma^k\tau^l$ mit $k \geqslant 1$; sei $k \geqslant 1$ minimal mit der Eigenschaft: es gibt ein $l \geqslant 0$ mit $\sigma^k\tau^l \in H$. Da H nicht zyklisch ist, gibt es zu mindestens einem k' Zahlen l', l'' mit $l' \not\equiv l'' \bmod p^t$, $\sigma^{k'}\tau^{l'} \in H$ und $\sigma^{k'}\tau^{l''} \in H$, also $1 \neq \sigma^{k'}\tau^{l'-l''}\sigma^{-k'} \in H \cap \langle\tau\rangle$. Sei $H \cap \langle\tau\rangle = \langle\tau^{p^u}\rangle$ mit $0 \leqslant u < t$; ist nun $\sigma^{k'}\tau^{l'} \in H$, so ist $k \mid k'$, $k' = kn$ mit $n \geqslant 1$ und $\sigma^{k'}\tau^{l'} \cdot (\sigma^k\tau^l)^{-n} \in H \cap \langle\tau\rangle$, also $\sigma^{k'}\tau^{l'} \in \langle \sigma^k\tau^l, \tau^{p^u} \rangle$. Damit habe ich

$$H = \langle \sigma^k\tau^l, \tau^{p^u} \rangle$$

bewiesen, und ich kann $0 \leqslant l < p^u$ annehmen. Nach Voraussetzung ist $\sigma^{k_0}\tau^{l_0} \in H$, also $k \mid k_0$, $k_0 = nk$, und im Falle $k = k_0$ ist $H \subseteq \langle \sigma^{k_0}, \tau \rangle$. Sei nun $k < k_0$; dann ist $\sigma^{k_0}\tau^{l_0} = (\sigma^k\tau^l)^n \cdot \tau^{p^u b}$ mit geeignetem $b \in \boldsymbol{Z}$, woraus mit (0)

$$l \cdot \frac{s^{nk}-1}{s^k-1} + p^u b \equiv l_0 \bmod p$$

folgt. Wegen $s^{nk} \equiv 1 \bmod p^\mu$, $s^k \not\equiv 1 \bmod p^\mu$ und $l_0 \not\equiv 0 \bmod p$ folgt $u = 0$, also $l = 0$ und

$$H = \langle \sigma^k, \tau \rangle \supseteq \langle \sigma^{k_0}, \tau \rangle.$$

Damit ist Satz 4 vollständig bewiesen.

4. Der folgende Satz gibt notwendige und hinreichende Kriterien für das Bestehen der bereits in 1. erwähnten Gleichheit $[L:K] = (O^n : K^{\times n})$ an.

Satz 5. *Sei L/K eine endlich-separable Körpererweiterung, $n \in \boldsymbol{N}$ teilerfremd zur Charakteristik von K, $K^\times \subseteq O \subseteq L^\times$ eine Untergruppe mit $O^n \subset K$ und $L = K(O)$. Sei $n = n_1 n_2$ derart, daß $(n_1, n_2) = 1$ und für jede Primzahl p mit $p \mid n$ gilt:*

$$p \quad \textit{teilt} \quad \begin{cases} n_1, & \textit{falls } \zeta_p \notin K, \\ n_2, & \textit{falls } \zeta_p \in K. \end{cases}$$

Sei $O \cap W_{n_1} = \langle w \rangle$ und $n_2 = 2^{a_2} \cdot n_2'$ mit $n_2' \equiv 1 \bmod 2$, $a_2 \geqslant 0$.

Genau dann ist $[L:K] = (O^n : K^{\times n})$, wenn die folgenden drei Bedingungen erfüllt sind:

I. *Es gibt Untergruppen C_1 und T von O mit $K^\times \subseteq C_1$, $\langle K^\times, w \rangle \subseteq T$, $O/K^\times = T/K^\times \times C_1/K^\times$ und $w \in K(C_1)$.*

II. $W_{n_2} \cap O \subset K$.

III. *Entweder $W_{2^{a_2}} \cap O \subset K$ oder $\zeta_4 \notin K$, $W_{2^{a_2}} \cap O \subset K(\zeta_4)$ und $\omega(a_2, K) \in O$;*

für die Definition von $\omega(a_2, K)$ siehe Lemma 4.

Setzt man die Gültigkeit von II *und* III *voraus, so ist* I *äquivalent zu der folgenden formal stärkeren Bedingung:*

I′. *Sind* C_1 *und* T *Untergruppen von* C *mit* $K^\times \subseteq C_1$, $\langle K^\times, w\rangle \subseteq T$ *derart, daß*

$$C/K^\times = T/K^\times \times C_1/K^\times \quad \text{und} \quad (n_2, (T:K^\times)) = 1$$

gilt, so folgt $w \in K(C_1)$.

Daß I aus I′ folgt, ist klar, da es stets Untergruppen C_1 und T von C mit $K^\times \subseteq C_1$, $\langle K^\times, w\rangle \subseteq T$, $C/K^\times = T/K^\times \times C_1/K^\times$ und $(n_2, (T:K^\times)) = 1$ gibt; man braucht ja nur $C/K^\times$ in die p-Sylowgruppen zu zerlegen. Ich werde zeigen, daß I, II, III hinreichend und daß I′, II, III notwendig für $[L:K] = (C^n : K^{\times n})$ sind. Die folgenden drei Lemmata bilden das Kernstück des Beweises.

Lemma 10. *Es seien die Voraussetzungen von Satz* 5 *erfüllt;* C_1 *und* T *seien Untergruppen von* C *mit* $K^\times \subseteq C_1$, $\langle K^\times, w\rangle \subseteq T$, $C/K^\times = T/K^\times \times C_1/K^\times$ *und* $(n_2, (T:K^\times)) = 1$. *Dann gilt:*

$$(C_n : K^{\times n}) = (T^n : K^{\times n})\cdot(C_1^n : K^{\times n}).$$

Beweis. Es genügt,

$$(C\cap W_n)\cdot K^\times/K^\times = (T\cap W_n)\cdot K^\times/K^\times \times (C_1\cap W_n)\cdot K^\times/K^\times$$

nachzuweisen; wegen $C\cap W_n = C\cap W_{n_1}\times C\cap W_{n_2}$ und $C\cap W_{n_1} = T\cap W_{n_1}$ genügt es dazu,

$$C\cap W_{n_2} \subseteq C_1$$

zu zeigen. Sei dazu $w_2 \in C\cap W_{n_2}$, $w_2 = zx$ $(z\in T, x\in C_1)$, also $1 = w_2^{n_2} = z^{n_2}x^{n_2}$; daraus folgt $z^{n_2}\in K$, $x^{n_2}\in K$, und da die Ordnung von $T/K^\times$ zu n_2 teilerfremd ist, erhalte ich $z\in K$, $w_2\in C_1$. □

Lemma 11. *Es seien die Voraussetzungen und die Bedingungen* II *und* III *von Satz* 5 *erfüllt.* C_1 *sei eine Untergruppe von* C *mit* $K^\times \subseteq C_1$, $C_1\cap\langle w\rangle = 1$ *und* $\omega = \omega(a_2, K)\in C_1$, *falls* $\omega\in C$. *Dann gilt:*

$$[K(C_1):K] = (C_1^n : K^{\times n}).$$

Beweis. Ist p eine Primzahl mit $W_p\cap C_1 \neq 1$, so ist $p|n$, also wegen $C_1\cap\langle w\rangle = 1$ auch $p|n_2$ und daher $W_p\subset K$; daraus folgt

$$W_p\cap C_1 \subset K \text{ für alle Primzahlen } p.$$

Fall 1. $W_{2^{a_2}}\cap C \subset K$. Dann ist wegen $W_{n_1}\cap C_1 = \langle w\rangle\cap C_1 = 1$ und $W_{n_2'}\cap C\subset K$ auch $W_n\cap C_1\subset K$, also

$$(C_1^n : K^{\times n}) = (C_1 : K^\times).$$

Die Behauptung folgt nun aus Satz 1, falls die dort angegebenen Bedingungen A und B erfüllt sind. A wurde bereits nachgeprüft. Gälte B nicht, so wäre $1+\zeta_4\in C_1$, aber $\zeta_4\notin K$; wegen $(1+\zeta_4)^n\in K$ wäre $4|n$, also $a_2\geqslant 2$ und daher $\zeta_4\notin C$ im Widerspruch zu $(1+\zeta_4)^2 = 2\zeta_4\in C$.

Fall 2. $W_{2^{a_2}}\cap C\notin K$. Nach III ist dann $W_{2^{a_2}}\cap C\subset K(\zeta_4)$, und daraus folgt $W_n\cap C_1\subset K(\zeta_4)$, also $W_n\cap C_1 = W_n\cap C_1\cap K(\zeta_4)$ und damit

$$\begin{aligned}(C_1^n : K^{\times n}) &= (C_1^n : [C_1\cap K(\zeta_4)]^n)\cdot([C_1\cap K(\zeta_4)]^n : K^{\times n})\\ &= (\langle C_1, K(\zeta_4)^\times\rangle : K(\zeta_4)^\times)\cdot([C_1\cap K(\zeta_4)]^n : K^{\times n}).\end{aligned}$$

Nach Lemma 5 und Satz 2 ist

$$([C_1\cap K(\zeta_4)]^n : K^{\times n}) = (C_2^{2^{a_2}} : K^{\times 2^{a_2}}),$$

wobei $C_2 = \{x\in C_1\cap K(\zeta_4) \mid x^{2^{a_2}}\in K\}$. Nach III ist $\omega\in C$, also nach Voraussetzung $\omega\in C_1$ und damit auch $\omega\in C_2$, woraus nach Lemma 4

$$(C_2^{2^{a_2}} : K^{\times 2^{a_2}}) = 2$$

folgt; damit bleibt nun noch

$$[L:K(\zeta_4)] = (\langle C_1, K(\zeta_4)^\times\rangle : K(\zeta_4)^\times)$$

zu beweisen, und ich wende dafür Satz 1 auf die Erweiterung $L = K(\zeta_4)(C_1)$ von $K(\zeta_4)$ an. Bedingung B ist hier automatisch erfüllt, und ich nehme an, für eine Primzahl $p\neq 2$ sei $\zeta_p\in\langle K(\zeta_4)^\times, C_1\rangle$, aber $\zeta_p\notin K(\zeta_4)$. Sicher ist $\zeta_p^n\in K(\zeta_4)$ und damit $p|n$, also $p|n_1$. Ferner ist nach Annahme $\zeta_p = zx$ mit $z\in K(\zeta_4)$, $x\in C_1$ und damit $1 = \zeta_p^n = z^n x^n$, also $z^n\in C^n\subset K$; sei $m|n$ minimal mit $z^m\in K$. Wäre nun $p\nmid m$, so wäre $\zeta_p^m = z^m x^m\in C_1$ und damit $W_p = \langle\zeta_p^m\rangle\subseteq C_1$ im Widerspruch zu $C_1\cap\langle w\rangle = 1$; wäre aber $p|m$, so wäre $z^{m/p}\in C_p(K(\zeta_4)/K) = K^\times$ wegen Lemma 2 und $W_p\cap K(\zeta_4) = 1$, was der Minimalität von m widerspräche. Damit ist auch die Bedingung A von Satz 1 nachgewiesen. □

Lemma 12. *Unter den Voraussetzungen von Satz* 5 *sei* $[L:K] = (C^n : K^{\times n})$. *Dann gilt:*

(a) $W_{n_2'}\cap L\subset K$.

(b) *Entweder* $W_{2^{a_2}}\cap L\subset K$ *oder*

$$\zeta_4\notin K, \quad W_{2^{a_2}}\cap L\subseteq K(\zeta_4)\cap C \text{ und } \quad \omega(a_2, K)\in C.$$

(c) $W_{n_2}\cap L\subseteq C$.

(d) $C_n(L/K) = \langle C, W_{n_1}\cap L\rangle$.

Beweis. (a) Ich werde zeigen:

(*) Sei $p|n_2$ eine Primzahl, $n_2 = p^{a_p}\cdot m$ mit $p\nmid m$; im Falle $p=2$ sei $\zeta_4\in K$. Ist dann $L\cap W_{p^{a_p}}\notin K$, so ist $[L:K]\neq (C_n(L/K)^n : K^{\times n})$.

Sei dazu $a \geqslant 1$ maximal mit $\zeta_{p^a} \in K$; dann ist $a < a_p$, und ich setze $K_1 = K(\zeta_{p^{a+1}}) \subseteq L$. Wäre $[L:K] = \big(C_n(L/K)^n : K^{\times n}\big)$, so wäre nach Lemma 7 auch $\big(C_n(K_1/K)^n : K^{\times n}\big) = [K_1 : K] = p$; nach den Lemmata 5, 2 und 3(b) gilt aber

$$\big(C_n(K_1/K)^n : K^{\times n}\big) = \big(C_{p^{a_p}}(K_1/K)^{p^{a_p}} : K^{\times p^{a_p}}\big) = 1,$$

was einen Widerspruch ergibt.

(b) Nach Lemma 7 ist $\big(C_n\big(L/K(\zeta_4)\big)^n : K(\zeta_4)^{\times n}\big) = [L : K(\zeta_4)]$, daraus folgt mit $(*)$

$$W_{2^{a_2}} \cap L \subset K(\zeta_4),$$

und ich kann $W_{2^{a_2}} \cap L \not\subset K$, $\zeta_4 \notin K$ annehmen. Nach Lemma 7 und Lemma 5 ist

$$2 = [K(\zeta_4) : K] = \big(C^n \cap K(\zeta_4)^{\times n} : K^{\times n}\big) = \big(C_2^{2^{a_2}} : K^{\times 2^{a_2}}\big)$$

mit

$$C_2 = \{x \in K(\zeta_4) \mid x^n \in C^n,\ x^{2^{a_2}} \in K\}.$$

Nach Lemma 4 ist $\omega = \omega(a_2, K) \in C_2$, also $\omega^n = y^n$ mit $y \in C$, und daraus folgt $\omega = \xi y$ mit $\xi^n = 1$. Wegen $\omega^{2^{a_2}} \in K$ kann ich ohne Einschränkung $\xi^{2^{a_2}} = 1$ annehmen, erhalte zunächst $\xi \in W_{2^{a_2}} \cap L \subset K(\zeta_4)$ und dann (wieder mit Lemma 4) $\xi \in \langle \omega^{1-\sigma} \rangle$, wobei $\sigma = (\zeta_4 \mapsto \zeta_4^{-1})$. Es gibt daher ein $r \in \mathbf{Z}$ mit $\xi = \omega^{r(1-\sigma)} = \omega^{2r} \cdot N\omega^{-1}$, also

$$y = \xi^{-1}\omega = \omega^{1-2r} \cdot N\omega,$$

woraus $\langle K^\times, \omega \rangle = \langle K^\times, y \rangle$ und damit $\omega \in C$ folgt. Für den Beweis von $W_{2^{a_2}} \cap L \subset C$ beachte man

$$W_{2^{a_2}} \cap L = W_{2^{a_2}} \cap K(\zeta_4) \subseteq C_{2^{a_2}}\big(K(\zeta_4)/K\big) = \langle K^\times, \omega \rangle \subseteq C.$$

(c) folgt unmittelbar aus (a) und (b), wenn man nur

$$W_{n_2} \cap L = (W_{2^{a_2}} \cap L) \times (W_{n_2'} \cap L)$$

beachtet.

(d) Sei $x \in C_n(L/K)$; nach Voraussetzung ist $C_n(L/K)^n = C^n$, also $x^n = y^n$ mit $y \in C$ und $x = \xi y$ mit $\xi \in W_n \cap L$. Schreibt man nun $\xi = \xi_1\xi_2$ mit $\xi_1 \in W_{n_1} \cap L$ und $\xi_2 \in W_{n_2} \cap L \subseteq C$ (nach (b)), so folgt die Behauptung. □

Beweis von Satz 5. (a) I, II *und* III *sind hinreichend.* Seien T_0 und T_1 Untergruppen von T mit $\langle K^\times, w \rangle \subseteq T_0$, $K^\times \subseteq T_1$, $T/K^\times = T_0/K^\times \times T_1/K^\times$ und $\big(n_2, (T_0 : K^\times)\big) = 1$; ich setze $C_0 = \langle T_1, C_1 \rangle$ und erhalte

$$C/K^\times = T_0/K^\times \times C_0/K^\times.$$

$T_0/K^\times$ hat insbesondere ungerade Ordnung, und daher ist $\omega \in C_0$, falls $\omega \in C$. C_0 erfüllt die Voraussetzungen von Lemma 11, also folgt

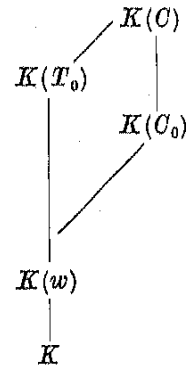
$$[K(C_0) : K] = (C_0^n : K^{\times n}).$$

Auf die Erweiterung $K(T_0)/K$ wende ich Satz 3 an; wegen $\big(n_2, (T_0 : K)\big) = 1$ ist $T_0^{n_1} \subset K$, ferner gilt $W_{n_1} \cap K = 1$ und $T_0 \cap W_{n_1} = \langle w \rangle$, und damit folgt

$$[K(T_0) : K(w)] = (T_0^{n_1} : K^{\times n_1}) = (T_0^n : K^{\times n}),$$

da $T_0^{n_1} \cap W_{n_2} \subseteq K^\times \cap W_{n_2} \subseteq K^{\times n_1}$, also $T_0^{n_1} \cap W_{n_2} = K^{\times n_1} \cap W_{n_2}$. Nach Lemma 10 ist schließlich

$$(C^n : K^{\times n}) = (T_0^n : K^{\times n}) \cdot (C_0^n : K^{\times n}) = [K(T_0) : K(w)] \cdot [K(C_0) : K].$$



Nach Voraussetzung ist $w \in K(C_1) \subseteq K(C_0)$. Beachtet man noch $L = K(C_0, T_0)$, so folgt:

$$\begin{aligned}[L : K] &= [K(C_0, T_0) : K(C_0)] \cdot [K(C_0) : K] \\ &\leqslant [K(T_0) : K(w)] \cdot [K(C_0) : K] = (C^n : K^{\times n});\end{aligned}$$

nach Satz 2 ist $(C^n : K^{\times n}) \mid [L : K]$, also folgt $(C^n : K^{\times n}) = [L : K]$. □

(b) I′, II *und* III *sind notwendig.* Die Notwendigkeit von II und III folgt aus Lemma 12. Seien also II und III erfüllt, und sei $[L : K] = (C^n : K^{\times n})$; seien C_1 und T Untergruppen von C mit $K^\times \subseteq C_1$, $\langle K^\times, w \rangle \subseteq T$ derart, daß $C/K^\times = T/K^\times \times C_1/K^\times$ und $\big(n_2, (T : K^\times)\big) = 1$. Setzt man nun

$$C_0 = C_1 \cap K(w),$$

so genügt es, $K(w) = K(C_0)$ zu zeigen, denn dann ist $w \in K(C_0) \subseteq K(C_1)$.

Nach Lemma 7 ist $[K(w) : K] = \big(C_n\big(K(w)/K\big)^n : K^{\times n}\big)$, nach dem Korollar zu Lemma 9 ist $\big(C_{n_1}\big(K(w)/K\big)^{n_1} : K^{\times n_1}\big) = 1$, also folgt mit Lemma 5

$$[K(w) : K] = \big(C_{n_2}\big(K(w)/K\big)^{n_2} : K^{\times n_2}\big).$$

In gleicher Weise erhält man

$$(C_0^n : K^{\times n}) = (C_{0(n_2)}^{n_2} : K^{\times n_2}),$$

und es genügt nun, $C_{0(n_2)} = C_{n_2}(K(w)/K)$ zu beweisen, denn dann ist $(C_0^n : K^{\times n}) = [K(w) : K]$, und aus Lemma 7 folgt $K(w) = K(C_0)$.

Offensichtlich ist $C_{0(n_2)} \subseteq C_{n_2}(K(w)/K)$. Sei nun

$$x \in C_{n_2}(K(w)/K) = \langle K^\times, C_{n_2}(K(w)/K)^{n_1} \rangle,$$

$x = zx_1^{n_1}$ mit $z \in K^\times$, $x_1 \in C_{n_2}(K(w)/K) \subseteq C_n(L/K) = \langle C, W_{n_1} \cap L \rangle$ (Lemma 12(d)), also $x_1 = x_2 \xi$ mit $x_2 \in C$, $\xi \in W_{n_1} \cap L$. Damit folgt

$$x = zx_2^{n_1} \in \langle K^\times, C^{n_1} \rangle \subseteq C_{(n_2)} \subseteq C_1,$$

da $(T : K^\times)$ zu n_2 prim ist, und ich erhalte

$$x \in (C_1 \cap K(w))_{(n_2)} = C_{0(n_2)};$$

also gilt auch $C_{n_2}(K(w)/K) \subseteq C_{0(n_2)}$. □

Literaturverzeichnis

[1] H. Hasse, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*, J. Reine Angew. Math. 188 (1950), S. 40–64.

[2] M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. 26 (1975), S. 307–308.

[3] S. Lang, *Algebra*, New York 1967.

[4] A. Schinzel, *On linear dependence of roots*, Acta Arith. 28 (1975), S. 161–175.

[5] — *Abelian binomials, power residues and exponential congruences*, ibid. 33 (1977), S. 245–274.

UNIVERSITÄT ESSEN – GESAMTHOCHSCHULE
Essen

Eingegangen am 30. 3. 1977
und in reviedierter Form am 20. 6. 1977 (930)

ACTA ARITHMETICA
XXXVI (1980)

The number of different lengths of irreducible factorization of a natural number in an algebraic number field

by

S. Allen (Milton Keynes)* and P. A. B. Pleasants (Cardiff)

1. Introduction. An integer in an algebraic number field k is *irreducible* if it is not a product of two other integers of k neither of which is a unit (or, equivalently, if it is not a product of two integers of smaller norm). Clearly every integer of k can be expressed as a product of irreducibles, and it is well known that every integer of k has a unique irreducible factorization (apart from the order of the factors and multiplying the factors by units of k) if and only if the class number h of k is 1. This remains true if we restrict attention to the irreducible factorization in k of rational integers only (instead of considering all integers of k). The number of irreducibles in such a factorization (counting each as many times as it occurs) is called the *length* of the factorization, and L. Carlitz [4] has pointed out the interesting fact that a necessary and sufficient condition for no integer of k to have irreducible factorizations of different lengths is that $h \leqslant 2$. Again, this remains true if we restrict attention to the lengths of irreducible factorizations in k of rational integers.

Let $f(m) = f_k(m)$ be the number of essentially different irreducible factorizations in k of the rational integer m, and let $g(m) = g_k(m)$ be the number of different lengths of irreducible factorizations of m in k. If $\varphi(m)$ is an arithmetic function then a function $\psi(m)$ is an *average order* for it if

$$\sum_{m \leqslant x} \varphi(m) \sim \sum_{m \leqslant x} \psi(m)$$

and is a *normal order* for it if, for every positive ε and x,

$$(1-\varepsilon)\psi(m) < \varphi(m) < (1+\varepsilon)\psi(m)$$

for all except $o_\varepsilon(x)$ of the positive integers less than x. In a conversation with W. Narkiewicz in 1965 P. Turán asked whether the functions $f(m)$

* This author was in receipt of financial support from the Science Research Council during the period in which the initial work for this paper was carried out.