ACTA ARITHMETICA
XXXIX (1981)

Große Faktoren in der Klassengruppe algebraischer Zahlkörper

von

Franz Halter-Koch (Essen)

Es ist unbekannt, ob man eine gegebene endliche abelsche Gruppe G als Divisorenklassengruppe eines algebraischen Zahlkörpers realisieren kann; man weiß ja nicht einmal, ob jede natürliche Zahl h als Klassenzahl auftritt. Dagegen ist es recht einfach, algebraische Zahlkörper K zu konstruieren, deren Divisorenklassengruppe einen zu G isomorphen Faktor besitzt; nach Uchida [12] kann man dabei sogar $[K:\mathbf{Q}] \leqslant 2\cdot(|G|-1)!$ erreichen. Schwierig wird das Problem erst wieder, wenn man den Körpergrad $n = [K:\mathbf{Q}]$ vorschreibt; abgesehen von speziellen Resultaten über quadratische Zahlkörper kennt man hier nur den folgenden Satz von Madan [7]: Zu jeder endlichen abelschen Gruppe $\mathfrak{G}$ vom Exponenten n gibt es unendlich viele galois'sche und unendlich viele nicht-galois'sche Zahlkörper K vom Grad n, deren Klassengruppe $\mathfrak{G}$ als Faktor besitzt.

In diesem Zusammenhang stellt sich die Frage, ob man gewissen algebraischen Zahlkörpern K große Faktoren ihrer Divisorenklassengruppe direkt „ansehen" kann; das klassische Beispiel hierfür ist die Geschlechtertheorie quadratischer Zahlkörper, die es gestattet, aus der Anzahl der Diskriminantenprimteiler auf große elementarabelsche 2-Gruppen in der Divisorenklassengruppe zu schließen. Ein ähnliches Resultat liefert die Geschlechtertheorie für alle galois'schen Zahlkörper K (vgl. [3]): ist t die Anzahl der in K verzweigten Primzahlen, so besitzt die Klassengruppe von K einen Faktor vom Typ $(n_1, \ldots, n_{t-\delta})$ mit $1 \neq n_i \mid [K:\mathbf{Q}]$ und einer nur von $\mathrm{Gal}(K/\mathbf{Q})$ abhängigen Zahl $\delta \geqslant 1$. Für beliebige algebraische Zahlkörper liefert der Satz von Brumer–Roquette–Zassenhaus [8] ein analoges Resultat: Ist l eine Primzahl und t die Anzahl derjenigen Primzahlen, deren sämtliche Primfaktoren in K eine durch l teilbare Verzweigungsordnung besitzen, so hat die Klassengruppe von K einen l-Rang $r_l \geqslant t-2\cdot([K:\mathbf{Q}]-1)$. Dieser Satz gestattet es, algebraische Zahlkörper K zu konstruieren, deren Klassengruppe für jeden Primteiler $l \mid [K:\mathbf{Q}]$ beliebig hohen l-Rang besitzt, erlaubt aber keine Aussagen

über den l-Rang der Klassengruppe für $l \nmid [K:\mathbf{Q}]$; Connell und Sussmann [2] verallgemeinerten den Satz auf Relativerweiterung K/k.

In der vorliegenden Arbeit gebe ich zunächst eine weitere Verallgemeinerung des Satzes von Brumer–Roquette–Zassenhaus und hierfür einen auch gegenüber [2] vereinfachten Beweis; daraus folgere ich dann das Resultat von Madan und diskutiere das Analogon im (wesentlich einfacheren) Funktionenkörperfall. Im zweiten Abschnitt konstruiere ich zu gegebenem $n \geqslant 3$ und zu jeder Primzahl l außerhalb einer endlichen (von n abhängigen) Ausnahmemenge unendlich viele algebraische Zahlkörper K vom Grade n derart, daß die Klassengruppe von $K(\zeta_l)$ eine elementar-abelsche l-Faktorgruppe vom Rang $n-1$ besitzt (mit K hat auch $K(\zeta_l)$ zu l teilerfremden Grad über $\mathbf{Q}$).

Für einen algebraischen Zahlkörper K sei $\mathfrak{D}_K$ die Divisorengruppe, $\mathfrak{H}_K$ die Gruppe der Hauptdivisoren, $\mathfrak{C}_K = \mathfrak{D}_K/\mathfrak{H}_K$ die Divisorenklassengruppe, $h_K = |\mathfrak{C}_K|$ die Klassenzahl, E_K die Einheitengruppe, $W_{K,d}$ die Gruppe der d-ten Einheitswurzeln und r_K die Anzahl der archimedischen Stellen von K. Für eine Primzahl p sei v_p die zu $v_p(p) = 1$ normierte Exponentenbewertung zu p.

1. Verallgemeinerung des Satzes von Brumer–Roquette–Zassenhaus. Sei K/k eine endliche Erweiterung algebraischer Zahlkörper, seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ $(t \geqslant 1)$ Primdivisoren von k, seien $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_t \in \mathfrak{D}_K$ und $e_1, \ldots, e_t \in \mathbf{N}$ mit $\mathfrak{Q}_j^{e_j} = \mathfrak{p}_j^{\mathfrak{f}}$ für $j = 1, \ldots, t$. Sei

$$\mathfrak{D}_0 = \langle \mathfrak{Q}_1, \ldots, \mathfrak{Q}_t \rangle \subset \mathfrak{D}_K$$

die von $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_t$ erzeugte Untergruppe von $\mathfrak{D}_K$, und sei $d \in \mathbf{N}$ mit $\mathfrak{Q}_j^d \in \mathfrak{H}_k$ für alle $j = 1, \ldots, t$ (dann ist $e_j \mid d$ für alle j).

Für $(a) \in \mathfrak{D}_0 \cap \mathfrak{H}_K$ ist $(a^d) \in \mathfrak{H}_k$, also

$$a^d = x\varepsilon \tag{0}$$

mit $x \in k^\times$, $\varepsilon \in E_K$, und es gilt:

Lemma 1. *Die durch* (0) *gegebene Zuordnung* $(a) \mapsto \varepsilon$ *definiert einen Homomorphismus*

$$\varphi\colon \mathfrak{D}_0 \cap \mathfrak{H}_K/\mathfrak{D}_0 \cap \mathfrak{H}_k \to E_K/E_K^d \cdot E_k$$

mit

$$\mathrm{Kern}(\varphi) = \{(a) \in \mathfrak{D}_0 \mid a \in K^\times, a^d \in k\}/\mathfrak{D}_0 \cap \mathfrak{H}_k.$$

Beweis. Ich zeige zunächst, daß $(a) \mapsto \varepsilon$ eine Abbildung $\mathfrak{D}_0 \cap \mathfrak{H}_K/\mathfrak{D}_0 \cap \mathfrak{H}_k \to E_K/E_K^d \cdot E_k$ definiert: Seien dazu $a, a' \in K^\times$ mit $[(a)] = [(a')] \in \mathfrak{D}_0 \cap \mathfrak{H}_K/\mathfrak{D}_0 \cap \mathfrak{H}_k$, und sei $a^d = x\varepsilon$, $a'^d = x'\varepsilon'$ mit $x, x' \in k^\times$, $\varepsilon, \varepsilon' \in E_K$; ich habe dann $\varepsilon\varepsilon'^{-1} \in E_K^d \cdot E_k$ zu zeigen. Wegen $[(a)] = [(a')]$ ist $(a) = (a') \cdot (a)$ mit $a \in k^\times$, also $a = a'a\eta$ mit $\eta \in E_K$, und daraus folgt $\varepsilon\varepsilon'^{-1} = \eta^d \cdot (x'x^{-1}a^d)$; nun ist aber $x'x^{-1}a^d = \varepsilon\varepsilon'^{-1}\eta^{-d} \in E_K \cap k^\times$, also $x'x^{-1}a^d \in E_k$ und daher $\varepsilon\varepsilon'^{-1} \in E_K^d E_k$.

φ ist offensichtlich ein Homomorphismus und aus $a \in K^\times$, $a^d \in k$, $(a) \in \mathfrak{D}_0$ folgt $(a) \in \mathrm{Kern}(\varphi)$. Sei umgekehrt $(\beta) \in \mathrm{Kern}(\varphi)$; dann ist $\beta^d = x\varepsilon^d\varepsilon_0$ mit $x \in K^\times$, $\varepsilon \in E_K$, $\varepsilon_0 \in E_k$, und für $a = \beta\varepsilon^{-1} \in K^\times$ gilt $a^d \in k$ und $(\beta) = (a)$. ∎

Sei nun

$$X = \{a \in K^\times \mid (a) \in \mathfrak{D}_0, a^d \in k\};$$

dann ist X eine Untergruppe der d-Radikalgruppe von K/k, und ich erhalte:

Satz 1. (a) *Ist* $h_0 = (\mathfrak{D}_0 \cap \mathfrak{D}_k : \mathfrak{D}_0 \cap \mathfrak{H}_k)$ *die Anzahl der von* $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ *erzeugten Divisorenklassen von* k, *so gilt für die Anzahl* $(\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{H}_K)$ *der von* $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_t$ *erzeugten Divisorenklassen von* K:

$$\frac{h_0 \prod_{j=1}^{t} e_j}{(X^d : X^d \cap k^{\times d}) \cdot |\mathrm{Bild}(\varphi)|} \Big| (\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{H}_K);$$

ist $k = \mathbf{Q}$ *und entweder* $W_{K,2} = W_{K,4}$ *oder* d *ungerade, so gilt*

$$(\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{H}_K) = \frac{h_0 \prod_{j=1}^{t} e_j}{(X^d : X^d \cap k^{\times d}) \cdot |\mathrm{Bild}(\varphi)|}.$$

(b) $$(X^d : X^d \cap k^{\times d}) \mid [k(X) : k] \mid [K : k].$$

(c) $$|\mathrm{Bild}(\varphi)| \Big| \frac{d^{r_K - r_k}}{(\mathcal{N}_{K/k} E_K : E_k^{\tilde{d}} \cap \mathcal{N}_{K/k} E_K)} \cdot \delta_{K/k,d}$$

mit $\tilde{d} = \mathrm{ggT}(d, [K:k])$ *und*

$$\delta_{K/k,d} = \begin{cases} |W_{K,d} \cap K^{\times d} k^\times|, & \text{falls} \quad W_{k,d} = 1, \\ (W_{K,d} : W_{k,d}), & \text{falls} \quad W_{k,d} \neq 1. \end{cases}$$

Beweis. (a) Es ist

$$(\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{H}_K) = \frac{(\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{D}_k) \cdot (\mathfrak{D}_0 \cap \mathfrak{D}_k : \mathfrak{D}_0 \cap \mathfrak{H}_k)}{(\mathfrak{D}_0 \cap \mathfrak{H}_K : \mathfrak{D}_0 \cap \mathfrak{H}_k)} = \frac{h_0 \prod_{j=1}^{t} e_j}{|\mathrm{Kern}(\varphi)| \cdot |\mathrm{Bild}(\varphi)|};$$

daher genügt es zu zeigen:

$$|\mathrm{Kern}(\varphi)| \mid (X^d : X^d \cap k^{\times d})$$

mit Gleichheit in den angegebenen Fällen. Dazu betrachte ich den durch $a \mapsto [(a)]$ definierten Epimorphismus

$$\psi\colon X \to \mathrm{Kern}(\varphi).$$

Offensichtlich ist $X \cap k^\times \cdot W_{K,d} \subseteq \mathrm{Kern}(\psi)$, ψ induziert also einen Epimorphismus

$$\psi_0 \colon X/X \cap k^\times \cdot W_{K,d} \to \mathrm{Kern}(\varphi).$$

Anderseits liefert aber Potenzieren mit d einen Isomorphismus

$$X/X \cap k^\times \cdot W_{K,d} \simeq X^d/X^d \cap k^{\times d},$$

woraus $|\mathrm{Kern}(\varphi)| \,|\, (X^d : X^d \cap k^{\times d})$ folgt. Sei nun $k = \boldsymbol{Q}$ und entweder $W_{K,2} = W_{K,4}$ oder d ungerade; dann habe ich

$$\mathrm{Kern}(\psi) = X \cap \boldsymbol{Q}^\times \cdot W_{K,d}$$

zu zeigen. Ist $a \in \mathrm{Kern}(\psi)$, so ist $(a) \in \mathfrak{H}_{\boldsymbol{Q}}$, also $a = a\varepsilon$ mit $a \in \boldsymbol{Q}^\times$, $\varepsilon \in E_K$ und $\alpha^d = a^d \varepsilon^d \in \boldsymbol{Q}$, woraus $\varepsilon^d \in \boldsymbol{Q}$, also $\varepsilon^d = \pm 1$ und $\varepsilon \in W_{K,2d}$ folgt. Ist nun d ungerade, so ist $\boldsymbol{Q}^\times \cdot W_{K,d} = \boldsymbol{Q}^\times \cdot W_{K,2d}$; ist d gerade und $W_{K,2} = W_{K,4}$, so ist $W_{K,2d} = W_{K,d}$.

(b) folgt unmittelbar aus [5], Satz 2.

(c) Es ist

$$\mathrm{Bild}(\varphi) \subseteq E_K \cap K^{\times d} k^\times / E_K^d E_k,$$

und daher ist $|\mathrm{Bild}(\varphi)|$ ein Teiler von

$$(E_K \cap K^{\times d} k^\times : E_K^d E_k) = \frac{(E_K : E_K^d E_k)}{(E_K : E_K \cap K^{\times d} k^\times)}.$$

Nun ist aber $E_K \cap K^{\times d} k^\times \subseteq \{\varepsilon \in E_K \mid \mathcal{N}_{K/k}(\varepsilon) \in E_k^{\tilde{d}}\}$, und im Falle $W_{k,d} = 1$ ist der Index $(\{\varepsilon \in E_K \mid \mathcal{N}_{K/k}(\varepsilon) \in E_k^{\tilde{d}}\} : E_K \cap K^{\times d} k^\times)$ durch $(W_{K,d} : W_{K,d} \cap K^{\times d} k^\times)$ teilbar, woraus nach Definition von $\delta_{K/k,d}$ folgt:

$$\frac{(W_{K,d} : W_{k,d})}{\delta_{K/k,d}} \,\Big|\, \big(\{\varepsilon \in E_K \mid \mathcal{N}_{K/k}(\varepsilon) \in E_k^{\tilde{d}}\} : E_K \cap K^{\times d} k^\times\big).$$

Anderseits ist $E_K/\{\varepsilon \in E_K \mid \mathcal{N}_{K/k}(\varepsilon) \in E_k^{\tilde{d}}\} \simeq \mathcal{N}_{K/k} E_K / E_k^{\tilde{d}} \cap \mathcal{N}_{K/k} E_K$, also insgesamt $(E_K : E_K \cap K^{\times d} k^\times)$ durch

$$\frac{(W_{K,d} : W_{k,d})}{\delta_{K/k,d}} \cdot (\mathcal{N}_{K/k} E_K : E_k^{\tilde{d}} \cap \mathcal{N}_{K/k} E_K)$$

teilbar. Somit gilt: $|\mathrm{Bild}(\varphi)|$ teilt

$$\frac{(E_K : E_K^d E_k) \cdot \delta_{K/k}}{(W_{K,d} : W_{k,d}) \cdot (\mathcal{N}_{K/k} E_K : E_k^{\tilde{d}} \cap \mathcal{N}_{K/k} E_K)},$$

woraus wegen $(E_K : E_K^d E_k) = d^{r_K - r_k} \cdot (W_{K,d} : W_{k,d})$ die Behauptung folgt. ∎

Korollar 1. *Sei K/k eine endliche Erweiterung algebraischer Zahlkörper, l eine Primzahl und t die Anzahl der Primdivisoren $\mathfrak{p}$ von k, für die gilt:*

(a) *Alle Primfaktoren von $\mathfrak{p}$ in K haben durch l teilbare Verzweigungsordnung;*

(b) *die Klasse von $\mathfrak{p}$ hat in der Divisorenklassengruppe von k zu l prime Ordnung.*

Dann ist

$$\dim_{\boldsymbol{F}_l}(\mathfrak{C}_K/\mathfrak{C}_K^l) \geqslant t - \Delta_{K/k}$$

mit

$$\Delta_{K/k} = r_K - r_k + v_l(n_l) + v_l(\delta_{K/k,l}) - \dim_{\boldsymbol{F}_l}(\mathcal{N}_{K/k} E_K : E_k^l \cap \mathcal{N}_{K/k} E_K),$$

$$n_l = [k(\{a \in K \mid a^l \in k\}) : k].$$

Beweis. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ die Primdivisoren von k, die (a) und (b) genügen. Seien $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_t \in \mathfrak{D}_K$ mit $\mathfrak{Q}_j^l = \mathfrak{p}_j$, und sei $d_0 \in \boldsymbol{N}$ mit $l \nmid d_0$ und $\mathfrak{p}_j^{d_0} \in \mathfrak{H}_k$ für alle j. Setzt man nun $\mathfrak{D}_0 = \langle \mathfrak{Q}_1, \ldots, \mathfrak{Q}_t \rangle$ und $d = d_0 l$, so erhält man nach Satz 1 eine Abschätzung für $(\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{H})$ im Teilbarkeitssinne und damit für $v_l(\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{H})$. Setzt man $\mathfrak{C}_0 = \mathfrak{D}_0/\mathfrak{D}_0 \cap \mathfrak{H}$, so ist die l-Sylow-gruppe von $\mathfrak{C}_0$ wegen $l \nmid d_0$ elementar-abelsch, also

$$\dim_{\boldsymbol{F}_l}(\mathfrak{C}_0/\mathfrak{C}_0^l) = v_l(\mathfrak{D}_0 : \mathfrak{D}_0 \cap \mathfrak{H}),$$

und wegen $\mathfrak{C}_0 \subseteq \mathfrak{C}_K$ gilt

$$\dim_{\boldsymbol{F}_l}(\mathfrak{C}_0/\mathfrak{C}_0^l) \leqslant \dim_{\boldsymbol{F}_l}(\mathfrak{C}_K/\mathfrak{C}_K^l),$$

woraus die Behauptung folgt. ∎

Mit einem etwas anderen (und im galois'schen Fall besseren) Wert von $\Delta_{K/k}$ wurde Korollar 1 in [2] bewiesen.

Im Falle $k = \boldsymbol{Q}$ liefert Satz 1 unmittelbar das folgende Resultat:

Korollar 2. *Sei K ein algebraischer Zahlkörper, seien $p_1, \ldots, p_t$ die in K verzweigten Primzahlen,*

$$p_i = \mathfrak{p}_{i,1}^{e_{i,1}} \cdot \ldots \cdot \mathfrak{p}_{i,g_i}^{e_{i,g_i}} \quad \text{in} \quad K,$$

$$e_i = \mathrm{ggT}(e_{i,1}, \ldots, e_{i,g_i}) \quad \text{und} \quad e = \mathrm{kgV}(e_1, \ldots, e_t).$$

Dann gilt:

$$\frac{\prod_{j=1}^{t} e_j}{[K : \boldsymbol{Q}] \cdot e^{r_K}} \,\Big|\, h_K.$$

Satz 2. *Für eine natürliche Zahl N sei*

$$V(N) = \sum_p v_p(N).$$

(Summe über alle Primzahlen p.) Sei K ein algebraischer Zahlkörper, $e \mid [K : \boldsymbol{Q}]$, $\delta(e, K) = V([K : \boldsymbol{Q}] \cdot e^{r_K})$ und t die Anzahl der Primzahlen p,

deren sämtliche Primfaktoren in K durch e teilbare Verzweigungsordnung besitzen. Dann besitzt $\mathfrak{C}_K$ eine Untergruppe vom $(t-\delta(e,K))$-gliedrigen Typ $(e,\dots,e)$.

Beweis. Seien $p_1,\dots,p_t$ die in K verzweigten Primzahlen, deren sämtliche Primfaktoren durch e teilbare Verzweigungsordnung besitzen; seien $\mathfrak{Q}_1,\dots,\mathfrak{Q}_t \in \mathfrak{D}_K$ mit $\mathfrak{Q}_j^e = p_j$, und sei $\mathfrak{D}_0 = \langle \mathfrak{Q}_1,\dots,\mathfrak{Q}_t\rangle$. Dann ist $\mathfrak{D}_0/\mathfrak{D}_0\cap\mathfrak{H}_K$ eine Untergruppe von $\mathfrak{C}_K$ vom Typ $\left(\frac{e}{e_1},\dots,\frac{e}{e_t}\right)$ mit $e_j \mid e$, und nach Satz 1 ist

$$\frac{e^{t-r_K}}{[K:\boldsymbol{Q}]}\,\Big|\,(\mathfrak{D}_0 : \mathfrak{D}_0\cap\mathfrak{H}_K) = \frac{e^t}{\prod_{j=1}^t e_j},$$

also

$$V\Big(\prod_{j=1}^t e_j\Big) = \sum_{j=1}^t V(e_j) \leqslant \delta(e,K).$$

Daher können höchstens $\delta(e,K)$ viele e_j von 1 verschieden sein, woraus die Behauptung folgt. ∎

Korollar (Madan [7]). *Seien $N, r \in \boldsymbol{N}$; dann gibt es unendlich viele galois'sche und, falls $N>2$, auch unendlich viele nicht-galois'sche algebraische Zahlkörper K vom Grad N, deren Divisorenklassengruppe eine Untergruppe vom r-gliedrigen Typ $(N,\dots,N)$ besitzt.*

Beweis. Nach Satz 2 genügt es zu zeigen:

Zu gegebenem $t \in \boldsymbol{N}$ gibt es unendlich viele (galois'sche und nicht-galois'sche) algebraische Zahlkörper vom Grade N, in denen t Primzahlen voll verzweigen.

(a) Seien $p_1,\dots,p_t$ Primzahlen mit $p_j \equiv 1 \bmod 2N$ für alle j (nach dem Dirichlet'schen Satz gibt es unendlich viele solche); seien w_j Primitivwurzeln mod p_j, normiert zu $w_j \equiv 1 \bmod p_i$ für $i \neq j$. Dann definiere ich

$$\chi_0 \colon (\boldsymbol{Z}/p_1\cdot\ldots\cdot p_r\boldsymbol{Z})^* \to \boldsymbol{Z}/N\boldsymbol{Z}$$

durch

$$\chi_0(w_1^{a_1}\cdot\ldots\cdot w_r^{a_r}) = \sum_{i=1}^r a_i + N\boldsymbol{Z};$$

χ_0 induziert einen Idealklassencharakter χ auf $\boldsymbol{Q}$, und der Klassenkörper zu χ ist ein zyklischer Körper N-ten Grades, in dem $p_1,\dots,p_r$ voll verzweigen.

(b) Sind $p_1,\dots,p_t$ beliebige Primzahlen so ist $\boldsymbol{Q}(\sqrt[N]{p_1\cdot\ldots\cdot p_t})$ ein nicht-galois'scher Körper N-ten Grades, in dem $p_1,\dots,p_t$ voll verzweigen. ∎

Im Funktionenkörperfall sind die Verhältnisse wesentlich einfacher. Es gilt:

Satz 1 a. *Sei F/K ein algebraischer Funktionenkörper (einer Variablen) mit genauem Konstantenkörper K, $x \in F\setminus K$, $\mathfrak{p}_0,\dots,\mathfrak{p}_t$ Primdivisoren von $K(x)$ $(t \geqslant 1)$, $\mathfrak{Q}_0,\dots,\mathfrak{Q}_t$ Divisoren von F und $e \in \boldsymbol{N}$ mit $e\mathfrak{Q}_i = \mathfrak{p}_i$ für $i = 0,1,\dots,t$. $\mathfrak{C}_0$ sei die von $\mathfrak{Q}_0-\mathfrak{Q}_1,\dots,\mathfrak{Q}_0-\mathfrak{Q}_t$ erzeugte Untergruppe der Divisorenklassengruppe 0-ten Grades von F. Dann gilt:*

$$\frac{e^t}{e_e(F/K(x))}\,\Big|\,|\mathfrak{C}_0|,$$

wobei

$$e_e(F/K(x)) = \big[K(x)\,(\{z\in F \mid z^e \in K(x)\}) : K(x)\big],\quad e_e(F/K(x)) \mid [F:K(x)].$$

Beweis. Sei $\mathfrak{D}_0$ die von $\mathfrak{Q}_0-\mathfrak{Q}_1,\dots,\mathfrak{Q}_0-\mathfrak{Q}_t$ erzeugte Untergruppe der Gruppe der Divisoren 0-ten Grades von F und $\mathfrak{D}_{K(x)}$ die Divisorengruppe von $K(x)$; dann induziert der kanonische Epimorphismus $\mathfrak{D}_0 \to \mathfrak{C}_0$ eine exakte Sequenz

$$0 \to \mathfrak{K} \to \mathfrak{D}_0/\mathfrak{D}_0\cap\mathfrak{D}_{K(x)} \to \mathfrak{C}_0 \to 0.$$

Ist nun $\mathfrak{A} \in \mathfrak{D}_0$ ein Hauptdivisor, so ist $\mathfrak{A} = (a)$ mit $a \in F^\times$ und $e\cdot\mathfrak{A} = (a^e) \in \mathfrak{D}_{K(x)}$ also $a^e \in K(x)$, und genau dann ist $\mathfrak{A} \in \mathfrak{D}_{K(x)}$, wenn $a \in K(x)$; also definiert $(a)\mapsto a$ einen Monomorphismus

$$\mathfrak{K} \to \{z\in F^\times \mid z^e \in K(x)\}/K(x)^\times$$

(K ist der genaue Konstantenkörper von F!), und Potenzieren mit e liefert $\{z\in F^\times \mid z^e\in K(x)\}/K(x)^\times \simeq F^{\times e}\cap K(x)/K(x)^{\times e}$, also nach [5], Satz 2

$$|\mathfrak{K}| \mid e_e(F/K(x)),$$

woraus die Behauptung folgt. ∎

Mit Hilfe von Satz 1a ist es nun wieder einfach, algebraische Funktionenkörper (mit beliebigem Konstantenkörper) zu konstruieren, deren Divisorenklassengruppe 0-ten Grades eine gegebene endliche abelsche Gruppe als Faktor enthält; insbesondere erhält man damit wieder neue Beweise der Resultate aus [7].

2. Konstruktion algebraischer Zahlkörper vom Grade $n(l-1)$ mit l-Rang $n-1$. Sei K ein algebraischer Zahlkörper, l eine Primzahl, ζ_l eine primitive l-te Einheitswurzel und $\overline{K} = K(\zeta_l)$; ich nenne $\varepsilon_1,\dots,\varepsilon_r \in K$ l-unabhängig (in K), wenn

$$\dim_{\boldsymbol{F}_l}(\langle\varepsilon_1,\dots,\varepsilon_r\rangle\cdot K^{\times l}/K^{\times l}) = r.$$

LEMMA 2. *Seien $\varepsilon_1, \dots, \varepsilon_r$ unabhängige Einheiten von K (d.h., $\langle \varepsilon_1, \dots, \varepsilon_r \rangle \simeq \mathbf{Z}^r$), und seien $\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r}$ fest gewählte l-te Wurzeln in einer algebraischen Hülle von K. Dann sind äquivalent:*

(a) *$\varepsilon_1, \dots, \varepsilon_r$ sind l-unabhängig in K.*

(b) *Die Gruppe $E_K/\langle \varepsilon_1, \dots, \varepsilon_r \rangle$ ist l-torsionsfrei.*

(c) $[K(\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r}) : K] = l^r$.

(d) $[\overline{K}(\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r}) : \overline{K}] = l^r$.

(e) *$\varepsilon_1, \dots, \varepsilon_r$ sind l-unabhängig in $\overline{K}$.*

(f) *Zu jeder endlichen Menge S von Primdivisoren von K gibt es paarweise nichtkonjugierte Primdivisoren 1. Grades $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathfrak{D}_{\overline{K}} \setminus S$ derart, daß gilt: ε_i ist l-ter Potenzrest* mod $\mathfrak{p}_j$ *genau dann, wenn $i \neq j$ $(i, j = 1, \dots, r)$.*

Beweis. (a) ist äquivalent zu (b): Genau dann sind $\varepsilon_1, \dots, \varepsilon_r$ l-abhängig in K, wenn eine Relation der Form $\varepsilon_1^{a_1} \cdot \ldots \cdot \varepsilon_r^{a_r} = x^l$ mit $a_1, \dots, a_r \in \mathbf{Z}$, nicht alle durch l teilbar, und $x \in K^\times$ besteht; dann besteht aber eine solche Relation auch mit $x \in E_K$, und das heißt, daß $E_K/\langle \varepsilon_1, \dots, \varepsilon_r \rangle$ l-Torsion besitzt.

Aus (b) folgt (c): Offensichtlich ist

$$[K(\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r}) : K] \leqslant \prod_{i=1}^{r} [K(\sqrt[l]{\varepsilon_i}) : K] \leqslant l^r;$$

setzt man nun $\Delta = \langle K^\times, \sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r} \rangle$, so ist $K(\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r}) = K(\Delta)$, $\Delta^l \subseteq K^\times$ und $(\Delta^l : K^{\times l}) = (\langle \varepsilon_1, \dots, \varepsilon_r \rangle \cdot K^{\times l} : K^{\times l}) = l^r$; nach [5], Satz 1, ist aber $(\Delta^l : K^{\times l})$ ein Teiler von $[K(\Delta) : K]$ und daraus folgt die Behauptung.

Aus (c) folgt (d): $\overline{K}/K$ ist eine galois'sche Erweiterung von zu l teilerfremdem Grad, und $\overline{K}(\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r}) = \overline{K} \cdot K(\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r})$, woraus die Behauptung folgt.

Aus (d) folgt (e): siehe [6], T. Ia, Satz 7.

Trivialerweise folgen (a) aus (c) und (e) aus (f); nach [6], T. Ia, Satz 11 folgt aber auch (f) aus (e). ∎

SATZ 3. *Sei K ein algebraischer Zahlkörper, und seien $\varepsilon_1, \dots, \varepsilon_r$ l-unabhängige Einheiten von K; sei*

$$[K : \mathbf{Q}] = n \not\equiv 0 \bmod l$$

und

$$\varepsilon_i^n \equiv 1 \bmod l^l \quad (i = 1, \dots, r).$$

Dann hat die Divisorenklassengruppe von $\overline{K}$ mindestens den l-Rang r:

$$\dim_{\mathbf{F}_l}(\mathfrak{C}_{\overline{K}}/\mathfrak{C}_{\overline{K}}^l) \geqslant r.$$

Beweis. Nach dem Hauptsatz der Klassenkörpertheorie genügt es zu zeigen:

$$\overline{K}(\sqrt[l]{\varepsilon_1}, \dots, \sqrt[l]{\varepsilon_r})/\overline{K}$$

ist eine unverzweigte, elementar-abelsche l-Erweiterung vom Grad l^r, und wegen Lemma 2 genügt es, die Erweiterungen $\overline{K}(\sqrt[l]{\varepsilon_i})/\overline{K}$ als unverzweigt nachzuweisen. Nach [6], T. Ia, Satz 9, habe ich zu zeigen: Ist $\mathfrak{L}$ ein Primteiler von l in $\overline{K}$ mit Verzweigungsordnung $e(\mathfrak{L}|l) = e_0(l-1)$, so ist ε_i l-ter Potenzrest mod $\mathfrak{L}^{e_0 l}$ in $\overline{K}$; nun ist aber $\mathfrak{L}^{e_0 l} | l^l$ und $\varepsilon_i \in K$, also genügt es, ε_i als l-ten Potenzrest mod l^l in K nachzuweisen. Wegen $(n, l) = 1$ gibt es $d, t \in \mathbf{Z}$ mit $nt = 1 + dl$ und es folgt

$$\varepsilon_i^{nt} = \varepsilon_i \varepsilon_i^{dl} \equiv 1 \bmod l^l;$$

ε_i ist l-ter Potenzrest mod l^l. ∎

Um die Voraussetzungen von Satz 3 zu realisieren, benutze ich die in [1] und [4] durchgeführten Konstruktionen; dazu sind zunächst die Resultate aus [4] in geeigneter Weise zu verschärfen.

DEFINITION. Seien $r_1, r_2 \geqslant 0$, $n = r_1 + 2r_2 \geqslant 3$. Ein ganzzahliges Polynom $f(X) \in \mathbf{Z}[X]$ heiße *erzeugendes Polynom vom Typ (r_1, r_2)*, wenn gilt:

$$f(X) = \prod_{i=1}^{n} (X - d_i) - d$$

mit $d, d_1, \dots, d_{r_1} \in \mathbf{Z}$, $d_1 > d_2 > \dots > d_{r_1}$, $d \neq 0$, ganzen imaginärquadratischen Zahlen $d_{r_1+1}, \dots, d_{r_1+r_2}$ und deren Konjugiert-Komplexen $d_{r_1+r_2+j} = \overline{d_{r_1+j}}$ $(j = 1, \dots, r_2)$ derart, daß für alle $i, j = 1, \dots, n$ gilt:

$$|d_i - d_j| \geqslant 2, \qquad d \,|\, d_i - d_j;$$

im Falle $r_1 = 3$, $r_2 = 0$, $|d| = 2$ sei ferner $d_1 - d_3 \geqslant 6$.

SATZ 4. *Sei $f(X) = \prod_{i=1}^{n} (X - d_i) - d \in \mathbf{Z}[X]$ ein erzeugendes Polynom vom Typ (r_1, r_2). Dann ist $f(X)$ irreduzibel; sei $f(\omega) = 0$ und $K = \mathbf{Q}(\omega)$. Für $i = 1, \dots, n$ sei*

$$\tilde{\varepsilon}_i = \begin{cases} \dfrac{(\omega - d_i)^n}{d}, & \text{falls} \quad |d| > 1, \\[2ex] \dfrac{\omega - d_i}{d}, & \text{falls} \quad |d| = 1; \end{cases}$$

für $i = 1, \dots, r_1 + r_2$ *sei*

$$\varepsilon_i = \begin{cases} \tilde{\varepsilon}_i, & \text{falls} \quad i = 1, \dots, r_1, \\ \tilde{\varepsilon}_i \tilde{\varepsilon}_{i+r_2}, & \text{falls} \quad i = r_1+1, \dots, r_1+r_2. \end{cases}$$

Dann gilt:

$\tilde{\varepsilon}_1, \dots, \tilde{\varepsilon}_n$ *sind Einheiten von* $K(d_{r_1+1}, \dots, d_{r_1+r_2})$ *mit* $\prod_{i=1}^{n} \tilde{\varepsilon}_i = 1$, *und jedes* $(n-1)$*-gliedrige Teilsystem von* $\tilde{\varepsilon}_1, \dots, \tilde{\varepsilon}_n$ *ist ein unabhängiges Einheitensystem.*

$\varepsilon_1, \dots, \varepsilon_{r_1+r_2}$ *sind Einheiten von* K *mit* $\prod_{i=1}^{r_1+r_2} \varepsilon_i = 1$, *und jedes* (r_1+r_2-1)*-gliedrige Teilsystem von* $\varepsilon_1, \dots, \varepsilon_{r_1+r_2}$ *ist ein unabhängiges Einheitensystem.*

Bemerkung. Satz 4 ist insofern eine Verschärfung von [4], Satz 2, als dort die Irreduzibilität des erzeugenden Polynoms nicht gezeigt, sondern vorausgesetzt wurde. Ein Irreduzibilitätsbeweis wurde bisher nur im Falle $r_2 = 0$ unter schärferen Voraussetzungen im Rahmen der Theorie des Jacobi–Perron'schen Algorithmus geführt (siehe [1]). Die Einbeziehung des Körpers $K(d_{r_1+1}, \dots, d_{r_1+r_2})$ hat rein technische Bedeutung und wird sich im folgenden als nützlich erweisen.

Der Irreduzibilitätsbeweis beruht auf dem folgenden Hilfssatz, den ich dem Beweis des Satzes voranstelle.

Lemma 3. *Sei* $f(X) \in \boldsymbol{Q}[X]$, *seien* $\omega^{(1)}, \dots, \omega^{(r_1)} \in \boldsymbol{R}$ *die reellen Nullstellen von* $f(X)$ *und* $\omega^{(r_1+1)}, \overline{\omega^{(r_1+1)}}, \dots, \omega^{(r_1+r_2)}, \overline{\omega^{(r_1+r_2)}} \in \boldsymbol{C}$ *die Paare konjugiert-komplexer Nullstellen von* $f(X)$. *Seien* $g_1, \dots, g_{r_1+r_2} \in \boldsymbol{Q}(X)$ *rationale Funktionen derart, daß gilt: die Zahlen*

$$g_i(\omega^{(j)}) \qquad (i, j = 1, \dots, r_1+r_2)$$

sind von Null verschiedene ganzalgebraische Zahlen, und für $i \neq j$ *ist*

$$|g_i(\omega^{(j)})| < 1.$$

Dann ist $f(X)$ *irreduzibel über* $\boldsymbol{Q}$.

Beweis. Wäre $f(X)$ reduzibel, so gäbe es eine echte Teilmenge $I \subset \{1, \dots, r_1+r_2\}$ derart, daß

$$\Omega = \{\omega^{(j)} \mid j \in I\} \cup \{\overline{\omega^{(j)}} \mid j \in I,\ r_1+1 \leqslant j \leqslant r_1+r_2\}$$

ein volles Konjugiertensystem algebraischer Zahlen ist. Sei nun $i \in \{1, \dots, r_1+r_2\} \setminus I$; dann ist $\{g_i(\xi) \mid \xi \in \Omega\}$ ein volles Konjugiertensystem ganzer algebraischer Zahlen, also $\prod_{\xi \in \Omega} g_i(\xi) \in \boldsymbol{Z}$; anderseits ist aber

$$0 < \prod_{\xi \in \Omega} |g_i(\xi)| < 1,$$

ein Widerspruch. ∎

Beweis von Satz 4. Nach [4], Satz 1, hat $f(X)$ in $\boldsymbol{C}$ genau r_1 reelle Nullstellen $\omega^{(1)}, \dots, \omega^{(r_1)}$ und r_2 Paare konjugiert-komplexer Nullstellen

$$\omega^{(r_1+1)}, \omega^{(r_1+r_2+1)} = \overline{\omega^{(r_1+1)}}, \dots, \omega^{(r_1+r_2)}, \omega^{(r_1+2r_2)} = \overline{\omega^{(r_1+r_2)}},$$

die alle der Bedingung

$$|\omega^{(i)} - d_i| < \tfrac{1}{2} \qquad (i = 1, \dots, n)$$

genügen. Für $i, j = 1, \dots, n$ setze ich nun

$$\tilde{\varepsilon}_i^{(j)} = \begin{cases} \dfrac{(\omega^{(j)} - d_i)^n}{d}, & \text{falls} \quad |d| > 1, \\ \dfrac{\omega^{(j)} - d_i}{d}, & \text{falls} \quad |d| = 1; \end{cases}$$

aus der Gestalt des erzeugenden Polynoms folgt $(\omega^{(j)} - d_i)^n \equiv 0 \bmod |d|$ und $\prod_{i=1}^{n} \tilde{\varepsilon}_i^{(j)} = 1$, also sind die $\tilde{\varepsilon}_i^{(j)}$ algebraische Einheiten, und für $i \neq j$ ist

$$(\tilde{*}) \qquad |\tilde{\varepsilon}_i^{(j)}| > 1.$$

Für $i, j = 1, \dots, r_2$ sei nun

$$\varepsilon_i^{(j)} = \begin{cases} \tilde{\varepsilon}_i^{(j)}, & \text{falls} \quad i = 1, \dots, r_1, \\ \tilde{\varepsilon}_i^{(j)} \tilde{\varepsilon}_{i+r_2}^{(j)}, & \text{falls} \quad i = r_1+1, \dots, r_1+r_2; \end{cases}$$

dann sind auch die $\varepsilon_i^{(j)}$ algebraische Einheiten mit $\prod_{i=1}^{r_1+r_2} \varepsilon_i^{(j)} = 1$, und für $i \neq j$ ist

$$(*) \qquad |\varepsilon_i^{(j)}| > 1.$$

Nun hat man aber im Falle $|d| > 1$

$$\frac{1}{\varepsilon_i^{(j)}} = \begin{cases} \dfrac{d}{(\omega^{(j)} - \overline{d_i})^n}, & \text{falls} \quad i = 1, \dots, r_1, \\ \dfrac{d^2}{[(\omega^{(j)} - d_i)(\omega^{(j)} - \overline{d_i})]^n}, & \text{falls} \quad i = r_1+1, \dots, r_1+r_2 \end{cases}$$

und im Falle $|d| = 1$

$$\frac{1}{\varepsilon_i^{(j)}} = \begin{cases} \dfrac{d}{(\omega^{(j)} - \overline{d_i})}, & \text{falls} \quad i = 1, \dots, r_1, \\ \dfrac{d}{(\omega^{(j)} - d_i)(\omega^{(j)} - \overline{d_i})}, & \text{falls} \quad i = r_1+1, \dots, r_1+r_2. \end{cases}$$

Also gilt in jedem Falle

$$\frac{1}{\varepsilon_i^{(j)}} = g_i(\omega^{(j)})$$

mit $g_i \in \boldsymbol{Q}(X)$; wegen (*) sind die Voraussetzungen von Lemma 3 erfüllt, $f(X)$ ist irreduzibel. Die $\varepsilon_i^{(j)}, \tilde{\varepsilon}_i^{(j)}$ sind gerade die Konjugierten der im Satz definierten $\varepsilon_i, \tilde{\varepsilon}_i$, und aus (*), (~) folgen wie in [4] die Behauptungen des Satzes. ∎

LEMMA 4. *Sei* $f(X) = \prod_{i=1}^{n}(X-d_i)-d$ *ein erzeugendes Polynom vom Typ* (r_1, r_2), *und seien* $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_n$ *wie in Satz 4 definiert. Für eine Primzahl* l *sei* $d_i - d_j \equiv 0 \bmod l^l$ *für alle* $i, j = 1, \ldots, n$; *im Falle* $|d| = 1$ *sei* $d^{n-1} \equiv 1 \bmod l^l$, *im Falle* $|d| > 1$ *sei* $d \equiv d_0^n \bmod l^l$ *mit* $d_0 \in \boldsymbol{Z}$, $l \nmid d_0$. *Dann gilt für* $i = 1, \ldots, n$:

$$\tilde{\varepsilon}_i \equiv 1 \bmod l^l, \quad \textit{falls} \quad |d| > 1,$$

$$\tilde{\varepsilon}_i^n \equiv 1 \bmod l^l, \quad \textit{falls} \quad |d| = 1.$$

Beweis. Im Falle $|d| = 1$ ist $\omega = d\tilde{\varepsilon}_i + d_i$, also

$$0 = f(\omega) = \prod_{j=1}^{n}(d\tilde{\varepsilon}_i + d_i - d_j) - d \equiv d(d^{n-1}\tilde{\varepsilon}_i^n - 1) \bmod l^l,$$

woraus nach Voraussetzung $\tilde{\varepsilon}_i^n \equiv 1 \bmod l^l$ folgt.

Im Falle $|d| > 1$ sei

$$\eta_i = \frac{\omega - d_i}{d_0};$$

dann ist η_i l-ganz und $\eta_i^n \equiv \tilde{\varepsilon}_i \bmod l^l$.

Nun ist aber $\omega = d_0\eta + d_i$, also

$$0 = f(\omega) = \prod_{j=1}^{n}(d_0\eta_i + d_i - d_j) - d \equiv d_0^n(\eta_i^n - 1) \bmod l^l,$$

woraus $\tilde{\varepsilon}_i \equiv \eta_i^n \equiv 1 \bmod l^l$ folgt. ∎

LEMMA 5. *Sei* $f(X) = \prod_{i=1}^{n}(X-d_i)-d \in \boldsymbol{Z}[X]$ *ein erzeugendes Polynom vom Typ* (r_1, r_2) *und seien* $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_n$ *wie in Satz 4 definiert,* l *sei eine Primzahl mit* $l \nmid n$; *dann sind äquivalent:*

(a) $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_{n-1}$ *sind* l*-unabhängig in* $\overline{K}(d_{r_1+1}, \ldots, d_{r_1+r_2}, \sqrt[n]{d})$.

(b) *Es gibt Primzahlen* $p_1, \ldots, p_{n-1}$ *mit folgenden Eigenschaften:*

(1) $p_i \nmid dn$, $p_i \equiv 1 \bmod l$, *und* p_i *ist vollzerlegt in* $\boldsymbol{Q}(d_{r_1+1}, \ldots, d_{r_1+r_2})$.

(2) *Im Falle* $|d| > 1$ *gibt es ein* $d_0 \in \boldsymbol{Z}$ *mit* $d \equiv d_0^n \bmod p_i$ *für* $i = 1, \ldots, n-1$; *im Falle* $|d| = 1$ *sei* $d_0 = d$.

(3) *Es gibt ein* $w \in \boldsymbol{Z}$ *so, daß* $w + p_j\boldsymbol{Z}$ *eine einfache Nullstelle von* $f(X) \bmod p_j$ *ist* $(j = 1, \ldots, n-1)$, *und für die* p_j*-ganzen Zahlen* $e_i = (w - d_i)/d_0$ $(i = 1, \ldots, n-1)$ *gilt:* e_i *ist* l*-ter Potenzrest* $\bmod p_j$ *genau dann, wenn* $i \neq j$.

Beweis. Seien $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_{n-1}$ l-unabhängig in $\overline{K}(d_{r_1+1}, \ldots, d_{r_1+r_2}, \sqrt[n]{d})$; dann gibt es nach Lemma 2 paarweise nicht-konjugierte Primdivisoren 1. Grades $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$ von $\overline{K}(d_{r_1+1}, \ldots, d_{r_1+r_2}, \sqrt[n]{d})$, welche nicht in der Diskriminante von $f(X)$ aufgehen derart, daß gilt: $\tilde{\varepsilon}_i$ ist l-ter Potenzrest $\bmod \mathfrak{p}_j$ genau dann, wenn $i \neq j$. Sind $p_1, \ldots, p_{n-1}$ die zugehörigen Primzahlen, so erfüllen diese (1) und (2), und die Restklassenkörper $\bmod \mathfrak{p}_j$ können mit $\boldsymbol{Z}/p_j\boldsymbol{Z}$ identifiziert werden. Sei nun $f(\omega) = 0$ und $w \in \boldsymbol{Z}$ mit $w \equiv \omega \bmod \mathfrak{p}_j$ für alle j; dann ist $w + p_j\boldsymbol{Z}$ eine einfache Nullstelle von $f(X) \bmod p_j$, es ist

$$(o) \qquad \tilde{\varepsilon}_i \equiv \begin{cases} e_i^n \bmod \mathfrak{p}_j, & \text{falls} \quad |d| > 1, \\ e_i \bmod \mathfrak{p}_j, & \text{falls} \quad |d| = 1, \end{cases}$$

und wegen $l \nmid n$ ist e_i l-ter Potenzrest $\bmod \mathfrak{p}_j$ (und auch $\bmod p_j$) genau dann, wenn $i \neq j$.

Seien nun $p_1, \ldots, p_{n-1}$ mit (1), (2) und (3) gegeben, und seien $w_j \in \boldsymbol{Q}_{p_j}$ die (nach dem Hensel'schen Lemma existierende) Nullstelle von $f(X)$ mit $w_j \equiv w \bmod p_j$; dann besitzt p_j in $\overline{K}(d_{r_1+1}, \ldots, d_{r_1+r_2}, \sqrt[n]{d})$ einen Primteiler 1. Grades $\mathfrak{p}_j$ mit $\omega \equiv w_j \equiv w \bmod \mathfrak{p}_j$, und man kann wieder den Restklassenkörper von $\mathfrak{p}_j$ mit $\boldsymbol{Z}/p_j\boldsymbol{Z}$ identifizieren. Also ist e_i l-ter Potenzrest $\bmod \mathfrak{p}_j$ genau dann, wenn $i \neq j$, und wegen (o) und $l \nmid n$ gilt das auch für die $\tilde{\varepsilon}_i$; wegen Lemma 2 folgt daraus die behauptete l-Unabhängigkeit von $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_{n-1}$. ∎

DEFINITION. Sei $n = r_1 + 2r_2 \geqslant 3$. $P(r_1, r_2)$ bestehe aus allen Primteilern von n und allen Primzahlen l, für die gilt:

Für jedes erzeugende Polynom

$$f(X) = \prod_{i=1}^{n}(X-d_i) - d \in \boldsymbol{Z}[X]$$

vom Typ (r_1, r_2) sind die in Satz 4 definierten Einheiten $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_{n-1}$ l-abhängig in $K(d_{r_1+1}, \ldots, d_{r_1+r_2}, \sqrt[n]{d})$.

Bemerkung. Die Mengen $P(r_1, r_2)$ sind endlich. Ich vermute, daß $P(r_1, r_2)$ jeweils nur aus den Primteilern von $n = r_1 + 2r_2$ besteht; in den Spezialfällen $(r_1, r_2) = (3, 0), (4, 0), (1, 1), (2, 1), (2, 2)$ folgt die Richtigkeit dieser Vermutung aus den Resultaten von Stender [9], [10], [11].

SATZ 5. *Sei* $n = r_1 + 2r_2 \geqslant 3$ *und* l *eine Primzahl mit* $l \notin P(r_1, r_2)$. *Dann gibt es unendlich viele algebraische Zahlkörper* K *mit* r_1 *reellen Konjugierten und* r_2 *Paaren komplexer Konjugierter derart, daß gilt:*

Die Divisorenklassengruppe von $\overline{K} = K(\zeta_l)$ *hat mindestens den* l*-Rang* r_1+r_2-1, *d.h.*

$$\dim_{\mathbf{F}_l}(\mathfrak{C}_{\overline{K}}/\mathfrak{C}_{\overline{K}}^l) \geqslant r_1+r_2-1.$$

KOROLLAR. *Sei* $n \geqslant 3$ *und* l *eine Primzahl mit* $l \notin P(n,0)$. *Dann gibt es unendlich viele algebraische Zahlkörper* $\overline{K}$ *mit* $[\overline{K}:\boldsymbol{Q}] = n(l-1)$ *und*

$$\dim_{\mathbf{F}_l}(\mathfrak{C}_{\overline{K}}/\mathfrak{C}_{\overline{K}}^l) \geqslant n-1.$$

Beweis. Das Korollar folgt aus Satz 5 mit $r_2 = 0$. Zum Beweis von Satz 5 sei l eine Primzahl mit $l \notin P(r_1, r_2)$; dann gibt es ein erzeugendes Polynom $f^*(X) = \prod_{i=1}^{n}(X-d_i^*) - d^* \in \boldsymbol{Z}[X]$ vom Typ (r_1, r_2) derart, daß gilt: Sind $\tilde{\varepsilon}_1^*, \ldots, \tilde{\varepsilon}_n^*$ zu $f^*(X)$ wie in Satz 4 definiert, so sind $\tilde{\varepsilon}_1^*, \ldots, \tilde{\varepsilon}_{n-1}^*$ l-unabhängig in $K(d_{r_1+1}^*, \ldots, d_{r_1+r_2}^*, \sqrt[n]{d^*})$, also nach Lemma 2 auch in $\overline{K}(d_{r_1+1}^*, \ldots, d_{r_1+r_2}^*, \sqrt[n]{d^*})$. Seien nun $p_1, \ldots, p_{n-1}$ Primzahlen, welche die Bedingungen (b) aus Lemma 5 bezüglich $f^*(X)$ erfüllen, und sei $D = \prod_{i=1}^{n-1} p_i$. Sei nun $f(X) = \prod_{i=1}^{n}(X-d_i) - d \in \boldsymbol{Z}[X]$ ein erzeugendes Polynom vom Typ (r_1, r_2) mit $d-d^* \in D\cdot\boldsymbol{Z}$ und $d_i - d_i^* \in D\cdot\boldsymbol{Z}$ für $i = 1, \ldots, n$, $f(\alpha) = 0$ und $K = \boldsymbol{Q}(\alpha)$; dann ist $\boldsymbol{Q}(d_{r_1+1}^*, \ldots, d_{r_1+r_2}^*) = \boldsymbol{Q}(d_{r_1+1}, \ldots, d_{r_1+r_2})$, und $p_1, \ldots, p_{n-1}$ erfüllen die Bedingungen (b) aus Lemma 5 auch bezüglich $f(X)$. Definiert man nun zu $f(X)$ $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_n \in K(d_{r_1+1}, \ldots, d_{r_1+r_2})$ und $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2} \in K$ wie in Satz 4, so sind nach Lemma 5 $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_{n-1}$ l-unabhängig in $\overline{K}(d_{r_1+1}^*, \ldots, d_{r_1+r_2}^*, \sqrt[n]{d^*})$, also $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ l-unabhängig in $\overline{K}$. Wegen $l \nmid D$ kann man nun noch d und die d_i so wählen, daß sie die Voraussetzungen von Lemma 4 erfüllen; dann ist $\tilde{\varepsilon}_i^n \equiv 1 \bmod l^l$ für alle $i = 1, \ldots, n$, also auch $\varepsilon_i^n \equiv 1 \bmod l^l$ für alle $i = 1, \ldots, r_1+r_2$. Nun ist Satz 3 anwendbar, und es folgt:

$$\dim_{\mathbf{F}_l}(\mathfrak{C}_{\overline{K}}/\mathfrak{C}_{\overline{K}}^l) \geqslant r_1+r_2-1.$$

Um sicherzustellen, daß es unendlich viele solche Körper gibt, zeige ich: ist q eine Primzahl mit $q \nmid Dl$, so kann man $f(X)$ als Eisensteinpolynom für q wählen; dann ist nämlich q in K verzweigt, und da es unendlich viele q gibt, folgt die Existenz unendlich vieler Körper K. Ist nun $q \nmid Dl$, so kann man nach dem Chinesischen Restsatz $f(X) = \prod_{i=1}^{n}(X-d_i) - d \in \boldsymbol{Z}[X]$ so wählen, daß außer den angegebenen Kongruenzen modulo $l^l D$ noch $d \equiv q \bmod q^2$ und $d_i \equiv 0 \bmod q^2$ $(i = 1, \ldots, n)$ gilt. ∎

Zusätze bei der Korrektur (6.5.1981):

1. B. Schmithals (Arch. Math. 34 (1980), S. 412–415) zeigte, daß in Korollar 1 auf S. 36 auf die Voraussetzung (b) verzichtet werden kann. Mit den Methoden der vorstehenden Arbeit kann man das wie folgt einsehen:

Bezeichnet $\mathrm{rg}_l(\mathfrak{A})$ den l-Rang der abelschen Gruppe $\mathfrak{A}$, so folgt

$$\mathrm{rg}_l(\mathfrak{C}_K) \geqslant \mathrm{rg}_l(\mathfrak{D}_0/\mathfrak{D}_0\cap\mathfrak{H}_K) \geqslant \mathrm{rg}_l(\mathfrak{D}_0/\mathfrak{D}_0\cap\mathfrak{H}_k) - \mathrm{rg}_l(\mathfrak{D}_0\cap\mathfrak{H}_K/\mathfrak{D}_0\cap\mathfrak{H}_k).$$

Nun ist $\mathrm{rg}_l(\mathfrak{D}_0/\mathfrak{D}_0\cap\mathfrak{H}_k) \geqslant \mathrm{erg}_l(\mathfrak{D}_0/\mathfrak{D}_0\cap\mathfrak{D}_k) = l$; $\mathfrak{D}_0\cap\mathfrak{H}_K/\mathfrak{D}_0\cap\mathfrak{H}_k$ ist elementarabelsch, also folgt $\mathrm{rg}_l(\mathfrak{D}_0\cap\mathfrak{H}_K/\mathfrak{D}_0\cap\mathfrak{H}_k) = \mathfrak{D}_l(\mathfrak{D}_0\cap\mathfrak{H}_K : \mathfrak{D}_0\cap\mathfrak{H}_k)$, und man kann den Beweis nun wie angegeben zu Ende führen.

2. H. W. Lenstra Jr. (Amsterdam) wies darauf hin, daß es in Abschnitt 2 stets ausreicht, Kongruenzen mod l^2 anstatt mod l^l zu betrachten; in $\overline{K}$ ist nämlich $l = \mathfrak{L}^{e_0(l-1)}$, also L/l^2 wegen $2e_0(l-1) \geqslant l$.

Literaturverzeichnis

[1] L. Bernstein und H. Hasse, *An explicit formula for the units of an algebraic number field of degree* $n \geqslant 2$, Pacific Journ. Math. 30 (1969), S. 293–365.

[2] I. Connell und D. Sussman, *The p-dimension of class groups of number fields*, J. London Math. Soc. 2 (1970), S. 525–529.

[3] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. 29 (1967), S. 281–285.

[4] F. Halter-Koch, *Unabhängige Einheitensysteme für eine allgemeine Klasse algebraischer Zahlkörper*, Abhandl. Math. Sem. Univ. Hamburg 43 (1975), S. 85–91.

[5] — *Über Radikalerweiterungen*, Acta Arith. 36 (1980), S. 43–58.

[6] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Ia und II. 2. Aufl., Würzburg 1965.

[7] M. L. Madan, *Class groups of global fields*, J. Reine Angew. Math. 252 (1972), S. 171–177.

[8] P. Roquette und H. Zassenhaus, *A class rank estimate for algebraic number fields*, J. London Math. Soc. 44 (1968), S. 31–38.

[9] H.-J. Stender, *Explizite Bestimmung von Einheiten für einige Klassen algebraischer Zahlkörper*, Dissertation, Köln 1970.

[10] — *Einheiten für eine allgemeine Klasse total reeller algebraischer Zahlkörper*, J. Reine Angew. Math. 257 (1972), S. 151–178.

[11] — *Eine Formel für Grundeinheiten in reinen algebraischen Zahlkörpern dritten, vierten und sechsten Grades*, J. Number Theory 7 (1975), S. 235–250.

[12] K. Uchida, *Unramified extensions of quadratic number fields I, II*, Tôhoku Math. J. 22 (1970), S. 138–141 und 220–224.

MATH. INST. d. UNIV. GRAZ
Halbärthgasse 1, A-8010 Graz, Austria

Eingegangen am 2. 3. 1978 (1047