Studia Scientiarum Mathematicarum Hungarica 23 (1988), 327—334

DURCH NORMEN DEFINIERTE IDEALKLASSENGRUPPEN

G. LETTL

1. Einleitung

Für einen algebraischen Zahlkörper K sei $\mathcal{J}_K$ die Gruppe der gebrochenen Ideale des Ganzheitsringes von K, und für jede Untergruppe $\mathcal{H} \subset \mathcal{J}_K$ ist $\mathcal{J}_K/\mathcal{H}$ eine „Idealklassengruppe" von K. Ist $\mathcal{H}_K$ die Gruppe der gebrochenen Hauptideale von K, so ist $\mathcal{C}_K = \mathcal{J}_K/\mathcal{H}_K$ die „gewöhnliche" Idealklassengruppe von K, eine der wichtigsten Invarianten der algebraischen Zahlentheorie. Ist $\mathcal{H}_K^+$ die Gruppe der von totalpositiven Körperelementen erzeugten Hauptideale, so ist $\mathcal{J}_K/\mathcal{H}_K^+$ die „engere" Idealklassengruppe von K, die bereits in der Gauss-schen Theorie der Geschlechter eine zentrale Rolle spielt. Für einen quadratischen Zahlkörper K ist $\mathcal{H}_K^+ = \{(\alpha) | \alpha \gg 0\} = \{(\beta) | N\beta \in \mathbf{Q}^+\}$, also $\mathcal{H}_K^+$ mit Hilfe der Norm N von $K/\mathbf{Q}$ beschreibbar. In der vorliegenden Arbeit werden nun ganz allgemein solche durch Normen definierte Idealklassengruppen untersucht. Ist L/K eine endliche Erweiterung algebraischer Zahlkörper und F eine (multiplikative) Untergruppe von $K^\times$, so sei $\mathcal{H}(F)$ die Gruppe aller Hauptideale (α) von L mit $N_{L/K}\alpha \in F$. Die Faktorgruppe nach $\mathcal{H}(F)$ ergibt dann eine Idealklassengruppe $\mathcal{C}(F)$ von L. Im Gegensatz zu den von Kuroda [3] definierten Klassengruppen enthalten die Gruppen $\mathcal{C}(F)$ im allgemeinen keine Information über das Zerlegungsverhalten von Primidealen in Oberkörpern, da die Primidealdichten in den einzelnen Klassen in Abhängigkeit von F beliebig variieren können (vgl. Satz 3). Auch die Struktur und die Ordnung von $\mathcal{C}(F)$ hängen im allgemeinen von F ab. Andererseits ermöglicht es diese Variabilität, durch geeignete Wahl von F die Gruppe $\mathcal{C}(F)$ mit vorgegebenen Eigenschaften zu versehen.

Von besonderem Interesse ist der Fall, wenn F direkter Kofaktor der Einheitengruppe ist, also $K^\times = E_K \times F$. Dann liegen zwei Hauptideale mit gleicher relativer Idealnorm bezüglich K genau dann in derselben Klasse von $\mathcal{C}(F)$, wenn sie Erzeugende mit gleicher Relativnorm besitzen. Bumby [1] untersuchte, wann eine endliche, normale Erweiterung L/K von algebraischen Zahlkörpern die folgende Eigenschaft besitzt, die er (N) nannte: je zwei ganze Zahlen $\alpha, \beta \in L$ mit $N_{L/K}\alpha = N_{L/K}\beta$ sind entweder beide irreduzibel oder beide nicht. Ein vollständige Charakterisierung aller Erweiterungen L/K mit der Eigenschaft (N) ist unbekannt. Ist $G = \mathrm{Gal}(L/K)$, $K^\times = E_K \times F$ und enthält jede Klasse von $\mathcal{C}(F)$ Primideale, so zeigt sich, daß die Eigenschaft (N) nur von der Struktur von $\mathcal{C}_L$ und $\mathcal{C}(F)$ als G-Moduln abhängt.

In dieser Arbeit wird auf den Zusammenhang von (N) mit den Gruppen $\mathcal{C}(F)$ nicht näher eingegangen, sondern es werden ausschließlich Resultate über die Klas-

1980 *Mathematics Subject Classification.* Primary 12A75; Secondary 12A45.
Key words and phrases. Ideal class group, prime ideal density.

Akadémiai Kiadó, Budapest

sengruppen $\mathscr{C}(F)$ hergeleitet. Für $L/\mathbf{Q}$ und $\mathbf{Q}^\times = \{1, -1\} \times F$ geben die Sätze 4 und 5 den genauen Zusammenhang zwischen den Klassengruppen $\mathscr{C}(F)$ und $\mathscr{C}_L$ an. Im allgemeinen Fall bleibt die Frage offen, welche F als Kofaktoren von E_K gewählt werden sollen, damit $\mathscr{C}(F)$ minimale Ordnung hat bzw. wann $\mathscr{C}(F)$ mit $\mathscr{C}_L$ übereinstimmt.

2. Die (F)-Idealklassengruppen

Für eine endliche Erweiterung algebraischer Zahlkörper L/K bezeichne $N\colon L^\times \to K^\times$ die Relativnorm, $\mathscr{H}_L$ die Gruppe der Hauptideale von L und $\mathscr{C}_L = \mathscr{J}_L/\mathscr{H}_L$.

DEFINITION. Es sei F eine Untergruppe von $K^\times$. Ein Hauptideal $(\alpha) \in \mathscr{J}_L$ heißt (F)-*Hauptideal*, wenn $N\alpha \in F$ ist. Bezeichnet $\mathscr{H}(F)$ die Gruppe aller (F)-Hauptideale von L, so heißt $\mathscr{C}(F) = \mathscr{J}_L/\mathscr{H}(F)$ die (F)-*Idealklassengruppe* von L.

Ist $\mathfrak{A} \in \mathscr{J}_L$, so bezeichnen wir mit $[\mathfrak{A}]$ bzw. $[\mathfrak{A}]_F$ die gewöhnliche Idealklasse bzw. die (F)-Idealklasse, welche $\mathfrak{A}$ enthält. Für $\alpha \in L^\times$ gilt $(\alpha) \in \mathscr{H}(F)$ genau dann, wenn $N\alpha \in F \cdot NE_L$ ist. Setzen wir $\Phi_F := (F \cdot NL^\times)/(F \cdot NE_L)$, so gilt $\mathscr{H}_L/\mathscr{H}(F) \cong \Phi_F \leqq K^\times/(F \cdot NE_L)$.

LEMMA 1. a) *Ist* $[K^\times : (F \cdot E_K)]$ *endlich, so ist* $\mathscr{C}(F)$ *endlich.*
b) *Ist* $K^\times/(F \cdot E_K)$ *keine Torsionsgruppe, so ist* $\mathscr{C}(F)$ *unendlich.*

BEWEIS. a) Da $[(F \cdot E_K) : (F \cdot NE_L)] \leqq [E_K : NE_L] < \infty$ ist, erhält man

$$[K^\times : (F \cdot NE_L)] = [K^\times : (F \cdot E_K)] \cdot [(F \cdot E_K) : (F \cdot NE_L)] < \infty.$$

Nun ist aber $K^\times/(F \cdot NE_L) \cong \Phi_F \cong \mathscr{H}_L/\mathscr{H}(F)$ und

$$0 \to \mathscr{H}_L/\mathscr{H}(F) \to \mathscr{C}(F) \to \mathscr{C}_L \to 0 \tag{1}$$

eine exakte Sequenz, woraus sich die Endlichkeit von $\mathscr{C}(F)$ ergibt.

b) Nach Voraussetzung existiert ein $\lambda \in K^\times$ mit $\lambda^n \notin F \cdot E_K$ für alle $n \in \mathbf{Z} \setminus \{0\}$. Die Potenzen von λ erzeugen Hauptideale in L, deren (F)-Idealklassen $[(\lambda^n)]_F$ paarweise verschieden sind, also ist $\mathscr{C}(F)$ unendlich.

SATZ 1. *Ist* F *direkter Kofaktor von* E_K *(d. h.* $K^\times = E_K \times F$*) und* h_L *die Klassenzahl von* L*, so gilt*

$$[(E_K \cap NL^\times) : NE_L] \cdot h_L \leqq \sharp\mathscr{C}(F) \leqq [E_K : NE_L] \cdot h_L. \tag{2}$$

BEWEIS. Wegen der exakten Sequenz (1) genügt es, $[(E_K \cap NL^\times) : NE_L] \leqq \sharp(\mathscr{H}_L/\mathscr{H}(F)) \leqq [E_K : NE_L]$ zu zeigen. Nun ist aber

$$\mathscr{H}_L/\mathscr{H}(F) \cong \Phi_F = (F \cdot NL^\times)/(F \cdot NE_L) \leqq K^\times/(F \cdot NE_L) =$$

$$= (E_K \times F)/(NE_L \times F) \cong E_K/NE_L,$$

andererseits gilt

$$\Phi_F \cong (F \cdot (E_K \cap NL^\times))/(F \cdot NE_L) = (F \times (E_K \cap NL^\times))/(F \times NE_L) \cong (E_K \cap NL^\times)/NE_L.$$

Wir setzen nun voraus, daß L/K normal mit Galoisgruppe G ist. Da G die Gruppe $\mathscr{H}(F)$ invariant läßt, operiert G auf $\mathscr{C}(F)$. Wie üblich, schreiben wir Klassengruppen additiv und daher die Operation von G auf $\mathscr{C}_L$ bzw. $\mathscr{C}(F)$ in Präfixnotation, auf L bzw. $\mathscr{J}_L$ jedoch in Exponentennotation. Der folgende Satz zeigt, daß der Stabilisator einer (F)-Idealklasse von F unabhängig ist.

SATZ 2. *Es sei L/K eine endliche, normale Erweiterung algebraischer Zahlkörper mit Galoisgruppe G. Für $a\in\mathscr{C}_L$ sei $G_a\leqq G$ der Stabilisator von a.*

Dann existiert ein Homomorphismus $\gamma_a\colon G_a\to E_K/NE_L$, sodaß für jedes $F\leqq K^\times$ mit $E_K\cap F\subseteq NE_L$ gilt: $G'_a:=\ker(\gamma_a)$ ist der Stabilisator für jede in a enthaltene (F)-Idealklasse.

BEWEIS. Wir wählen ein Ideal $\mathfrak{A}\in a$. Für $\sigma\in G_a$ sei $\alpha_\sigma\in L$ mit $\mathfrak{A}^{\sigma-1}=(\alpha_\sigma)$. Dann definieren wir $\gamma_a\colon G_a\to E_K/NE_L$ durch $\gamma_a(\sigma):=N\alpha_\sigma\cdot NE_L$. Zunächst zeigen wir, daß diese Definition von der Wahl von $\mathfrak{A}$ unabhängig ist. Ist $\mathfrak{B}\in a$, so gibt es zu jedem $\sigma\in G_a$ ein $\beta_\sigma\in L$ mit $\mathfrak{B}^{\sigma-1}=(\beta_\sigma)$. Weiters gibt es ein $\delta\in L$ mit $\mathfrak{B}=\mathfrak{A}\cdot(\delta)$, womit wir $(\beta_\sigma)=(\alpha_\sigma\cdot\delta^{\sigma-1})$ und wegen $N\delta^{\sigma-1}=1$ $N\beta_\sigma\in N\alpha_\sigma\cdot NE_L$ erhalten.

Nun beweisen wir, daß γ_a ein Homomorphismus ist. Für $\sigma,\tau\in G_a$ seien $\alpha_\sigma,\alpha_\tau\in L$ mit $\mathfrak{A}^{\sigma-1}=(\alpha_\sigma)$ und $\mathfrak{A}^{\tau-1}=(\alpha_\tau)$. Wegen $\mathfrak{A}^{\sigma\tau-1}=(\mathfrak{A}^{\sigma-1})^\tau\cdot\mathfrak{A}^{\tau-1}=(\alpha_\sigma^\tau\cdot\alpha_\tau)$ ergibt sich $\gamma_a(\sigma\tau)=N(\alpha_\sigma^\tau\cdot\alpha_\tau)\cdot NE_L=N\alpha_\sigma\cdot N\alpha_\tau\cdot NE_L=\gamma_a(\sigma)\cdot\gamma_a(\tau)$.

Schließlich sei $F\leqq K^\times$ mit $E_K\cap F\subseteq NE_L$, $a'\in\mathscr{C}(F)$ mit $a'\subseteq a$ und $\mathfrak{A}\in a'$. Für $\sigma\in G_a$ sei wieder $\mathfrak{A}^{\sigma-1}=(\alpha_\sigma)$. Dann gilt $(\sigma a'=a')\Leftrightarrow([\mathfrak{A}^\sigma]_F=[\mathfrak{A}]_F)\Leftrightarrow(N\alpha_\sigma\in F\cdot NE_L)$. Nun ist aber $N\alpha_\sigma\in E_K$, und die Voraussetzung über F ergibt $(F\cdot NE_L)\cap E_K=NE_L$, also gilt $(N\alpha_\sigma\in F\cdot NE_L)\Leftrightarrow(N\alpha_\sigma\in NE_L)\Leftrightarrow(\sigma\in G'_a)$.

3. Primidealdichten der (F)-Idealklassen

In diesem Abschnitt sei L/K eine endliche, normale Erweiterung algebraischer Zahlkörper mit Galoisgruppe G. Weiters sei F ein direkter Kofaktor der Einheitengruppe von K. Dann ist F eine freie abelsche Gruppe mit abzählbarer Basis (siehe z. B. Narkiewicz [4], S. 123). Wir werden zeigen, daß durch geeignete Wahl von F „beliebig" vorgegebene Primidealdichten der einzelnen (F)-Idealklassen erreicht werden können. Da (F)-Idealklassen, die unter G konjugiert sind, gleiche Primidealdichte haben, muß dies bei der „beliebigen" Vorgabe der Dichten ebenso berücksichtigt werden wie die Tatsache, daß die Dichte der Primideale in einer gewöhnlichen Idealklasse $1/h_L$ ist.

Nach Skolem [5] läßt sich ein direkter Kofaktor F_0 zu E_K folgendermaßen konstruieren. Die Menge aller Primideale[1] von K sei $\{\mathfrak{p}_i|i\in\mathbf{N}\}$, wobei die Reihenfolge so gewählt wird, daß für ein $n_0\in\mathbf{N}\cup\{0\}$ die Menge $\{[\mathfrak{p}_i]|1\leqq i\leqq n_0\}$ eine Basis für $\mathscr{C}_K$ ist. Für $n\in\mathbf{N}$ und $1\leqq i\leqq n_0$ existieren eindeutig bestimmte Zahlen $h_{i,n}\in\mathbf{Z}$ mit $0\leqq h_{i,n}<\operatorname{ord}[\mathfrak{p}_i]$, sodaß $\mathfrak{p}_n\prod_{i=1}^{n_0}\mathfrak{p}_i^{h_{i,n}}=(\pi_n)$ ein Hauptideal ist. Dann ist $F_0=\coprod_{n\in\mathbf{N}}\langle\pi_n\rangle$ eine freie Gruppe und $E_K\times F_0=K^\times$. Ist v_n die zu $\mathfrak{p}_n$ gehörige

[1] Primideale seien stets ungleich (0).

und auf 1 normierte Exponentenbewertung, so gilt für jedes $\lambda \in K^\times$

$$\lambda = \varepsilon \prod_{n=1}^{n_0} \pi_n^{c_n} \prod_{n=n_0+1}^{\infty} \pi_n^{v_n(\lambda)}, \tag{3}$$

wobei $\varepsilon \in E_K$ und $c_n \in \mathbf{Z}$ durch λ eindeutig bestimmt sind. Das folgende Lemma zeigt, daß sich jeder direkte Kofaktor F zu E_K in der Form $F = \coprod_{n \in \mathbf{N}} \langle \varepsilon_n \pi_n \rangle$ mit eindeutig bestimmten $\varepsilon_n \in E_K$ schreiben läßt.

LEMMA 2. *Es seien A eine multiplikative, abelsche Gruppe, B eine Untergruppe von A, F_0 und F freie Untergruppen von A mit $A = B \times F_0 = B \times F$. Ist $\{f_i | i \in I\}$ eine Basis von F_0, so existieren eindeutig bestimmte $b_i \in B$, sodaß $\{b_i f_i | i \in I\}$ eine Basis von F ist.*

BEWEIS. Ist $\{g_j | j \in J\}$ eine Basis von F, so existieren für $i \in I$, $j \in J$ eindeutig bestimmte $b_i \in B$ und $\varepsilon_{i,j} \in \mathbf{Z}$ mit $f_i = b_i^{-1} \prod_{j \in J} g_j^{\varepsilon_{i,j}}$. Für $F' = \coprod_{i \in I} \langle b_i f_i \rangle$ gilt $F' \subseteq F$. Ist $a \in F$, so existieren $b \in B$ und $\gamma_i \in \mathbf{Z}$ mit

$$a = b \prod_{i \in I} f_i^{\gamma_i} = b \prod_{i \in I} \left(b_i^{-\gamma_i} \prod_{j \in J} g_j^{\varepsilon_{i,j}\gamma_i} \right).$$

Daraus ergibt sich $b = \prod_{i \in I} b_i^{\gamma_i}$ und $a = \prod_{i \in I} (b_i f_i)^{\gamma_i}$, womit wir $F \subseteq F'$ und somit $F = F'$ bewiesen haben.

Es sei nun L/K normal mit Galoisgruppe G und $K^\times = E_K \times F$. Jede Idealklasse $a \in \mathscr{C}_L$ enthält wegen (2) höchstens $[E_K : NE_L]$ (F)-Idealklassen. G_a, γ_a und G_a' seien wie in Satz 2 definiert und $\Gamma_a := \operatorname{im}(\gamma_a) \subseteq E_K/NE_L$. Auf der Menge der in a enthaltenen (F)-Idealklassen operiert G_a, wodurch diese in höchstens $m(a) = [E_K : NE_L]/\sharp \Gamma_a$ Bahnen der Mächtigkeit $i(a) = [G_a : G_a'] = \sharp \Gamma_a$ zerfällt. Da G_a' und Γ_a nur von a, nicht aber von F abhängen, gilt dies auch für $i(a)$ und $m(a)$. Mit $\mathscr{N}: \mathscr{J}_L \to \mathscr{J}_K$ bzw. $\mathscr{N}_{L/\mathbf{Q}}: \mathscr{J}_L \to \mathbf{Q}$ bezeichnen wir die relative bzw. absolute Idealnorm. Ist $M \subseteq \mathscr{J}_L$, so ist die Primidealdichte von M durch

$$\delta(M) = \lim_{n \to \infty} \frac{\sharp \{\mathfrak{P} \in M | \mathfrak{P} \text{ Primideal und } \mathscr{N}_{L/\mathbf{Q}}(\mathfrak{P}) \leqq n\}}{\sharp \{\mathfrak{P} \in \mathscr{J}_L | \mathfrak{P} \text{ Primideal und } \mathscr{N}_{L/\mathbf{Q}}(\mathfrak{P}) \leqq n\}}$$

definiert, falls dieser Grenzwert existiert. Bekanntlich hängt $\delta(M)$ nur von den Primidealen mit Restklassengrad 1, also auch nur von den Primidealen mit Relativgrad $f_{L/K} = 1$ ab. Jede zu M unter G konjugierte Menge hat dieselbe Primidealdichte, also können nur solche (F)-Idealklassen verschiedene Dichten haben, die unter G nicht konjugiert sind.

SATZ 3. *Es sei L/K eine normale Erweiterung algebraischer Zahlkörper mit Galoisgruppe G. Für $1 \leqq j \leqq l$ seien $a_j \in \mathscr{C}_L$ Repräsentanten für die verschiedenen Bahnen, in die $\mathscr{C}_L$ unter G zerfällt. Weiters seien $m_j \in \mathbf{N}$ mit $m_j \leqq m(a_j)$ und $\varepsilon_{i,j} \in \mathbf{R}$ mit $0 \leqq \varepsilon_{i,j} \leqq 1$ und $\sum_{i=1}^{m_j} \varepsilon_{i,j} = 1$. Dann existieren eine Gruppe F mit $K^\times = E_K \times F$ und für $1 \leqq j \leqq l$, $1 \leqq i \leqq m_j$ paarweise verschiedene (F)-Idealklassen $b_{i,j}$ mit $b_{i,j} \subseteq a_j$ und Primidealdichten $\delta(b_{i,j}) = \varepsilon_{i,j}/(h_L \cdot i(a_j))$.*

BEWEIS. Wir gehen von einer Zerlegung $K^\times = E_K \times F_0$ aus, wie sie zu Beginn des Kapitels beschrieben wurde, d. h. $F_0 = \coprod_{n\in\mathbf{N}} \langle \pi_n \rangle$, $\{[\mathfrak{p}_n] | 1 \leqq n \leqq n_0\}$ ist eine Basis von $\mathscr{C}_K$, und für jedes $\lambda \in K^\times$ gilt (3). Für $1 \leqq j \leqq l$ sei $\mathfrak{A}_j \in a_j$ fest gewählt. Die endliche Menge $S \subseteq \mathscr{J}_L$ enthalte genau die Primideale von L, welche über den Idealen $\mathfrak{p}_n$ mit $1 \leqq n \leqq n_0$ oder mit $\mathfrak{p}_n | \mathscr{N}\mathfrak{A}_j$ für $j \in \{1, \ldots, l\}$ liegen. Mit geeigneten $\varepsilon_n \in E_K$ werden wir $F = \coprod_{n\in\mathbf{N}} \langle \varepsilon_n \pi_n \rangle$ bilden und damit alle Behauptungen des Satzes verifizieren.

Es sei nun $j \in \{1, \ldots, l\}$. Wir wählen $\eta_1, \ldots, \eta_{m_j} \in E_K$ so, daß $\eta_1 NE_L, \ldots, \eta_{m_j} NE_L$ m_j verschiedene Nebenklassen von $(E_K/NE_L)/\Gamma_{a_j}$ repräsentieren.

μ: $\mathbf{N} \to \{1, 2, \ldots, m_j\}$ sei eine Funktion mit $\mu(k) = k$ für $1 \leqq k \leqq m_j$ und $\lim_{n\to\infty} \#\{k | \mu(k) = i \text{ und } k \leqq n\}/n = \varepsilon_{i,j}$ für $1 \leqq i \leqq m_j$.

$\{\mathfrak{P}_i | i \in \mathbf{N}\}$ sei eine maximale Menge von unverzweigten Primidealen aus a_j mit Relativgrad $f_{L/K} = 1$, die nicht in S enthalten sind und paarweise nicht konjugiert unter G sind. Außerdem sei ihre Reihenfolge so gewählt, daß $\mathscr{N}_{L/Q}\mathfrak{P}_i \leqq \mathscr{N}_{L/Q}\mathfrak{P}_{i+1}$ gilt. Für $i \in \mathbf{N}$ ist dann $\mathscr{N}\mathfrak{P}_i = \mathfrak{p}_{n_i}$ mit $n_i > n_0$ und $\mathfrak{P}_i \mathfrak{A}_j^{-1} = (\alpha_i)$ mit $v_{n_i}(N\alpha_i) = 1$. Wir erhalten daher $N\alpha_i = \varepsilon \pi_{n_i} \coprod_{n\in\mathbf{N}\setminus\{n_i\}} \pi_n^{c_n}$ mit $\varepsilon \in E_K$, $c_n \in \mathbf{Z}$ und setzen $\varepsilon_{n_i} := \eta_{\mu(i)}^{-1} \varepsilon$.

In dieser Darstellung ist $c_n \neq 0$ nur möglich, wenn $\mathfrak{p}_n | \mathscr{N}\mathfrak{A}_j$ oder $n \leqq n_0$. Auf diese Weise konstruieren wir ε_{n_i} für alle $i \in \mathbf{N}$ und analog für jede Klasse a_k $(1 \leqq k \leqq l)$. Für die von dieser Konstruktion nicht erfaßten Indizes $n \in \mathbf{N}$ (das sind genau die, wo über $\mathfrak{p}_n$ Ideale aus S, Primideale mit Relativgrad $f_{L/K} > 1$ oder verzweigte Primideale liegen) definieren wir $\varepsilon_n := 1$ und setzen

$$F := \coprod_{n\in\mathbf{N}} \langle \varepsilon_n \pi_n \rangle.$$

Wir kehren nun zu der oben betrachteten Idealklasse a_j zurück und behaupten, daß für $1 \leqq i \leqq m_j$, $b_{i,j} = \{\mathfrak{B} \in a_j | \mathfrak{B}\mathfrak{A}_j^{-1} = (\beta) \text{ mit } N\beta \in \eta_i NE_L \times F\}$ alle Behauptungen des Satzes erfüllt.

Man prüft leicht nach, daß $b_{i,j}$ eine (F)-Idealklasse ist, die $\mathfrak{P}_k$ genau dann enthält, wenn $\mu(k) = i$ ist. Insbesondere ist $b_{i,j}$ wegen $\mathfrak{P}_i \in b_{i,j}$ nicht leer. Aus der Wahl der η_i folgt, daß die (F)-Idealklassen $b_{i,j}$ paarweise nicht konjugiert unter G sind. Für die Primidealdichte von $b_{i,j}$ erhalten wir:

$$\delta(b_{i,j}) = \lim_{n\to\infty} \frac{\#\{\mathfrak{P} \in b_{i,j} \setminus S | \mathfrak{P} \text{ prim}, f_{L/K}(\mathfrak{P}) = 1, \mathscr{N}_{L/Q}\mathfrak{P} \leqq n\}}{h_L \#\{\mathfrak{P} \in a_j \setminus S | \mathfrak{P} \text{ prim}, f_{L/K}(\mathfrak{P}) = 1, \mathscr{N}_{L/Q}\mathfrak{P} \leqq n\}} =$$

$$= \frac{1}{h_L} \lim_{n\to\infty} \frac{\#\{\mathfrak{P}_k^\sigma | k \leqq n, \sigma \in G'_{a_j}, \mu(k) = i\}}{\#\{\mathfrak{P}_k^\sigma | k \leqq n, \sigma \in G_{a_j}\}} = \frac{1}{h_L} \lim_{n\to\infty} \frac{\#\{k | k \leqq n, \mu(k) = i\} \# G'_{a_j}}{n \# G_{a_j}} =$$

$$= \varepsilon_{i,j}/(h_L i(a_j)).$$

BEMERKUNG. Durch geeignete Wahl der Funktion μ im Beweis kann erreicht werden, daß für einige oder für alle (F)-Idealklassen die Primidealdichten nicht existieren. Es kann auch (F)-Idealklassen geben, die keine Primideale enthalten, wie das folgende Beispiel zeigt: Für $K = \mathbf{Q}$ und $L = \mathbf{Q}(\sqrt{34})$ ist $NE_L = \{1\}$, aber

$E_K \cap NL^\times = \{1, -1\}$, da $N((3+\sqrt{34})/5) = -1$ ist. Nach Satz 1 gilt $\sharp\,\mathscr{C}(F) = 2h_L = 4$ für jedes F mit $\mathbf{Q}^\times = \{1, -1\} \times F$. Wählt man nun F so, daß die Normen aller Primelemente von L in F liegen, so enthält die (F)-Idealklasse $\{(\alpha) | N\alpha \in (-F)\}$ kein Primideal.

4. (F)-Idealklassengruppen von Erweiterungen über $\mathbf{Q}$

In diesem Kapitel betrachten wir algebraische Zahlkörper L über $K = \mathbf{Q}$ und untersuchen, für welche $F \subseteq \mathbf{Q}^\times$ mit $\mathbf{Q}^\times = \{1, -1\} \times F$, $\mathscr{C}(F) = \mathscr{C}_L$ gelten kann. Außerdem werden wir zeigen, daß die exakte Sequenz (1) unabhängig von der Wahl von F als Kofaktor zu $\{1, -1\}$ spaltet bzw. nicht spaltet. Lemma 2 zeigt, daß für jedes solche F die mit geeigneten Vorzeichen versehenen Primzahlen eine Basis bilden. Ist $NE_L = \{1, -1\}$ (z. B. wenn $[L: \mathbf{Q}]$ ungerade ist), so ist $\mathscr{C}(F) = \mathscr{C}_L$ für jedes F mit $\mathbf{Q}^\times = \{1, -1\} \times F$.

SATZ 4. *Ist $L/\mathbf{Q}$ ein algebraischer Zahlkörper und $NE_L = \{1\}$, so sind folgende Aussagen äquivalent:*

(i) *Es existiert ein F_0 mit $\mathbf{Q}^\times = \{1, -1\} \times F_0$ und $\mathscr{C}(F_0) = \mathscr{C}_L$.*

(ii) *Es gibt kein $\alpha \in L^\times$ mit $N\alpha = -r^2$, $r \in \mathbf{Q}$.*

Zum Beweis dieses Satzes benötigen wir das folgende Lemma.

LEMMA 3. *Für $n \in \mathbf{N}$ sei $V_n = \mathbf{F}_2^n$ der n-dimensionale Vektorraum über $\mathbf{F}_2 = \{0, 1\}$. Es seien $M_n = \{(\alpha_1, \ldots, \alpha_n) \in V_n | \forall\ 1 \leqq i \leqq n: \alpha_i = 0$ oder $\sharp\,\{i | \alpha_i = 0\} = \sharp\,\{i | \alpha_i = 1\}\}$ und $\pi_i: V_n \to \mathbf{F}_2$ die Projektion auf die i-te Komponente $(1 \leqq i \leqq n)$. Ist A eine Untergruppe von V_n mit $A \subseteq M_n$, so existiert ein $i_0 \in \{1, \ldots, n\}$ mit $\pi_{i_0}(A) = \{0\}$.*

BEWEIS. Ist n ungerade oder A trivial, ergibt sich die Behauptung unmittelbar. Es sei nun $m \in \mathbf{N}$ und $n = 2m$. Nehmen wir an, es gäbe eine Untergruppe $A = \{e_1, \ldots, e_{2^d}\} \subseteq M_n$ mit $d \geqq 1$ und für alle i sei $\pi_i(A) \neq 0$. Ist $\varepsilon(A)$ die Anzahl der „1", die als Komponenten in den Elementen von A auftreten, so erhält man $\varepsilon(A) = (2^d - 1)m$. Ist aber $\pi_i(A) \neq \{0\}$, so ist $\pi_i(e_j) = 1$ für genau 2^{d-1} Indizes $j \in \{1, 2, \ldots, 2^d\}$, womit sich $\varepsilon(A) = 2^{d-1}n = 2^d m$ ergibt, was wegen $m \geqq 1$ einen Widerspruch darstellt.

BEWEIS von Satz 4. (i)$\Rightarrow$(ii) ist klar, denn $\mathscr{C}(F_0) = \mathscr{C}_L$ und $NE_L = \{1\}$ ergeben $N\alpha \in F_0$ für alle $\alpha \in L^\times$, und es ist $F_0 \cap \{-r^2 | r \in \mathbf{Q}^\times\} = \emptyset$.

(ii)$\Rightarrow$(i). $\mathbf{P}$ bezeichne die Menge aller rationalen Primzahlen. Für $p \in \mathbf{P}$ sei $v_p: \mathbf{Q}^\times \to \mathbf{Z}$ die p-adische Exponentenbewertung und

$$m(p) = \min\{v_p(N\alpha) | \alpha \in L^\times \text{ und } v_p(N\alpha) > 0\}.$$

$m(p)$ ist der größte gemeinsame Teiler der Restklassengrade aller Primideale von L, die über p liegen, und $m(p) | v_p(N\beta)$ für alle $\beta \in L^\times$. Es sei $\mathbf{P}_1 = \{p \in \mathbf{P} | m(p) \equiv 0 \bmod (2)\}$ und $\mathbf{P} \setminus \mathbf{P}_1 = \{p_1, p_2, \ldots\}$. Wir beweisen zunächst folgende Behauptung:

Ist $n \in \mathbf{N}$ und

$$L_n = \Big\{\alpha \in L^\times | N\alpha \in \{1, -1\} \times \coprod_{p \in \mathbf{P}_1} \langle p \rangle \times \coprod_{i=1}^{n} \langle p_i \rangle\Big\}, \tag{4}$$

so existieren $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$, *sodaß*

$$NL_n \subseteq \coprod_{p \in \mathbf{P}_1} \langle p \rangle \times \prod_{i=1}^{n} \langle \varepsilon_i p_i \rangle \text{ gilt.}$$

Für $1 \leqq j \leqq 2^n$ sei $F_j = \coprod_{p \in \mathbf{P}_1} \langle p \rangle \times \prod_{i=1}^{n} \langle \varepsilon_i p_i \rangle$, wobei $(\varepsilon_1, \ldots, \varepsilon_n)$ die Menge $\{1, -1\}^n$ durchläuft. Wir definieren die Abbildung $\varphi: L_n \to \mathbf{F}_2^{2^n}$ durch $\varphi(\alpha) = (e_1, \ldots, e_{2^n})$ und $e_j = \begin{cases} 0, & \text{wenn } N\alpha \in F_j \\ 1, & \text{wenn } N\alpha \notin F_j \end{cases}$. Man prüft leicht nach, daß φ ein Gruppenhomomorphismus ist. Für $\alpha \in L_n$ ist $N\alpha = \pm \coprod_{p \in \mathbf{P}_1} p^{a(p)} \prod_{i=1}^{n} p_i^{a_i}$. Aus der Definition von $\mathbf{P}_1$ folgt, daß für alle $p \in \mathbf{P}_1$ $a(p) \equiv 0 \bmod (2)$ ist. Sind alle a_i gerade, so gilt wegen (ii) das positive Vorzeichen für $N\alpha$, und es ist $\varphi(\alpha) = (0, \ldots, 0)$. Ist hingegen a_{i_0} ungerade und sind $\varepsilon_i \in \{1, -1\}$ für alle $i \neq i_0$ gewählt, so ist je nach der Wahl von $\varepsilon_{i_0} \in \{1, -1\}$ $N\alpha$ in der zu $(\varepsilon_1, \ldots, \varepsilon_n)$ gehörigen Menge F_j enthalten oder nicht. Es folgt, daß in diesem Fall $N\alpha$ in genau 2^{n-1} der Mengen F_j enthalten ist und $\varphi(\alpha)$ gleich viele „0" wie „1" als Komponenten besitzt. $\varphi(L_n)$ erfüllt somit die Voraussetzungen von Lemma 3. Es existieren daher ein $j \in \{1, \ldots, 2^n\}$, sodaß für $\varphi(L_n)$ die j-te Komponente 0 ist. Das heißt aber $NL_n \subseteq F_j$, womit (4) bewiesen ist.

Wollen wir mit (4) durch Induktion eine Vorzeichenfolge $(\varepsilon_i)_{i \in \mathbf{N}}$ konstruieren, sodaß $NL \subseteq F_0 = \coprod_{p \in \mathbf{P}_1} \langle p \rangle \times \prod_{i \in \mathbf{N}} \langle \varepsilon_i p_i \rangle$ gilt, müssen wir noch zeigen, daß für ein $n_0 \in \mathbf{N}$ und für alle $k \in \mathbf{N}$ mit $k \geqq n_0$ gilt:

Sind $\varepsilon_1, \ldots, \varepsilon_k \in \{1, -1\}$ *und*

$$NL_k \subseteq \coprod_{p \in \mathbf{P}_1} \langle p \rangle \times \prod_{i=1}^{k} \langle \varepsilon_i p_i \rangle,$$

(5) *so existiert ein* $\varepsilon_{k+1} \in \{1, -1\}$ *mit*

$$NL_{k+1} \subseteq \coprod_{p \in \mathbf{P}_1} \langle p \rangle \times \prod_{i=1}^{k+1} \langle \varepsilon_i p_i \rangle.$$

Wählen wir dazu $n_0 \in \mathbf{N}$ so, daß die Idealklassen der über $\mathbf{P}_1 \cup \{p_1, \ldots, p_{n_0}\}$ liegenden Primideale von L die Klassengruppe $\mathscr{C}_L$ erzeugen, und $k \geqq n_0$. Nach (4) existieren $\varepsilon_1, \ldots, \varepsilon_k \in \{1, -1\}$ mit $NL_k \subseteq \coprod_{p \in \mathbf{P}_1} \langle p \rangle \times \prod_{i=1}^{k} \langle \varepsilon_i p_i \rangle$. Wegen der Wahl von n_0 existiert ein $\alpha \in L_{k+1}$ mit $v_{p_{k+1}}(N\alpha) = m(p_{k+1}) \equiv 1 \bmod (2)$, also

$$N\alpha = \varepsilon p_{k+1}^{m(p_{k+1})} \coprod_{p \in \mathbf{P}_1} p^{a(p)} \prod_{i=1}^{k} (\varepsilon_i p_i)^{a_i}$$

mit $\varepsilon \in \{1, -1\}$. Wir behaupten, daß $\varepsilon_{k+1} := \varepsilon$ die gewünschte Eigenschaft besitzt. Gäbe es nämlich ein $\beta \in L_{k+1}$ mit

$$N\beta = - \coprod_{p \in \mathbf{P}_1} p^{b(p)} \prod_{i=1}^{k} (\varepsilon_i p_i)^{b_i} (\varepsilon_{k+1} p_{k+1})^{bm(p_{k+1})}$$

mit $b \in \mathbf{Z}$, so ist

$$N(\beta\alpha^{-b}) = -\prod_{p \in \mathbf{P}_1} p^{b(p)-ba(p)} \prod_{i=1}^{k} (\varepsilon_i p_i)^{b_i - ba_i}.$$

Wegen $\beta\alpha^{-b} \in L_k$ ist dies aber ein Widerspruch zur Voraussetzung von (5). Mit dem Beweis von (5) ist aber auch der Beweis von Satz 4 abgeschlossen.

Abschließend bringen wir noch ein Resultat über die exakte Sequenz (1).

SATZ 5. *Ist L ein algebraischer Zahlkörper und $NE_L = \{1\}$, so sind folgende Aussagen äquivalent:*

(a) *Es existiert ein F_0 mit $\mathbf{Q}^\times = \{1, -1\} \times F_0$, sodaß die Sequenz (1) spaltet.*
(b) *Für jedes F mit $\mathbf{Q}^\times = \{1, -1\} \times F$ spaltet die Sequenz (1).*
(c) *Es existiert kein Hauptideal $(\alpha) \in \mathfrak{J}_L^2$ mit $N\alpha = -r^2$, $r \in \mathbf{Q}$.*

BEWEIS. Eine exakte Sequenz von abelschen Gruppen $0 \to A \to B \to C \to 0$ spaltet genau dann, wenn A eine reine Untergruppe von B ist. (1) spaltet in unserem Fall daher genau dann, wenn für alle $a' \in \mathscr{C}(F)$ gilt: ist $2a' \in \mathscr{H}_L/\mathscr{H}(F)$, so ist $2a' = \mathscr{H}(F)$.

(a)$\Rightarrow$(c). Es spalte $0 \to \mathscr{H}_L/\mathscr{H}(F_0) \to \mathscr{C}(F_0) \to \mathscr{C}_L \to 0$. Es seien $\mathfrak{A} \in \mathfrak{J}_L$ und $\alpha \in L$ mit $\mathfrak{A}^2 = (\alpha)$ und $N\alpha = \pm r^2$, $r \in \mathbf{Q}$. Weiters sei $a' = [\mathfrak{A}]_{F_0} \in \mathscr{C}(F_0)$. Dann ist aber $(\alpha) \in 2a' = \mathscr{H}(F_0)$ und somit $N\alpha = r^2$.

(c)$\Rightarrow$(b). Es sei $\mathbf{Q}^\times = \{1, -1\} \times F$ und $a' \in \mathscr{C}(F)$ mit $2a' \in \mathscr{H}_L/\mathscr{H}(F)$. Wählen wir $\mathfrak{A} \in a'$, so ist $\mathfrak{A}^2 = (\alpha)$ ein Hauptideal. (c) ergibt $N\alpha = r^2 \in F$, also $2a' = \mathscr{H}(F)$. Daher spaltet die Sequenz (1).

(b)$\Rightarrow$(a). Klar.

Ich möchte Herrn Professor F. Halter-Koch für viele anregende Diskussionen und für seine Ratschläge beim Verfassen des Manuskripts an dieser Stelle herzlichst danken.

REFERENCES

[1] BUMBY, R. T., Irreducible integers in Galois extensions, *Pacific J. Math.* **22** (1967), 221—229. *MR* **35** #4186.
[2] HASSE, H., *Number theory*, Grundlehren der mathematischen Wissenschaften, Band 229, Springer-Verlag, Berlin—New York, 1980. *MR* **81c:** 12001b.
[3] KURODA, S.-N., Idealgruppen und Dirichletsche Reihen in algebraischen Zahlkörpern, *J. Math. Soc. Japan* **22** (1970), 353—387. *MR* **42** #1796.
[4] NARKIEWICZ, W., *Elementary and analytic theory of algebraic numbers*, Monografie Matematyczne, tom 57, PWN—Polish Scientific Publishers, Warszawa, 1974. *MR* **50** #268.
[5] SKOLEM, TH., On the existence of a multiplicative basis for an arbitrary algebraic field, *Norske Vid. Selsk. Forhandlinger* **20** (1947), no. 2, 4—7. *MR* **10**—104.

(Received February 3, 1984)

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HALBÄRTHGASSE 1
A—8010 GRAZ
AUSTRIA

87-5434 — Szegedi Nyomda — Felelős vezető: Surányi Tibor igazgató