ACTA ARITHMETICA
XXXIII (1977)

Einheiten und Divisorenklassen in Galois'schen algebraischen Zahlkörpern mit Diedergruppe der Ordnung $2l$ für eine ungerade Primzahl l*

von

FRANZ HALTER-KOCH (Essen)

Ziel dieser Arbeit ist ein arithmetisch-körpertheoretischer Beweis der Klassenzahlproduktformel für galois'sche Zahlkörper vom Grade $2l$ mit Diedergruppe (für eine ungerade Primzahl l) sowie einige damit verbundene Strukturuntersuchungen für die Einheitengruppen und die Divisorenklassengruppen solcher Körper; dabei werden Resultate von G. Gras [5] über die Divisorenklassengruppen und von N. Moser [11] über die Einheitengruppen zum Teil neu begründet und verschärft.

Einen analytischen Beweis der Klassenzahlproduktformel findet man in [11], im Falle $l = 3$ auch schon in [12], ein arithmetisch-körpertheoretischer Beweis wurde bisher nur im Falle $l = 3$ gegeben (Callahan [3]). Der hier durchgeführte Beweis bringt auch im Falle $l = 3$ gegenüber dem Callahan'schen Beweis wesentliche Vereinfachungen.

1. Bezeichnungen und gruppentheoretische Vorbereitungen. Sei l eine ungerade Primzahl. Für einen algebraischen Zahlkörper k bezeichne E_k die Einheitengruppe von k, E_k^* die Gruppe der Einheiten $\varepsilon \in E_k$ mit $N_{k/\mathbf{Q}}(\varepsilon) = +1$ (normpositive Einheiten), $\mathfrak{D}_k$ die Divisorengruppe, $\mathfrak{H}_k$ die Gruppe der Hauptdivisoren, $\mathfrak{C}_k = \mathfrak{D}_k/\mathfrak{H}_k$ die Divisorenklassengruppe und $h_k = |\mathfrak{C}_k|$ die Klassenzahl von k.

Für eine endliche abelsche Gruppe A sei $\tilde{A}$ die l-Sylowgruppe von A und $\hat{A}$ die Gruppe der Elemente mit zu l teilerfremder Ordnung von A; es ist dann $A = \tilde{A} \oplus \hat{A}$. Insbesondere ist für einen algebraischen Zahlkörper k $\tilde{\mathfrak{C}}_k$ die l-Divisorenklassengruppe und $\hat{\mathfrak{C}}_k$ die Gruppe der Divisorenklassen mit zu l primer Ordnung; $\tilde{h}_k = |\tilde{\mathfrak{C}}_k|$ sei die l-Klassenzahl von k und $\hat{h}_k = |\hat{\mathfrak{C}}_k| = h_k/\tilde{h}_k$.

* Diese Arbeit entstand im Rahmen eines durch das Land Nordrhein-Westfalen geförderten Forschungsvorhabens.

G sei die Diedergruppe der Ordnung $2l$,

$$G = \langle \sigma, \tau \mid \sigma^l = \tau^2 = 1,\ \sigma\tau = \tau\sigma^{-1} \rangle,$$

und L/Q eine galois'sche Erweiterung mit Gruppe G. Es sei Ω der Fixkörper von σ und K der Fixkörper von τ; dann ist $K' = K^\sigma$ der Fixkörper von $\tau\sigma^2$. Ω ist ein quadratischer Zahlkörper, $\tau \mid \Omega$ die erzeugende Substitution von Ω/Q, L/Ω ist eine zyklische Erweiterung vom Grade l mit Galoisgruppe $\langle\sigma\rangle$; $K, K' = K^\sigma, K^{\sigma^2}, \ldots, K^{\sigma^{l-1}}$ ist ein System von l zueinander konjugierten Körpern und L ist der zugehörige Normalkörper. Um lästige Fallunterscheidungen zu vermeiden, will ich den Fall reiner kubischer Körper ($l = 3$, $\Omega = Q(\sqrt{-3})$) ausschließen, zumal dieser Fall bereits mehrfach erschöpfend behandelt wurde (vgl. [1], [2], [3], [5], [7]); insbesondere kann ich dann annehmen, daß L die l-ten Einheitswurzeln nicht enthält.

Für einen (multiplikativ geschriebenen) G-Modul A sei

$$A_0 = \{c \in A \mid c^\sigma = c\}, \qquad A^+ = \{c \in A \mid c^\tau = c\}$$

und

$$A^- = \{c \in A \mid c^\tau = c^{-1}\}.$$

Dann gilt:

Lemma 1. (a) *Für jeden G-Modul A ist*

$$A^+ \cdot (A^+)^\sigma = \prod_{i=0}^{l-1} (A^+)^{\sigma^i}$$

und

$$A^- \cdot (A^-)^\sigma = \prod_{i=0}^{l-1} (A^-)^{\sigma^i}.$$

(b) *Ist A ein G-Modul endlicher ungerader Ordnung, so ist*

$$A^+ = A^{1+\tau}, \qquad A^- = A^{1-\tau}$$

und

$$A = A^+ \oplus A^-.$$

Beweis. (a) Zum Nachweis der ersten Gleichung genügt es, zu zeigen, daß mit jedem $c \in A^+ \cdot (A^+)^\sigma$ auch c^σ in $A^+ \cdot (A^+)^\sigma$ liegt. Es ist $(A^+)^\sigma = \{c \in A \mid c^{\tau\sigma^2} = c\}$, und für jedes $x \in A$ ist $x^{1+\tau} \in A^+$, $x^{1+\tau\sigma^2} \in (A^+)^\sigma$. Ist nun $c \in A^+ \cdot (A^+)^\sigma$, so ist

$$c^{\sigma^2} = \left(\frac{c^{1+\tau}}{c}\right)^{1+\tau\sigma^2} \cdot \left(\frac{c^{1+\tau}}{c}\right)^{-1},$$

also $c^{\sigma^2} \in A^+ \cdot (A^+)^\sigma$, und wegen $\sigma = (\sigma^2)^{(l+1)/2}$ ist auch $c^\sigma \in A^+ \cdot (A^+)^\sigma$. Die zweite Gleichung beweist man analog.

(b) Die Zerlegung $e = \frac{1}{2}(e+\tau) + \frac{1}{2}(e-\tau)$ der Eins von G liefert die entsprechende Zerlegung für 2-divisible Moduln, woraus die Behauptung folgt.

2. Die Struktur der Einheitengruppe. Nach Lemma 1 ist $E_K \cdot E_{K'} = \prod_{i=0}^{l-1} E_{K^{\sigma^i}}$; wegen

$$E_K \cap E_{K'} = E_K \cdot E_{K'} \cap E_\Omega = \{1\}$$

ist der $\mathbf{Z}$-Rang von $E_K \cdot E_{K'} \cdot E_\Omega$ gleich der Summe der $\mathbf{Z}$-Ränge von E_K, $E_{K'}$ und E_Ω, also $l-1$, falls L imaginär ist, und $2l-1$, falls L reell ist. Daher ist der Index

$$a = (E_L : E_K \cdot E_{K'} \cdot E_\Omega)$$

endlich. Sei

$$E_{L/\Omega} = \{\varepsilon \in E_L \mid N_{L/\Omega}(\varepsilon) = 1\}$$

die Relativeinheitengruppe für L/Ω; dann ist $E_K^* \cdot E_{K'}^* \subseteq E_{L/\Omega}$, und da L nach Voraussetzung die l-ten Einheitswurzeln nicht enthält, ist $E_{L/\Omega} \cap E_\Omega = \{1\}$, also

$$a = (E_L : E_{L/\Omega} \cdot E_\Omega) \cdot (E_{L/\Omega} : E_K^* \cdot E_{K'}^*).$$

Ich setze

$$a_0 = (E_{L/\Omega} : E_K^* \cdot E_{K'}^*)$$

und erhalte damit

$$a = \begin{cases} a_0, & \text{falls } L \text{ imaginär}, \\ \dfrac{a_0 l}{(E_\Omega : N_{L/\Omega} E_L)}, & \text{falls } L \text{ reell}. \end{cases}$$

Nach N. Moser [11] ist $a \in \{1, l\}$, falls L imaginär ist, und $a \in \{1, l, l^2\}$, falls L reell. Darüber hinaus werden in [11] alle möglichen Isomorphietypen von E_L als G-Modul angegeben. Ohne die gesamte Theorie der ganzzahligen Darstellungen von G zu verwenden, zeige ich:

Satz 1. (a) *Es ist $a_0 \in \{1, l\}$, falls L imaginär, und $a_0 \in \{1, l, l^2\}$, falls L reell ist.*

(b) $a_0 = (E_K^{1-\sigma} \cap E_{L/\Omega}^l : E_K^{l(1-\sigma)})$.

(c) $N_{L/K} E_{L/\Omega} = E_K^*$.

(d) $E_K^{1-\sigma} \cap E_{L/\Omega}^l / E_K^{l(1-\sigma)} \cong \mathfrak{H}_{K,0} \cdot \mathfrak{H}_\Omega / \mathfrak{H}_\Omega$; *dabei ist* $\mathfrak{H}_{K,0} = \mathfrak{H}_K \cap \mathfrak{H}_{L,0} \subseteq \mathfrak{H}_{L,0}^+$.

Beweis. Sei ζ eine primitive l-te Einheitswurzel, $R = \mathbf{Z}[\zeta]$ und $R_0 = \mathbf{Z}[\zeta + \zeta^{-1}]$; dann ist $R \cong \mathbf{Z}[\langle\sigma\rangle]/(1+\sigma+\ldots+\sigma^{l-1})$, und

$$\Lambda = \mathbf{Z}[G]/(1+\sigma+\ldots+\sigma^{l-1}) \cong R \oplus R\bar{\tau}$$

mit $\bar{\tau} = \tau + (1+\sigma+\ldots+\sigma^{l-1}) \in \Lambda$.

Da L die l-ten Einheitswurzeln nicht enthält, ist $E_{L/\Omega}$ ein torsionsfreier R-Modul vom $\boldsymbol{Z}$-Rang $l-1$ (falls L imaginär ist) oder $2(l-1)$ (falls L reell ist); daher ist $E_{L/\Omega}$ ein R-projektiver Λ-Modul vom R-Rang 1 (im imaginären Fall) oder 2 (im reellen Fall) und es ist nach [8]

$$E_{L/\Omega} \cong \begin{cases} (1-\zeta)^{\varepsilon}\cdot\mathfrak{a}R, & \text{falls } L \text{ imaginär},\\ (1-\zeta)^{\varepsilon_1}\cdot\mathfrak{a}_1R\oplus(1-\zeta)^{\varepsilon_2}\cdot\mathfrak{a}_2R, & \text{falls } L \text{ reel}\end{cases}$$

mit Idealen $\mathfrak{a},\mathfrak{a}_1,\mathfrak{a}_2$ von R_0 und $\varepsilon,\varepsilon_1,\varepsilon_2\in\{0,1\}$. Bei diesem Isomorphismus entspricht der Anwendung von σ auf $E_{L/\Omega}$ auf der rechten Seite die Multiplikation mit ζ, und der Anwendung von τ entspricht der (im reellen Fall komponentenweise) Übergang zum Konjugiert-Komplexen.

Sei nun zunächst L imaginär. Setzt man $(1-\zeta)R\cap R_0=\mathfrak{p}$, so wird $E_K^*\cong\mathfrak{p}^{\varepsilon}\mathfrak{a}$ und $E_K^*\cdot E_{K'}^*\cong\mathfrak{p}^{\varepsilon}\mathfrak{a}R$, also

$$a_0=(E_{L/\Omega}:E_K^*\cdot E_{K'}^*)=l^{\varepsilon}\in\{1,l\}.$$

Anderseits ist aber

$$E_K^{1-\sigma}\cap E_{L/\Omega}^l = E_K^{*1-\sigma}\cap E_{L/\Omega}^l\cong l\cdot(1-\zeta)\mathfrak{a}$$

und

$$E_K^{l(1-\sigma)}=E_K^{*l(1-\sigma)}\cong l\cdot(1-\zeta)\mathfrak{p}^{\varepsilon}\mathfrak{a},$$

also sicher

$$(E_K^{1-\sigma}\cap E_{L/\Omega}^l:E_K^{l(1-\sigma)})=l^{\varepsilon}.$$

Sei nun L reell; dann erhält man durch Anwendung desselben Schlusses wie eben auf die beiden Komponenten von $(1-\zeta)^{\varepsilon_1}\mathfrak{a}_1R\oplus(1-\zeta)^{\varepsilon_2}\mathfrak{a}_2R$

$$a_0=(E_{L/\Omega}:E_K^*E_{K'}^*)=l^{\varepsilon_1+\varepsilon_2}\in\{1,l,l^2\}$$

und

$$a_0=(E_K^{1-\sigma}\cap E_{L/\Omega}^l:E_K^{l(1-\sigma)}).$$

Damit ist (a) und (b) bewiesen.

Zum Beweis von (c) beachte man, daß R/R_0 eine zahmverzweigte Erweiterung ist. Daher ist $\mathrm{Sp}_{R/R_0}(R)=R_0$, also auch $\mathrm{Sp}_{R/R_0}\big((1-\zeta)^{\varepsilon}\mathfrak{a}R\big)=\mathfrak{p}^{\varepsilon}\mathfrak{a}$, woraus nach dem oben Gesagten die Behauptung folgt.

Für den Beweis von (d) sei zunächst $a\in K^\times$ mit $(a)\in\mathfrak{H}_{K,0}\subseteq\mathfrak{D}_{L,0}$; wegen $\mathfrak{D}_{L,0}^l\subseteq\mathfrak{D}_\Omega$ ist $(a)^l\in\mathfrak{H}_\Omega^+\subseteq\mathfrak{D}_\Omega^+$. Nun ist aber $\mathfrak{D}_\Omega^+\cap\mathfrak{D}_K=\mathfrak{D}_{\boldsymbol{Q}}=\mathfrak{H}_{\boldsymbol{Q}}$, also $(a)^l\in\mathfrak{H}_{\boldsymbol{Q}}$; daher existieren $m\in\boldsymbol{Q}$ und $\varepsilon\in E_K$ mit $a^l=m\varepsilon$, und genau dann ist $\varepsilon\in E_K^l$, wenn $m\in\boldsymbol{Q}^{\times l}$, also $(a)\in\mathfrak{H}_\Omega$, was wegen der τ-Invarianz von a äquivalent ist zu $(a)\in\mathfrak{H}_{\boldsymbol{Q}}$. Aus $a^l=m\varepsilon$ folgt $\varepsilon^{1-\sigma}=(a^{1-\sigma})^l$, also $a^{1-\sigma}\in E_{L/\Omega}$ und $\varepsilon^{1-\sigma}\in E_{L/\Omega}^l$. Die Zuordnung $(a)\mapsto\varepsilon^{1-\sigma}$ definiert einen Homorphismus

$$f\colon\ \mathfrak{H}_{K,0}\cdot\mathfrak{H}_\Omega/\mathfrak{H}_\Omega\to E_K^{1-\sigma}\cap E_{L/\Omega}^l/E_K^{l(1-\sigma)}.$$

Ist $f\big((a)\cdot\mathfrak{H}_\Omega\big)=1$, so ist $a^l=m\varepsilon$ mit $m\in\boldsymbol{Q}$ und $\varepsilon^{1-\sigma}\in E_K^{l(1-\sigma)}$; also gibt es eine Einheit $\eta\in E_K$ mit $\varepsilon^{1-\sigma}=\eta^{l(1-\sigma)}$, woraus $\varepsilon=\pm\eta^l\in E_K^l$ und damit $(a)\in\mathfrak{H}_\Omega$ folgt. Für den Beweis der Surjektivität von f sei $\varepsilon\in E_K$ und $\gamma\in E_{L/\Omega}$ mit $\varepsilon^{1-\sigma}=\gamma^l$; dann ist aber $\gamma=\delta^{1-\sigma}$ mit einem $\delta\in L^\times$. Setzt man nun $m=N_{L/K}\left(\frac{\varepsilon}{\delta^l}\right)^{(l-1)/2}$ und $a=\varepsilon\cdot N_{L/K}(\delta)^{-(l-1)/2}$, so ist $m\in\boldsymbol{Q}$, $a\in K^\times$ und $m\varepsilon=a^l$, also $f\big((a)\cdot\mathfrak{H}_\Omega\big)=\varepsilon^{1-\sigma}\cdot E_K^{l(1-\sigma)}$. ∎

3. Die Struktur der ambigen Klassen. $\mathfrak{D}_{L,0}$ ist die Gruppe der für L/Ω ambigen Divisoren von L, $\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0}$ ist die Gruppe der von den ambigen Divisoren erzeugten Klassen (stark ambige Klassen) und $\mathfrak{C}_{L,0}$ ist die Gruppe der für L/Ω ambigen Divisorenklassen von L. Nach [13] ist

$$|\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0}|=\frac{h_\Omega\cdot l^{w-1}}{(E_\Omega:N_{L/\Omega}E_L)}$$

und

$$(\mathfrak{C}_{L,0}:\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})=(E_\Omega\cap N_{L/\Omega}L^\times:N_{L/\Omega}E_L);$$

dabei ist w die Anzahl der in L verzweigten Primdivisoren von Ω. Seien $\mathfrak{q}_1,\dots,\mathfrak{q}_t$ die τ-invarianten Primdivisoren von Ω, die in L verzweigt sind, und $\mathfrak{p}_1,\dots,\mathfrak{p}_s,\mathfrak{p}_1^\tau,\dots,\mathfrak{p}_s^\tau$ die nicht τ-invarianten in L verzweigten Primdivisoren von Ω, $\mathfrak{q}_i=\mathfrak{Q}_i^l$, $\mathfrak{p}_i=\mathfrak{P}_i^l$, $\mathfrak{p}_i^\tau=\mathfrak{P}_i'^l$ ($\mathfrak{P}_i'=\mathfrak{P}_i^\tau$); dann ist $w=2s+t$, und es gilt:

Satz 2. (a) *Die Einlagerung $\mathfrak{C}_K\to\mathfrak{C}_L$ ist injektiv.*

(b) *$\mathfrak{H}_{L,0}^+\cdot\mathfrak{H}_\Omega/\mathfrak{H}_\Omega$ ist eine l-Gruppe, und es ist*

$$(\mathfrak{H}_{L,0}^+\cdot\mathfrak{H}_\Omega:\mathfrak{H}_\Omega)\leqslant l\cdot(E_\Omega:N_{L/\Omega}E_L).$$

(c) $\mathfrak{H}_{L,0}^+\cdot\mathfrak{H}_\Omega/\mathfrak{H}_\Omega=\mathfrak{H}_{K,0}\cdot\mathfrak{H}_\Omega/\mathfrak{H}_\Omega\cong\mathfrak{H}_{K,0}/\mathfrak{H}_{\boldsymbol{Q}}\cong K^l\boldsymbol{Q}\cap E_K/E_K^l$.

(d) $$|\mathfrak{C}_{L,0}^+|=|\mathfrak{C}_\Omega^+|\cdot\frac{l^{s+t}\cdot(E_\Omega\cap N_{L/\Omega}L^\times:N_{L/\Omega}E_L)}{(\mathfrak{H}_{L,0}^+\cdot\mathfrak{H}_\Omega:\mathfrak{H}_\Omega)} = |\mathfrak{C}_\Omega^+|\cdot\frac{l^{s+t}\cdot(E_\Omega\cap N_{L/\Omega}L^\times:N_{L/\Omega}E_L)}{a_0}.$$

(e) *Ist L/Ω unverzweigt, so ist $\mathfrak{H}_{L,0}^+\cdot\mathfrak{H}_\Omega/\mathfrak{H}_\Omega=1$ und*

$$|\mathfrak{C}_{L,0}^+|=|\mathfrak{C}_\Omega^+|\cdot(E_\Omega:N_{L/\Omega}E_L).$$

Beweis. (a) Sei H die Gruppe aller $\varepsilon\in E_L^-$, für die es ein $\beta\in L^\times$ mit $\beta^{1-\tau}=\varepsilon$ und $(\beta)\in\mathfrak{D}_K$ gibt. Dann ist nach [10]

$$\mathrm{Ke}(\mathfrak{C}_K\to\mathfrak{C}_L)\cong H/E_L^{1-\tau};$$

nun ist aber

$$H/E_L^{1-\tau}\subseteq E_L^-/E_L^{1-\tau}\cong H^1(\langle\tau\rangle,E_L)\quad\text{und}\quad|H^1(\langle\tau\rangle,E_L)|=\frac{2}{v}\cdot(E_K:N_{L,K}E_L)$$

mit $v = 1$, falls L reell, und $v = 2$, falls L imaginär ist (vgl. [13]). Wegen $E_K^* = N_{L/K}E_{L/\Omega}$ ist

$$(E_K : N_{L/K}E_L) = \begin{cases} 2, & \text{falls } -1 \notin N_{L/K}E_L, \\ 1, & \text{falls } -1 \in N_{L/K}E_L. \end{cases}$$

In jedem Falle ist $-1 \in E_L^-$, aber $-1 \notin H$, da $L = K(\sqrt{d_\Omega})$ (d_Ω ist die Diskriminante von Ω) und d_Ω in K kein Divisorquadrat ist. Ist nun entweder L imaginär oder L reell und $-1 \in N_{L/K}E_L$, so ist $E_L^-/E_L^{1-\tau}$ von der Ordnung 2 und wird von -1 erzeugt; daher ist $H = E_L^{1-\tau}$. Ist L reell und $-1 \notin N_{L/K}E_L$, so gilt für die Grundeinheit ω_0 von Ω: $\omega_0 \in E_L^-$, aber $\omega_0 \notin H$ und $-\omega_0 \notin H$; also ist $E_L^-/E_L^{1-\tau}$ eine Gruppe der Ordnung 4, erzeugt von -1 und ω_0, woraus wieder $H = E_L^{1-\tau}$ folgt.

(b) Es ist $\mathfrak{H}_{L,0}^+ \cdot \mathfrak{H}_\Omega \subseteq \mathfrak{H}_{L,0}$ und

$$(\mathfrak{H}_{L,0} : \mathfrak{H}_\Omega) = \frac{(\mathfrak{D}_{L,0} : \mathfrak{D}_\Omega) \cdot (\mathfrak{D}_\Omega : \mathfrak{H}_\Omega)}{(\mathfrak{D}_{L,0} : \mathfrak{H}_{L,0})} = l \cdot (E_\Omega : N_{L/\Omega}E_L).$$

(c) Wegen $\mathfrak{H}_{K,0} \cap \mathfrak{H}_\Omega = \mathfrak{H}_{\boldsymbol{Q}}$ ist $\mathfrak{H}_{K,0} \cdot \mathfrak{H}_\Omega/\mathfrak{H}_\Omega \cong \mathfrak{H}_{K,0}/\mathfrak{H}_{\boldsymbol{Q}}$, und wegen $\mathfrak{H}_{K,0} \subseteq \mathfrak{H}_{L,0}^+$ ist auch $\mathfrak{H}_{K,0} \cdot \mathfrak{H}_\Omega/\mathfrak{H}_\Omega \subseteq \mathfrak{H}_{L,0}^+ \cdot \mathfrak{H}_\Omega/\mathfrak{H}_\Omega$. Sei nun $(\alpha) \in \mathfrak{H}_{L,0}^+$; dann ist (α) von der Form

$$(\alpha) = \mathfrak{a} \cdot \prod_{i=1}^{s} (\mathfrak{P}_i\mathfrak{P}_i')^{\varepsilon_i} \cdot \prod_{i=1}^{t} \mathfrak{Q}_i^{\delta_i}$$

mit $\varepsilon_i, \delta_i \in \{0, 1, \ldots, l-1\}$ und $\mathfrak{a} \in \mathfrak{D}_\Omega^+$, also $(\alpha)^2 \in \mathfrak{D}_{K,0}$; wegen (a) ist dann aber $(\alpha)^2 \in \mathfrak{H}_{K,0}$, und da nach (b) $\mathfrak{H}_{L,0}^+ \cdot \mathfrak{H}_\Omega/\mathfrak{H}_{K,0} \cdot \mathfrak{H}_\Omega$ eine l-Gruppe ist, folgt $(\alpha) \cdot \mathfrak{H}_\Omega \in \mathfrak{H}_{K,0} \cdot \mathfrak{H}_\Omega/\mathfrak{H}_\Omega$. Für den Beweis von $\mathfrak{H}_{K,0}/\mathfrak{H}_{\boldsymbol{Q}} \cong K^l\boldsymbol{Q} \cap \cap E_K/E_K^l$ sei $(\alpha) \in \mathfrak{H}_{K,0}$; dann ist $(\alpha)^l \in \mathfrak{H}_{\boldsymbol{Q}}$, also gibt es ein $\varepsilon \in E_K$ und ein $m \in \boldsymbol{Q}$ mit $\varepsilon = \alpha^l \cdot m$. Man rechnet nun leicht nach, daß $(\alpha) \mapsto \varepsilon$ den gewünschten Isomorphismus definiert.

(d) Ist $E_\Omega \cap N_{L/\Omega}L^\times = N_{L/\Omega}E_L$, so ist $\mathfrak{C}_{L,0} = \mathfrak{D}_{L,0}/\mathfrak{H}_{L,0}$, also auch $\mathfrak{C}_{L,0}^+ = (\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+$. Ist $E_\Omega \cap N_{L/\Omega}L^\times \neq N_{L/\Omega}E_L$, so existiert eine Klasse $C_0 \in \mathfrak{C}_{L,0}^+$ mit $C_0^l \in \mathfrak{C}_\Omega$ derart, daß $\mathfrak{C}_{L,0} = \langle \mathfrak{D}_{L,0}/\mathfrak{H}_{L,0}, C_0 \rangle$ (vgl. [5]); daher ist in diesem Falle $|\mathfrak{C}_{L,0}^+| = |(\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+| \cdot l$. In jedem Falle genügt es also, zu zeigen:

$$|(\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+| = |\mathfrak{C}_\Omega^+| \cdot \frac{l^{s+t}}{(\mathfrak{H}_{L,0}^+ \cdot \mathfrak{H}_\Omega : \mathfrak{H}_\Omega)}.$$

Aus der Exaktheit der Sequenz

$$1 \to \mathfrak{H}_{L,0}^+ \to \mathfrak{D}_{L,0}^+ \to (\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+ \to H^1(\langle\tau\rangle, \mathfrak{H}_{L,0}^+)$$

folgt zunächst $\mathfrak{D}_{L,0}^+/\mathfrak{H}_{L,0}^+ \subseteq (\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+$ und $C^2 \in \mathfrak{D}_{L,0}^+/\mathfrak{H}_{L,0}^+$ für jede Klasse $C \in (\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+$.

Sei $\iota\colon \mathfrak{C}_\Omega \to \mathfrak{C}_L$ die Einlagerung von $\mathfrak{C}_\Omega$ in $\mathfrak{C}_L$; dann ist

$$(\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^l \subseteq \iota(\mathfrak{C}_\Omega),$$

und für $C \in (\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+$ ist

$$C = (C^2)^{(l+1)/2} \cdot C^{-l} \in (\mathfrak{D}_{L,0}^+/\mathfrak{H}_{L,0}^+) \cdot \iota(\mathfrak{C}_\Omega)^+,$$

woraus

$$(\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+ = (\mathfrak{D}_{L,0}^+/\mathfrak{H}_{L,0}^+) \cdot \iota(\mathfrak{C}_\Omega)^+$$

folgt. $(\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+$ wird also erzeugt von $\iota(\mathfrak{C}_\Omega)^+$ und den durch die Divisoren $\mathfrak{P}_1\mathfrak{P}_1', \ldots, \mathfrak{P}_s\mathfrak{P}_s', \mathfrak{Q}_1, \ldots, \mathfrak{Q}_t$ definierten Klassen von L, es ist daher

$$|(\mathfrak{D}_{L,0}/\mathfrak{H}_{L,0})^+| = \frac{|\iota(\mathfrak{C}_\Omega)^+| \cdot l^{s+t}}{b};$$

dabei ist b die Anzahl der Hauptdivisoren

$$(\alpha) = \mathfrak{a} \cdot \prod_{i=1}^{s} (\mathfrak{P}_i\mathfrak{P}_i')^{\varepsilon_i} \cdot \prod_{i=1}^{t} \mathfrak{Q}_i^{\delta_i} \in \mathfrak{H}_{L,0}^+$$

mit $\varepsilon_i, \delta_i \in \{0, 1, \ldots, l-1\}$ und $\mathfrak{a} \in \mathfrak{D}_\Omega$ derart, daß $\mathfrak{a}^{1-\tau} \in \mathfrak{H}_L$. Nun ist aber $\mathfrak{a}^2 = \mathfrak{a}^{1-\tau} \cdot \mathfrak{a}^{1+\tau}$, und daher ist mit $\mathfrak{a}^{1-\tau}$ auch $\mathfrak{a}^2$ Hauptdivisor. Ist nun $(\alpha) \in \mathfrak{H}_{L,0}^+$ wie eben, so liegt mit

$$\Big[\prod_{i=1}^{s} (\mathfrak{P}_i\mathfrak{P}_i')^{\varepsilon_i} \cdot \prod_{i=1}^{t} \mathfrak{Q}_i^{\delta_i}\Big]^2 \quad \text{auch} \quad \prod_{i=1}^{s} (\mathfrak{P}_i\mathfrak{P}_i')^{\varepsilon_i} \cdot \prod_{i=1}^{t} \mathfrak{Q}_i^{\delta_i} \quad \text{in} \quad \mathfrak{H}_{L,0};$$

daher ist b die Anzahl der Hauptdivisoren

$$(\alpha) = \prod_{i=1}^{s} (\mathfrak{P}_i\mathfrak{P}_i')^{\varepsilon_i} \cdot \prod_{i=1}^{t} \mathfrak{Q}_i^{\delta_i} \in \mathfrak{H}_{L,0}^+$$

mit $\varepsilon_i, \delta_i \in \{0, 1, \ldots, l-1\}$; diese bilden aber gerade ein Repräsentantensystem für $\mathfrak{H}_{L,0}^+ \cdot \mathfrak{H}_\Omega/\mathfrak{H}_\Omega$, woraus $b = (\mathfrak{H}_{L,0}^+ \cdot \mathfrak{H}_\Omega : \mathfrak{H}_\Omega)$ folgt. Zum Beweis von (d) ist nun noch $|\iota(\mathfrak{C}_\Omega)^+| = |\mathfrak{C}_\Omega^+|$ zu zeigen. Dazu beweise ich:

$\iota | \mathfrak{C}_\Omega^+$ definiert einen Isomorphismus $\mathfrak{C}_\Omega^+ \to \iota(\mathfrak{C}_\Omega)^+$.

Für $C \in \mathfrak{C}_\Omega$ ist genau dann $\iota(C) \in \iota(\mathfrak{C}_\Omega)^+$, wenn $\iota(C)^\tau = \iota(C^\tau) = \iota(C)$, also $C^{1-\tau} \in \operatorname{Ke}\iota$, was äquivalent ist zu $C^2 \in \operatorname{Ke}\iota$; damit erhält man einen Isomorphismus

$$\{C \in \mathfrak{C}_\Omega \mid C^2 \in \operatorname{Ke}\iota\}/\operatorname{Ke}\iota \xrightarrow{\sim} \iota(\mathfrak{C}_\Omega)^+.$$

Ist $C^2 \in \operatorname{Ke}\iota$, so ist $C^{2l} = 1$, also

$$C^l \in \mathfrak{C}_\Omega^+ \quad \text{und} \quad C = (C^2)^{(l+1)/2} \cdot C^{-l} \in (\operatorname{Ke}\iota) \cdot \mathfrak{C}_\Omega^+,$$

woraus wegen $\operatorname{Ke}\iota \cap \mathfrak{C}_\Omega^+ = 1$ die Isomorphie

$$\{C \in \mathfrak{C}_\Omega \mid C^2 \in \operatorname{Ke}\iota\}/\operatorname{Ke}\iota \cong \mathfrak{C}_\Omega^+$$

folgt.

(e) Ist L/Ω unverzweigt, so gibt es keine in K vollverzweigte Primzahl, und daher ist $\mathfrak{H}_{K,0} = \mathfrak{H}_\Omega$, woraus mit (c), (d) und $E_\Omega \subseteq N_{L/\Omega}L^\times$ die Behauptung folgt. ■

Satz 2 hat die folgenden Konsequenzen für die Struktur der Einheitengruppe:

KOROLLAR. (a) $a_0 = (K^l\cdot Q \cap E_K : E_K^l)$.

(b) *Ist* L/Ω *unverzweigt, so ist* $a_0 = 1$.

(c) *Ist* L *imaginär, so ist* $a \in \{1, l\}$; *ist* L *reell, so ist* $a \in \{1, l, l^2\}$.

Beweis. (a) und (b) folgen unmittelbar aus Satz 1 und Satz 2. Ist L imaginär, so ist $a = a_0 \in \{1, l\}$ nach Satz 1; ist L reell, so ist $a = \dfrac{a_0 l}{(E_\Omega : N_{L/\Omega}E_L)}$, aber $a_0 = (\mathfrak{H}_{K,0}\cdot\mathfrak{H}_\Omega : \mathfrak{H}_\Omega) \leqslant l\cdot(E_\Omega : N_{L/\Omega}E_L)$. ■

4. Die Klassenzahlproduktformel. Ziel dieses letzten Paragraphen ist ein arithmetischer Beweis der Formel

$$h_L = \frac{a h_\Omega h_K^2}{l^r}$$

mit

$$r = \begin{cases} 1, & \text{falls } L \text{ imaginär}, \\ 2, & \text{falls } L \text{ reell}. \end{cases}$$

Den Beweis führe ich getrennt für den zu l primen Teil und den l-Anteil der Divisorenklassengruppe; der zu l prime Teil ist einfacher:

SATZ 3. $\hat h_L = \hat h_\Omega \cdot \hat h_K^2$.

Beweis. Wegen der Injektivität der Einlagerungen $\hat{\mathfrak{C}}_\Omega \to \hat{\mathfrak{C}}_L$ und $\hat{\mathfrak{C}}_K \to \hat{\mathfrak{C}}_L$ kann ich $\hat{\mathfrak{C}}_\Omega$ und $\hat{\mathfrak{C}}_K$ als Untergruppen von $\hat{\mathfrak{C}}_L$ betrachten. Wegen $H^1(\langle\sigma\rangle, \hat{\mathfrak{C}}_L) = 1$ ist $\hat{\mathfrak{C}}_K\cdot\hat{\mathfrak{C}}_{K'} \subseteq \hat{\mathfrak{C}}_L^{1-\sigma}$, und wegen $\hat{\mathfrak{C}}_{L,0} = \hat{\mathfrak{C}}_\Omega$ ist $\hat{\mathfrak{C}}_L^{1-\sigma} \cong \hat{\mathfrak{C}}_L/\hat{\mathfrak{C}}_\Omega$. Ist $C \in \hat{\mathfrak{C}}_K \cap \hat{\mathfrak{C}}_{K'}$, so ist $C^\tau = C^{\tau\sigma^2} = C$, also auch $C^\sigma = C$ und $C^l = 1$, also $C = 1$. Das Produkt $\hat{\mathfrak{C}}_K\cdot\hat{\mathfrak{C}}_{K'}$ ist somit direkt, und ich erhalte $\hat h_K^2 = \hat h_K \cdot \hat h_{K'} \leqslant \hat h_L/\hat h_\Omega$. Anderseits betrachte ich nun den Homomorphismus

$$\varphi\colon \hat{\mathfrak{C}}_L \to \hat{\mathfrak{C}}_K \oplus \hat{\mathfrak{C}}_{K'} \oplus \hat{\mathfrak{C}}_\Omega,$$

definiert durch $\varphi(C) = \big(N_{L/K}(C), N_{L/K'}(C), N_{L/\Omega}(C)\big)$; für $C \in \operatorname{Ke}\varphi$ ist $C^\tau = C^{\tau\sigma^2} = C^{-1}$, also $C^\sigma = C$ und damit wieder wie oben $C = 1$. φ ist also injektiv und daher $\hat h_L \leqslant \hat h_K^2 \cdot \hat h_\Omega$. ■

Die Untersuchung der l-Klassengruppe wird besonders einfach, wenn L/Ω unverzweigt ist.

SATZ 4. *Ist* L/Ω *unverzweigt, so gilt*:

(a) $\tilde{\mathfrak{C}}_K \cap \tilde{\mathfrak{C}}_{K'} = \tilde{\mathfrak{C}}_{L,0}^+$.

(b) $\tilde{\mathfrak{C}}_L^{1-\sigma} = \tilde{\mathfrak{C}}_K \cdot \tilde{\mathfrak{C}}_{K'}$.

(c) $\tilde h_L = \dfrac{a\cdot\tilde h_\Omega\cdot\tilde h_K^2}{l^r}$ *mit* $r = \begin{cases} 1, & \textit{falls } L \textit{ imaginär}, \\ 2, & \textit{falls } L \textit{ reell}. \end{cases}$

Beweis. (a) Nach Lemma 1 ist $\tilde{\mathfrak{C}}_{L,0}^+ \subseteq \tilde{\mathfrak{C}}_K \cap \tilde{\mathfrak{C}}_{K'}$; ist nun $C \in \tilde{\mathfrak{C}}_K \cap \tilde{\mathfrak{C}}_{K'}$, so ist $C^\tau = C^{\tau\sigma^2} = C$, also $C^\tau = C^\sigma = C$ und $C \in \tilde{\mathfrak{C}}_{L,0}^+$.

(b) Wegen der Unverzweigtheit von L/Ω ist $H^1(\langle\sigma\rangle, \tilde{\mathfrak{C}}_L) = 1$ und daher $\tilde{\mathfrak{C}}_K\cdot\tilde{\mathfrak{C}}_{K'} \subseteq \tilde{\mathfrak{C}}_L^{1-\sigma}$. Ich betrachte nun den Homomorphismus $\varphi\colon \tilde{\mathfrak{C}}_L \to \tilde{\mathfrak{C}}_K \oplus \tilde{\mathfrak{C}}_{K'}$, definiert durch

$$\varphi(C) = \big(N_{L/K}(C), N_{L/K'}(C)\big).$$

Genau dann ist $C \in \operatorname{Ke}\varphi$, wenn $C^\tau = C^{\tau\sigma^2} = C^{-1}$, d.h., wenn $C^\tau = C^{-1}$ und $C^\sigma = C$, also $C \in \tilde{\mathfrak{C}}_{L,0}^-$. Aus $\operatorname{Ke}\varphi = \tilde{\mathfrak{C}}_{L,0}^-$ folgt mit Lemma 1

$$|\tilde{\mathfrak{C}}_K \oplus \tilde{\mathfrak{C}}_{K'}| = \tilde h_K^2 \geqslant \frac{|\tilde{\mathfrak{C}}_L|}{|\tilde{\mathfrak{C}}_{L,0}^-|} = \frac{|\tilde{\mathfrak{C}}_L|\cdot|\tilde{\mathfrak{C}}_{L,0}^+|}{|\tilde{\mathfrak{C}}_{L,0}|} = |\tilde{\mathfrak{C}}_L^{1-\sigma}|\cdot|\tilde{\mathfrak{C}}_{L,0}^+|,$$

aber anderseits ist auch

$$|\tilde{\mathfrak{C}}_L^{1-\sigma}| \geqslant |\tilde{\mathfrak{C}}_K\cdot\tilde{\mathfrak{C}}_{K'}| = \frac{\tilde h_K^2}{|\tilde{\mathfrak{C}}_{L,0}^+|},$$

woraus $\tilde{\mathfrak{C}}_L^{1-\sigma} = \tilde{\mathfrak{C}}_K\cdot\tilde{\mathfrak{C}}_{K'}$ folgt.

(c) Es ist $\tilde h_L = |\tilde{\mathfrak{C}}_L| = |\tilde{\mathfrak{C}}_L^{1-\sigma}|\cdot|\tilde{\mathfrak{C}}_{L,0}|$, $|\tilde{\mathfrak{C}}_{L,0}| = \tilde h_\Omega/l$, und nach Satz 2(e) ist

$$|\tilde{\mathfrak{C}}_L^{1-\sigma}| = \frac{\tilde h_K^2}{|\tilde{\mathfrak{C}}_{L,0}^+|} = \frac{\tilde h_K^2}{(E_\Omega : N_{L/\Omega}E_L)},$$

da $\tilde{\mathfrak{C}}_\Omega^+ = 1$. Nach dem Korollar zu Satz 2 ist $a_0 = 1$, also im imaginären Fall $a = 1$ und

$$\tilde h_L = \frac{\tilde h_K^2\cdot h_\Omega}{l};$$

im reellen Fall ist $a = \dfrac{a_0 l}{(E_\Omega : N_{L/\Omega}E)}$, also

$$\tilde h_L = \frac{a\tilde h_K^2\cdot\tilde h_\Omega}{l^2}.$$

Sei nun L/Ω verzweigt, $\tilde K$ der l-Klassenkörper von K, $\tilde K'$ der von K' und $\tilde L$ der von L; dann ist $\tilde K\cdot\tilde K' \subseteq L$. $\tilde K L/L$ ist Klassenkörper zu $\tilde{\mathfrak{C}}_L^-$

$= \{C \in \tilde{\mathfrak{C}}_L \mid C^\tau = C^{-1}\}$, $\tilde K' L/L$ ist Klassenkörper zu $(\tilde{\mathfrak{C}}_L^-)^\sigma = \{C \in \tilde{\mathfrak{C}}_L \mid C^{\tau\sigma^2} = C^{-1}\}$, und $\tilde K \tilde K'/L$ ist Klassenkörper zu $\tilde{\mathfrak{C}}_L^- \cap (\tilde{\mathfrak{C}}_L^-)^\sigma = \tilde{\mathfrak{C}}_{L,0}^-$.

Daraus erhält man

$$[\tilde K\tilde K':L] = \frac{\tilde h_L}{|\tilde{\mathfrak{C}}_{L,0}^-|} = [\tilde K \tilde K':\tilde K L]\cdot[\tilde K L:L] = \frac{[\tilde K' L:L]\cdot[\tilde K L:L]}{[\tilde K L\cap \tilde K' L:L]}$$

und damit

$$\tilde h_L = \frac{\tilde h_K^2\cdot|\tilde{\mathfrak{C}}_{L,0}|}{|\tilde{\mathfrak{C}}_{l,0}^+|\cdot[\tilde KL\cap\tilde K'L:L]} = \frac{a_0\tilde h_\Omega \tilde h_K^2\cdot l^{s-1}}{(E_\Omega:N_{L/\Omega}E_L)\cdot[\tilde KL\cap \tilde K'L:L]}.$$

Ich werde beweisen:

LEMMA 2. *Es ist*

$$[\tilde KL\cap\tilde K'L:L] = l^s.$$

Dann berechnet man

$$\tilde h_L = \frac{a_0\tilde h_\Omega\tilde h_K^2}{l\cdot(E_\Omega:N_{L/\Omega}E_L)},$$

also gilt:

SATZ 5.

$$\tilde h_L = \begin{cases} \dfrac{a\tilde h_\Omega\cdot\tilde h_K^2}{l} & \textit{falls } L \textit{ imaginär},\\[2mm] \dfrac{a\tilde h_\Omega\cdot h_K^2}{l^2}, & \textit{falls } L \textit{ reell}.\end{cases}$$

Beweis von Lemma 2. $\tilde KL\cap\tilde K'L/L$ ist Klassenkörper zu

$$\mathfrak{E} = \tilde{\mathfrak C}_L^-\cdot(\tilde{\mathfrak C}_L^-)^\sigma \subseteq \tilde{\mathfrak C}_L.$$

Nach Lemma 1 ist $\mathfrak E^\sigma = \mathfrak E = \prod_{i=0}^{l-1}(\tilde{\mathfrak C}_L^-)^{\sigma^i}$; ferner ist $(\tilde{\mathfrak C}_L^-)^\tau = \tilde{\mathfrak C}_L^-$, und für $C\in\tilde{\mathfrak C}_L^-$ ist $(C^\sigma)^\tau = C^{-\sigma^{-1}}\in\mathfrak E$, also auch $\mathfrak E^\tau=\mathfrak E$. Für $C\in\tilde{\mathfrak C}_L$ ist $C^{\tau-1}\in\mathfrak E$ und $C^{\tau\sigma^2-1}\in\mathfrak E$, also $C^\tau\equiv C^{\tau\sigma^2}\equiv C \bmod \mathfrak E$ und daher auch $C^\tau \equiv C^\sigma\equiv C \bmod\mathfrak E$. Folglich ist $\tilde KL\cap\tilde K'L/\boldsymbol{Q}$ galoissch und $\tilde KL\cap\tilde K'L/\Omega$ abelsch; sei U die Galoisgruppe von $\tilde KL\cap\tilde K'L/\Omega$. U ist ein endlicher G-Modul mit ungerader Ordnung, also ist nach Lemma 1 $U = U^+\oplus U^-$, und da τ auf den Klassen nach $\mathfrak E$ trivial operiert, ist $U^+\supseteq \mathrm{Gal}(\tilde KL\cap\tilde K'L/L)$; auf $\mathrm{Gal}(L/\Omega) = \langle\sigma\rangle$ operiert aber τ nichttrivial, und daher ist $U^+ = \mathrm{Gal}(\tilde KL\cap\tilde K'L/L)$. Setzt man $M = \mathrm{Fix}(U^-)$, so ist $M/\boldsymbol{Q}$ abelsch und $\tilde KL\cap\tilde K'L = L\cdot M$.

Sei nun umgekehrt $M_1/\boldsymbol{Q}$ eine abelsche l-Erweiterung und M_1L/L unverzweigt. Dann ist M_1L/L Klassenkörper zu einer Untergruppe $\mathfrak E_1\subseteq\tilde{\mathfrak C}_L$ mit $\mathfrak E_1^\sigma = \mathfrak E_1^\tau = \mathfrak E_1$ und $C^\sigma\equiv C^\tau\equiv C\bmod\mathfrak E_1$ für alle $C\in\tilde{\mathfrak C}_L$; es ist also $\tilde{\mathfrak C}_1^{1-\tau} = \tilde{\mathfrak C}_1^-\subseteq\mathfrak E_1$ und wegen $\mathfrak E_1^\sigma=\mathfrak E_1$ ist $\mathfrak E\subseteq\mathfrak E_1$ und damit $M_1L\subseteq\tilde KL\cap\tilde K'L$.

$\tilde KL\cap\tilde K'L/L$ ist nach dem Bewiesenen die größte unverzweigte Erweiterung von L der Form $L\cdot M$ mit einer abelschen l-Erweiterung $M/\boldsymbol{Q}$ (Geschlechterkörper im Sinne von Fröhlich [4]). Für $C\in\tilde{\mathfrak C}_L$ ist

$$C^l = \prod_{i=0}^{l-1} C^{1-\sigma^i\tau}\cdot N_{L/\Omega}(C)^\tau\in\mathfrak E$$

und daher $\tilde KL\cap\tilde K'L/L$ vom Exponenten l;

$$[\tilde KL\cap\tilde K'L:L] = l^v,$$

wobei v die Anzahl der Primzahlen p ist, für die gilt:

Ist $M/\boldsymbol{Q}$ eine zyklische Erweiterung vom Grade l und p die einzige in M verzweigte Primzahl, so ist ML/L unverzweigt. Ich werde zeigen:

Genau dann ist ML/L unverzweigt, wenn p in Ω zerlegt und in L verzweigt ist; daraus folgt dann $v = s$ und damit die Behauptung. Somit bleibt zu beweisen:

LEMMA 2a. *Sei $M/\boldsymbol{Q}$ eine zyklische Erweiterung vom Grade l und p die einzige in M verzweigte Primzahl (also $p\equiv 1 \bmod l$ oder $p = l$). Dann gilt:*

(a) *Ist ML/L unverzweigt, so sind die Primteiler von p in L/Ω verzweigt.*

(b) *Ist p in Ω zerlegt und in L verzweigt, so ist ML/L unverzweigt.*

(c) *Ist p in Ω träge oder verzweigt, und ist der Primteiler von p in L verzweigt, so ist notwendig $p = l$ und ML/L ist verzweigt.*

Beweis. (a) Da p in M verzweigt ist, hat p in LM eine durch l teilbare Verzweigungsordnung, die wegen der Unverzweigtheit von ML/L von einer Verzweigung in L/Ω herkommen muß.

(b) Ist p in Ω zerlegt und in L verzweigt und ist $\mathfrak P$ ein Primteiler von p in L, so ist $L_{\mathfrak{P}}/\boldsymbol{Q}_p$ eine totalverzweigte zyklische Erweiterung vom Grade l; wäre nun ML/L verzweigt und $\mathfrak Q$ ein Primteiler von p in ML, so wäre $(ML)_{\mathfrak{Q}}/\boldsymbol{Q}_p$ eine totalverzweigte Erweiterung vom Typ (l, l), was nicht geht.

(c) Ist p in Ω träge und in L verzweigt, so ist nach [9] $p\equiv -1\bmod l$ oder $p = l$, in unserem Falle also notwendig $p = l$. In LM hat l nur einen Primteiler $\mathfrak L$ (die lokale Erweiterung ist vom Grade $2l^2$); sei T der Trägheitskörper für $\mathfrak L|l$. Dann ist $\Omega\subseteq T$ und $T/\boldsymbol{Q}$ ist zyklisch; da aber $M\Omega/\Omega$ verzweigt ist, ist notwendig $T=\Omega$, also ML/Ω totalverzweigt und insbesondere ML/L nicht unverzweigt. Ist p in L totalverzweigt, so ist notwendig $p = l$, und l hat in ML wieder nur einen Primteiler $\mathfrak L$. Ist T der Trägheitskörper für $\mathfrak L|l$, so ist $T/\boldsymbol{Q}$ zyklisch und l in T unverzweigt, also notwendig $T = \boldsymbol{Q}$ und l in ML totalverzweigt. ■

Literaturverzeichnis

[1] P. Barrucand and H. Cohn, *A rational genus, class number divisibility and unit theory for pure cubic fields*, J. Number Theory 2 (1970), S. 7–21.
[2] — — *Remarks on principal factors in a relative cubic field*, ibid. 3 (1971), S. 226–239.
[3] T. Callahan, *The 3-class groups of non-Galois cubic fields I, II*, Mathematika 21 (1974), S. 72–89 und 168–188.
[4] A. Fröhlich, *The genus field and genus group in finite number fields*, ibid. 6 (1959), S. 40–46.
[5] G. Gras, *Sur les l-classes d'idéaux des extensions non galoisiennes de Q de degré premier impair l à cloture galoisienne diédrale de degré 2l*, J. Math. Soc. Japan 26 (1974), S. 677–685.
[6] — *Sur le 3-rang des corps cubiques non galoisiens*, erscheint demnächst.
[7] F. Halter-Koch, *Eine Bemerkung über kubische Einheiten*, Archiv d. Math. 27 (1976), S. 593–595.
[8] M. P. Lee, *Integral representations of dihedral groups of order 2p*, Trans. Amer. Math. Soc. 110 (1964), S. 213–231.
[9] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédrale d'ordre 2p*, Ann. Inst. Fourier 19 (1969), S. 1–90.
[10] M. Moriya, *Über die Klassenzahl eines relativ-zyklischen Körpers vom Primzahlgrad*, Jap. J. Math. 10 (1933), S. 1–18.
[11] N. Moser, *Unités et nombre de classes d'une extension galoisienne diédrale de Q*, Asterisque 24/25 (1975), S. 29–35.
[12] A. Scholz, *Idealklassen und Einheiten in kubischen Körpern*, Monatshefte Math. Phys. 40 (1933), S. 211–222.
[13] H. Yokoi, *On the class number of a relatively cyclic number field*, J. Math. Soc. Japan 20 (1968), S. 411–418.

Eingegangen am 30. 12. 1975
und in revidierter Form am 18. 5. 1976 (802)

ACTA ARITHMETICA
XXXIII (1977)

A rational sixteenth power reciprocity law

by

PHILIP A. LEONARD* (Tempe, Ariz.) and
KENNETH S. WILLIAMS* (Ottawa, Canada)

1. Introduction. Let p and q be distinct primes $\equiv 1 \pmod 4$ such that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. There are integers a, b, A, B satisfying

$$(1.1)\qquad \begin{aligned} p &= a^2+b^2, & a-1 &\equiv b \equiv 0 \pmod 2,\\ q &= A^2+B^2, & A-1 &\equiv B \equiv 0 \pmod 2. \end{aligned}$$

Moreover, it is well known that $\left(\frac{B}{q}\right) = (-1)^{(q-1)/4}$. If $k \not\equiv 0 \pmod q$ is a 2^l-th power modulo q, we set

$$\left(\frac{k}{q}\right)_{2^{l+1}} = \begin{cases} +1, & \text{if } k \text{ is a } 2^{l+1}\text{-th power } (\text{mod}\, q),\\ -1, & \text{otherwise.} \end{cases}$$

In 1969, Burde [1] proved the following rational biquadratic reciprocity law.

THEOREM 1.

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{(q-1)/4} \left(\frac{aB-bA}{q}\right).$$

If p and q are $\equiv 1 \pmod 8$, and $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, it follows from Burde's law that $\left(\frac{aB-bA}{q}\right) = 1$, and from the classical law of biquadratic reciprocity that $\left(\frac{B}{q}\right)_4 = 1$. Integers c, d, C, D exist satisfying

$$(1.2)\qquad p = c^2+2d^2, \qquad q = C^2+2D^2,$$

*This research was supported by National Research Council of Canada Grant A-7233.