Math. Z. 121, 346–368 (1971)

Quadratische Formen und quadratische Reziprozitätsgesetze über algebraischen Zahlkörpern

M. KNEBUSCH und W. SCHARLAU

Herrn Ernst Witt zum 60. Geburtstag am 26. 6. 1971

Witt hat in seiner fundamentalen Arbeit [19] die allgemeine Theorie der quadratischen Formen über Körpern entwickelt und dabei insbesondere den Begriff der „Witt-Gruppe" eingeführt. Außerdem faßte er die damals bekannten Kenntnisse über die Klassifikation der quadratischen Formen über speziellen Körpern (insbesondere über algebraischen Zahlkörpern) zusammen. Diese Resultate gipfeln im Satz von Hasse-Minkowski ([19], Satz 19, Satz 20) und der „Umkehrung" des Satzes von Hasse-Minkowski ([19], Satz 21).

Im Anschluß an Witts Arbeit sind in dieser Arbeit folgende drei Probleme behandelt:

1. Die Berechnung der Witt-Gruppe eines algebraischen Zahlkörpers. (Was unter „Berechnung" verstanden werden soll, ist natürlich etwas vage. Eine befriedigende Lösung wäre das Auftreten der Witt-Gruppe in einer exakten Sequenz, deren andere Terme bekannt sind und die in geeigneter Weise das Lokal-Global-Prinzip widerspiegelt.) Den Beitrag unserer Arbeit dazu findet man in § 2 und Korollar 6.9.

2. Die Rolle des quadratischen Reziprozitätsgesetzes in der Weilschen Form ([17], S. 179, Proposition 5), also für beliebige quadratische Formen und nicht nur für die Normformen von Quaternionen-Algebren (vgl. [14]).

3. Die Eindeutigkeit des quadratischen Reziprozitätsgesetzes im Sinne von Moore [11], Chap. II.

Wir benutzen in der vorliegenden Arbeit nur algebraische Hilfsmittel, die nicht über die globale und lokale Klassenkörpertheorie für quadratische Erweiterungen hinausgehen (vgl. die Darstellung in [12]). Insbesondere geben wir einen elementaren algebraischen Beweis für das Weilsche Reziprozitätsgesetz. Er verläuft analog dem Beweis des „Residuensatzes" für differentialwertige symmetrische Bilinearformen über einem algebraischen Funktionenkörper in einer Variablen [6]. Differentialwertige Formen spielen wieder eine entscheidende Rolle. Auf Grund des Zusammenhangs zwischen Differentialen und der Differente ergibt sich als leichte Konsequenz des Weilschen Reziprozitätsgesetzes der Heckesche Satz, daß die Differente ein Quadrat in der Idealklassengruppe ist. Es ergibt sich auch die von Armitage [1] gegebene Charakterisierung der Differente in der engeren Klassengruppe.

Für die in dieser Arbeit benötigten Dinge über quadratische Formen und symmetrische Bilinearformen verweisen wir auf [7, 12, 13, 19]. Wir setzen insbesondere eine genaue Kenntnis der lokalen Theorie voraus. Von der algebraischen Zahlentheorie benötigen wir nirgends mehr, als etwa in dem Buch [12] von O'Meara enthalten ist (wobei der komplizierte § 71 durch [14] § 2 ersetzt werden kann). Zwar benutzen wir auch zwei Existenzsätze über unverzweigte quadratische Körpererweiterungen aus der Klassenkörpertheorie. Doch lassen sich diese aus dem Weilschen Reziprozitätsgesetz bei Benutzung des Satzes von Hasse-Minkowski und seiner Umkehrung schnell herleiten. Dies wird in einem Anhang zu unserer Arbeit erläutert (vgl. [5], Kap. VIII).

§ 1. Modulare Formen über Dedekind-Ringen

Der Inhalt dieses Abschnittes ist mehr oder weniger „wohlbekannt". (Vgl. [4, 7, 10].)

1.1. *Modulare Formen.* Es sei A ein Dedekind-Ring mit Quotientenkörper F. Wir setzen $\mathrm{char}(F)\neq 2$ voraus. Es sei Ω ein eindimensionaler F-Vektorraum und $W(\Omega)$ die Witt-Gruppe der nicht-singulären quadratischen Formen $q\colon V\to\Omega$, die auf endlich-dimensionalen F-Vektorräumen V definiert sind und Werte in Ω haben. Da wir $\mathrm{char}(F)\neq 2$ voraussetzen, identifizieren wir über F quadratische Formen q mit symmetrischen Bilinearformen b durch die Gleichung $q(x)=\frac{1}{2}b(x,x)$. Es sei $\Gamma\subset\Omega$ ein von 0 verschiedener endlich-erzeugter (also projektiver) A-Modul und M ein endlich-erzeugter projektiver A-Modul. Eine symmetrische Bilinearform

$$b\colon M\times M\to\Gamma$$

heißt nicht-singulär (oder Γ-modular), wenn b einen Isomorphismus $M\cong\mathrm{Hom}_A(M,\Gamma)$ induziert. Ist $b\colon V\times V\to\Omega$ nicht-singulär, so heißt ein Gitter M auf V Γ-modular falls $b|_{M\times M}$ Γ-modular ist. Eine quadratische Form $q\colon M\to\Gamma$ heißt Γ-modular, falls die zugehörige symmetrische Bilinearform

$$b_q(m,m'):=q(m+m')-q(m)-q(m')$$

Γ-modular ist. Es ist offensichtlich, daß die direkte Summe Γ-modularer Formen wieder Γ-modular ist.

1.2. *Hyperbolische Formen.* Ist M endlich-erzeugter projektiver A-Modul und $q\colon M\to\Gamma$ eine beliebige (nicht notwendig Γ-modulare) quadratische Form, so wird eine quadratische Form $\mathbb{H}(M,q)$ (metabolische Form im Sinne von [7]) auf dem Modul $M\oplus M^*$ mit $M^*=\mathrm{Hom}_A(M,\Gamma)$ definiert durch

$$M\oplus M^*\to\Gamma,\qquad (m,f)\mapsto q(m)+f(m).$$

Die zugehörige symmetrische Bilinearform ist dann

$$(M\oplus M^*)\times(M\oplus M^*)\to\Gamma,$$
$$(m,f)\times(m',f')\mapsto b_q(m,m')+f(m')+f'(m).$$

Man prüft leicht nach, daß $\mathbb{H}(M, q)$ Γ-modular ist. M^* ist ein totalisotroper Untermodul, der sein eigener Orthogonalraum ist. Die Untermoduln M und M^* stehen unter der Bilinearform zu $\mathbb{H}(M, q)$ in Dualität. Ist $q=0$, so ist auch M totalisotrop und $M=M^{\perp}$. In diesem Fall schreiben wir $\mathbb{H}(M)=\mathbb{H}(M, 0)$ und nennen $\mathbb{H}(M)$ die hyperbolische Form zu M.

Geht man statt von einer quadratischen Form von einer symmetrischen Bilinearform b: $M \times M \to \Gamma$ aus, so definiert man die Form $\mathbb{H}(M, b)$ ganz analog. Natürlich ist $b_{\mathbb{H}(M, q)}=\mathbb{H}(M, b_q)$.

Die Grothendieck-Gruppe der Γ-modularen quadratischen Formen modulo der Untergruppe, die von den hyperbolischen Formen $\mathbb{H}(M)$ erzeugt wird, heißt Witt-Gruppe der Γ-modularen quadratischen Formen und wird mit $W(\Gamma)$ bezeichnet. Analog wird die Witt-Gruppe der Γ-modularen symmetrischen Bilinearformen definiert und mit $B(\Gamma)$ bezeichnet. $W(\Gamma)$ wird als Untergruppe von $B(\Gamma)$ aufgefaßt vermöge $q \mapsto b_q$. Ist 2 eine Einheit in A, so ist $W(\Gamma)=B(\Gamma)$.

Bemerkung 1.3. Eine Form kann offenbar nur dann Γ-modular sein, wenn für die Steinitz-Invariante $\mathfrak{m}$ von M und für die Steinitz-Invariante $\mathfrak{c}$ von Γ in der Idealklassengruppe C von A die Gleichung

$$\mathfrak{m}^2=\mathfrak{c}^{\mathrm{Rang}(M)}$$

gilt.

Lemma 1.4. *Die kanonischen Homomorphismen*

$$W(\Gamma) \to W(\Omega), \qquad q \mapsto q \otimes_A F$$

$$B(\Gamma) \to B(\Omega), \qquad b \mapsto b \otimes_A F$$

sind injektiv.

Beweis. Wir zeigen nur die Injektivität von $B(\Gamma) \to B(\Omega)$; für quadratische Formen verläuft der Beweis analog. O.B.d.A. nehmen wir an $\Omega=F$ und $\Gamma=\mathfrak{a}$, wobei $\mathfrak{a}$ ein gebrochenes Ideal ist. Sei b: $M \times M \to \mathfrak{a}$ eine $\mathfrak{a}$-modulare Form. Wir betrachten M als Gitter in dem F-Vektorraum $V:=M \otimes_A F$, und wir setzen b auf V fort. Die Fortsetzung bezeichnen wir ebenfalls mit b.

Angenommen (V, b) ist hyperbolisch, d.h. $V=V_1+V_2$ mit $V_1^{\perp}=V_1$, $V_2^{\perp}=V_2$. Es sei $M_1:=V_1 \cap M$. Der A-Modul M/M_1 ist torsionsfrei und endlich erzeugt, also projektiv. Daher besitzt M eine Zerlegung $M=M_1+M_2$ mit $M_1^{\perp}=M_1$, $M_1 \cap M_2=0$. Unter b können wir M_1 mit $M_2^*=\mathrm{Hom}_A(M_2, \mathfrak{a})$ identifizieren. Wir haben also

$$(M, b) \cong \mathbb{H}(N, b_N)$$

mit $N:=M_2$, $b_N:=b|_{N \times N}$. Daß (M, b) das Element 0 von $B(\mathfrak{a})$ repräsentiert, folgt nun aus

Lemma 1.5. *Für einen $\mathfrak{a}$-modularen Raum $\mathbb{H}(N, b)$ gilt*

$$\mathbb{H}(N, b) \oplus \mathbb{H}(N, -b) \cong \mathbb{H}(N) \oplus \mathbb{H}(N, -b).$$

Beweis. Wir betrachten in $F=\mathbb{H}(N,b)\oplus\mathbb{H}(N,-b)$ den von $(u,u^*,u,0)$, $u\in N$, $u^*\in N^*$ erzeugten Unterraum $\hat{N}$. Man stellt ohne Schwierigkeiten fest, daß $\hat{N}$ isomorph zu $\mathbb{H}(N)$ ist. Insbesondere ist also $\hat{N}$ $\mathfrak{a}$-modular, also ist das orthogonale Komplement $\hat{N}^\perp$ $\mathfrak{a}$-modular und $F=\hat{N}\oplus\hat{N}^\perp$. Der Modul $\hat{N}^\perp$ besteht aus den (v,v^*,w,w^*), die zu allen $(u,u^*,u,0)$ orthogonal sind. Es ergeben sich folgende Bedingungen: $v=0$ und

$$v^*(u)-b(u,w)+w^*(u)=0.$$

Fixiert man (w,w^*), so hat man eine eindeutig bestimmte lineare Abbildung

$$\varphi(w,w^*)\colon\ N\to\mathfrak{a},\qquad u\mapsto b(u,w)-w^*(u).$$

Also ist $v^*=\varphi(w,w^*)$ eindeutig durch (w,w^*) bestimmt. Offensichtlich ist aber

$$\mathbb{H}(N,-b)\to\hat{N}^\perp$$
$$(w,w^*)\mapsto(0,\varphi(w,w^*),w,w^*)$$

eine Isometrie, q.e.d.

Auf Grund von Lemma 1.3 werden wir $W(\Gamma)$ und $B(\Gamma)$ als Untergruppen von $W(\Omega)=B(\Omega)$ auffassen.

Die Menge der maximalen Ideale von A werde mit $\mathrm{Max}(A)$ bezeichnet. Für $\mathfrak{p}\in\mathrm{Max}(A)$ führen wir folgende Bezeichnungen ein:

$A_\mathfrak{p}=$ Komplettierung von A an der „Stelle" $\mathfrak{p}$,

$F_\mathfrak{p}=$ Komplettierung von F an der „Stelle" $\mathfrak{p}$,

$\Omega_\mathfrak{p}=\Omega\otimes_F F_\mathfrak{p}$,

$\Gamma_\mathfrak{p}=\Gamma\otimes_A A_\mathfrak{p}$.

Satz 1.6. *Die kanonischen Sequenzen*

$$0\to W(\Gamma)\to W(\Omega)\to\coprod_{\mathfrak{p}\in\mathrm{Max}(A)}W(\Omega_\mathfrak{p})/W(\Gamma_\mathfrak{p}),$$
$$0\to B(\Gamma)\to B(\Omega)\to\coprod_{\mathfrak{p}\in\mathrm{Max}(A)}B(\Omega_\mathfrak{p})/B(\Gamma_\mathfrak{p})$$

sind exakt.

Beweisskizze. (Vgl. [4, 7, 10].) O.B.d.A. sei wieder $\Omega=F$, $\Gamma=\mathfrak{a}$. Ersichtlich sind die zusammengesetzten Homomorphismen gleich 0. Es sei $b\colon V\times V\to F$ eine symmetrische Bilinearform, so daß $b_\mathfrak{p}$ an jeder Stelle $\mathfrak{p}$ in $B(\mathfrak{a}_\mathfrak{p})$ liegt. Wir wählen ein beliebiges A-Gitter M auf V. An fast allen Primstellen ist M $\mathfrak{a}$-modular (denn $\mathfrak{a}$-modular = unimodular fast überall). An den verbleibenden Stellen kann man wegen unserer Voraussetzung über b in $V_\mathfrak{p}$ ein $\mathfrak{a}_\mathfrak{p}$-modulares Gitter $M'_\mathfrak{p}$ finden (vgl. [7] 13.3.3). Nach elementarer Gittertheorie ([12], 81:14) hat V ein Gitter N mit $N_\mathfrak{p}=M_\mathfrak{p}$, sofern $M_\mathfrak{p}$ $\mathfrak{a}_\mathfrak{p}$-modular ist, und $N_\mathfrak{p}=M'_\mathfrak{p}$ sonst. N ist $\mathfrak{a}$-modular, also liegt b im Bild von $B(\mathfrak{a})$. Für quadratische Formen verfährt man analog.

Bemerkung 1.7. Die kanonischen Abbildungen $B(\Omega) \to B(\Omega_\mathfrak{p})/B(\Gamma_\mathfrak{p})$ aus Satz 1.6 entsprechen den bekannten Restklassenformen ([6, 7, 9, 14, 16]). Ist $A_\mathfrak{p}$ vollständiger diskreter Bewertungsring mit maximalem Ideal $\mathfrak{p}$, Primelement π, Quotientenkörper $F_\mathfrak{p}$ (char $F_\mathfrak{p} \neq 2$) und Restklassenkörper $k(\mathfrak{p})$, und ist b eine symmetrische Bilinearform über F, so kann man eine Basis finden, bezüglich der die Form b sich folgendermaßen schreibt

$$a_1 x_1 y_1 + \cdots + a_m x_m y_m + \pi b_{m+1} x_{m+1} y_{m+1} + \cdots + \pi b_n x_n y_n$$

mit Einheiten a_i, b_j. Die Form

$$\bar{a}_1 \bar{x}_1 \bar{y}_1 + \cdots + \bar{a}_m \bar{x}_m \bar{y}_m$$

liefert ein wohldefiniertes Element von $B(k(\mathfrak{p}))$. Der sich so ergebende *kanonische* Homomorphismus

$$\partial_\mathfrak{p}^1 \colon B(F_\mathfrak{p}) \to B(k(\mathfrak{p}))$$

heißt 1. Restklassenform. Der Kern ist $B(\mathfrak{p})$. Man hat also eine kanonische exakte Sequenz

$$0 \to B(\mathfrak{p}) \to B(F_\mathfrak{p}) \xrightarrow{\partial_\mathfrak{p}^1} B(k(\mathfrak{p})) \to 0.$$

Die Form

$$\bar{b}_{m+1} \bar{x}_{m+1} \bar{y}_{m+1} + \cdots + \bar{b}_n \bar{x}_n \bar{y}_n$$

liefert ebenfalls ein wohldefiniertes (aber von der Wahl von π abhängiges) Element $\partial_\mathfrak{p}^2(b)$ von $B(k(\mathfrak{p}))$. Man hat dann eine von π abhängige exakte Sequenz

$$0 \to B(A_\mathfrak{p}) \to B(F_\mathfrak{p}) \xrightarrow{\partial_\mathfrak{p}^2} B(k(\mathfrak{p})) \to 0.$$

$\partial_\mathfrak{p}^2$ heißt 2. Restklassenform.

Ist $\mathfrak{p}$ nicht-dyadisch (char$(k(\mathfrak{p})) \neq 2$), so hat man nach dem Henselschen Lemma ferner kanonische Isomorphismen

$$B(A_\mathfrak{p}) = B(k(\mathfrak{p})) = W(k(\mathfrak{p})) = W(A_\mathfrak{p}),$$

in der Situation von 1.6 hat man also

$$W(k(\mathfrak{p})) \cong W(\Omega_\mathfrak{p})/W(\Gamma_\mathfrak{p}) = B(\Omega_\mathfrak{p})/B(\Gamma_\mathfrak{p}) \cong B(k(\mathfrak{p})).$$

Ist dagegen $\mathfrak{p}$ eine dyadische Primstelle (d. h. char $k(\mathfrak{p}) = 2$), so gilt $W(\Gamma_\mathfrak{p}) \neq B(\Gamma_\mathfrak{p})$. Ist z. B. $k(\mathfrak{p})$ vollkommen, so gilt $B(k(\mathfrak{p})) \cong \mathbb{Z}/2\mathbb{Z}$, d. h. $B(\Gamma_\mathfrak{p})$ ist vom Index 2 in $B(\Omega_\mathfrak{p})$. Andererseits ist

$$W(\Gamma_\mathfrak{p}) \cong W(k(\mathfrak{p})) \cong k(\mathfrak{p})/\wp(k(\mathfrak{p}))$$

mit $\wp(x) = x^2 + x$. Hier wird der erste Isomorphismus durch Hensels Lemma und der zweite durch die Arf-Invariante hergestellt. Für endliches k ist also $W(\Gamma_\mathfrak{p}) \cong \mathbb{Z}/2\mathbb{Z}$.

§ 2. Die Witt-Gruppe eines algebraischen Zahlkörpers

Sei zunächst A ein beliebiger Dedekind-Ring mit Quotientenkörper F. Sei $\Omega = F$ und $\Gamma = \mathfrak{a}$ ein (gebrochenes) Ideal. Es sei $\mathfrak{a} = \prod \mathfrak{p}^{a(\mathfrak{p})}$, $a(\mathfrak{p}) \in \mathbb{Z}$, wobei hier und im folgenden $\mathfrak{p}$ die Menge $\mathrm{Max}(A)$ der maximalen Ideale von A durchläuft.

Wir wollen die kanonische exakte Sequenz

$$0 \to B(\mathfrak{a}) \to B(F) \to \coprod B(F_{\mathfrak{p}})/B(\mathfrak{a}_{\mathfrak{p}})$$

nach rechts fortsetzen. C sei die Idealklassengruppe von A. Mit $\hat{c}_{\mathfrak{p}}^{\mathfrak{a}}$ oder kurz $\hat{c}_{\mathfrak{p}}$ bezeichnen wir die 2. Restklassenform auf $B(F_{\mathfrak{p}})$, falls $\mathfrak{p}$ in $\mathfrak{a}$ in gerader Potenz enthalten ist, und die 1. Restklassenform sonst. Dazu muß (im 1. Falle) eine Ortsuniformisierende $\pi_{\mathfrak{p}}$ fest ausgewählt werden. Nach Bemerkung 1.7 liefert $\hat{c}_{\mathfrak{p}}$ einen Isomorphismus von $B(F_{\mathfrak{p}})/B(\mathfrak{a}_{\mathfrak{p}})$ auf $B(k(\mathfrak{p}))$. Wir betrachten nun den kanonischen surjektiven Homomorphismus

$$\coprod B(F_{\mathfrak{p}})/B(\mathfrak{a}_{\mathfrak{p}}) \to C/C^2,$$

der ein Element $\{\bar{\eta}_{\mathfrak{p}}\}$ auf die Klasse von $\prod \mathfrak{p}^{\dim \hat{c}_{\mathfrak{p}} \eta_{\mathfrak{p}}}$ abbildet. (Dieser Homomorphismus hängt nicht von der Wahl der $\pi_{\mathfrak{p}}$ ab.)

Lemma 2.1. *Das Bild eines ungerade-dimensionalen Elements von $B(F)$ unter der zusammengesetzten Abbildung*

$$B(F) \to \coprod_{\mathfrak{p}} B(F_{\mathfrak{p}})/B(\mathfrak{a}_{\mathfrak{p}}) \to C/C^2$$

ist die Klasse von $\mathfrak{a}$. Das Bild eines gerade-dimensionalen Elements ist also trivial.

Beweis. Es genügt, das für eine eindimensionale Form axy zu beweisen. Das Bild dieser Form in C/C^2 wird durch das Ideal

$$\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(a) + a(\mathfrak{p})} \equiv (a)\, \mathfrak{a} \equiv \mathfrak{a}$$

gegeben, q.e.d.

Es bezeichne B_0 (bzw. W_0) die Untergruppe der gerade-dimensionalen Formen. Ist $\mathfrak{a}$ nicht Quadrat in C, so hat man einen Komplex

$$0 \to B(\mathfrak{a}) \to B_0(F) \to \coprod B(F_{\mathfrak{p}})/B(\mathfrak{a}_{\mathfrak{p}}) \to C/C^2 \to 0.$$

Dabei ist zu beachten, daß $B(\mathfrak{a})$ nach 1.3 jetzt nur aus Formen gerader Dimensionen besteht. Ist $\mathfrak{a}$ ein Quadrat in C, so hat man einen Komplex

$$0 \to B(\mathfrak{a}) \to B(F) \to \coprod B(F_{\mathfrak{p}})/B(\mathfrak{a}_{\mathfrak{p}}) \to C/C^2 \to 0.$$

Satz 2.2. *Es sei F ein algebraischer Zahlkörper und A ein Dedekind-Ring mit Quotientenkörper F, z.B. der Ring der ganzen Zahlen von F. Dann sind diese Sequenzen exakt.*

Beweis. Es genügt, für jedes $\mathfrak{a}$ die Exaktheit der Sequenz

$$0 \to B_0(\mathfrak{a}) \to B_0(F) \to \coprod B(F_\mathfrak{p})/B(\mathfrak{a}_\mathfrak{p}) \to C/C^2 \to 0$$

einzusehen. Wird das Element $\{\bar{\eta}_\mathfrak{p}\} \in B(F_\mathfrak{p})/B(\mathfrak{a}_\mathfrak{p})$ auf das Einselement von C/C^2 abgebildet, so existiert ein $d \in F^*$ mit

$$\dim \hat{c}_\mathfrak{p}(\eta_\mathfrak{p}) \equiv v_\mathfrak{p}(d) + a(\mathfrak{p}) \pmod 2.$$

Wir konstruieren jetzt für jedes $\mathfrak{p}$ eine vierdimensionale Form $\zeta_\mathfrak{p}$ über $F_\mathfrak{p}$, die Diskriminate d hat, und so daß gilt $\bar{\eta}_\mathfrak{p} = \bar{\zeta}_\mathfrak{p}$ in $B(F_\mathfrak{p})/B(\mathfrak{a}_\mathfrak{p})$. Es ist leicht zu sehen, daß das immer möglich ist. An den dyadischen Stellen können wir außerdem das Hasse-Minkowski-Symbol $c_\mathfrak{p}(\zeta_\mathfrak{p})$ beliebig vorschreiben. An den reellen Primstellen und an den endlichen Primstellen, die nicht in $\mathrm{Max}(A)$ liegen, wählen wir ebenfalls vierdimensionale Formen $\zeta_\mathfrak{p}$ mit Diskriminante d. Diese Wahlen können so vorgenommen werden, daß fast alle Hasse-Minkowski-Symbole gleich 1 sind. Indem wir notfalls $\zeta_\mathfrak{p}$ an einer einzigen dyadischen Primstelle abändern, können wir erreichen, daß $\prod c_\mathfrak{p}(\zeta_\mathfrak{p}) = 1$. Nach [19], Satz 21 oder [12], 72:1 existiert eine vierdimensionale Form ζ über F mit $\zeta \otimes F_\mathfrak{p} = \zeta_\mathfrak{p}$ für alle $\mathfrak{p}$, also mit dem Bild $\{\bar{\eta}_\mathfrak{p}\}$ in $\coprod B(F_\mathfrak{p})/B(\mathfrak{a}_\mathfrak{p})$. q.e.d.

Bemerkung. Dieser Satz wurde unabhängig von uns von Milnor [10] bewiesen.

Wir haben in 1.7 schon darauf hingewiesen, daß man $\coprod B(F_\mathfrak{p})/B(\mathfrak{a}_\mathfrak{p})$ unkanonisch durch $\coprod B(k(\mathfrak{p}))$ ersetzen kann. In einem kuriosen Fall kann dies in kanonischer Weise geschehen:

Satz 2.3. *Es sei $F/\mathbb{Q}$ normal und A der Ring der ganzen Zahlen von F. Es sei D die Differente von $F/\mathbb{Q}$. Dann hat man eine kanonische exakte Sequenz*

$$0 \to B(D) \to B(F) \xrightarrow{\hat{c}} \coprod_\mathfrak{p} B(k(\mathfrak{p})) \to C/C^2 \to 0.$$

Beweis. Wie wir noch zeigen werden (5.4) ist die Differente ein Quadrat in C; deshalb haben wir eine exakte Sequenz. Es ist jetzt noch eine kanonische Wahl des Homomorphismus $\hat{c}$ anzugeben. Es sei $D = \prod \mathfrak{p}^{m(\mathfrak{p})}$. Ist $m(\mathfrak{p})$ ungerade, so sei

$$\hat{c}_\mathfrak{p}\colon\ B(F) \to B(k(\mathfrak{p}))$$

die kanonische 1. Restklassenform. Ist $m(\mathfrak{p})$ gerade, was fast überall der Fall ist, so ist

$$\hat{c}_\mathfrak{p}\colon\ B(F) \to B(k(\mathfrak{p}))$$

jedenfalls eine 2. Restklassenform. Zunächst bemerken wir, daß an den dyadischen Stellen kein (!) Problem entsteht, weil $W(k(\mathfrak{p})) \cong \mathbb{Z}/2\mathbb{Z}$; es gibt also nur eine 2. Restklassenform. Für eine nicht-dyadische Stelle $\mathfrak{p}$ gilt, wie wir gleich zeigen werden

$$m(\mathfrak{p}) \equiv e(\mathfrak{p}) - 1 \pmod 2, \qquad (*)$$

wobei $e(\mathfrak{p})$ den Verzweigungsindex bezeichnet. Ist $m(\mathfrak{p})$ gerade, so ist also $e(\mathfrak{p})$ ungerade, also ist die rationale Primzahl p unter $\mathfrak{p}$ bis auf Quadrate ein uniformisierendes Element für $\mathfrak{p}$. Wir wählen dann $\hat{c}_\mathfrak{p}$ als 2. Restklassenform bzgl. p.

Der Beweis von (*) ergibt sich aus der Hilbertschen Formel ([15], Chap. IV, § 1, Prop. 4)

$$m(\mathfrak{p}) = \sum_{i=0}^{\infty} ([V_i : 1] - 1),$$

wobei $V_0 \supset V_1 \supset \cdots$ die Folge der Verzweigungsgruppen bei $\mathfrak{p}$ bezeichnet. Es ist V_i eine p-Gruppe für $i \geqq 1$ und $[V_0 : 1] = e(\mathfrak{p})$, q.e.d.

§ 3. Lokale Untersuchung differentialwertiger Formen

Sei F ein algebraischer Zahlkörper mit ganzen Zahlen A. Sei

$$T = \{z \in \mathbb{C} \mid |z| = 1\}$$

und $\mathbf{A}(F)$ der Adelring von F. Es bezeichne $\Omega = \Omega(F)$ die additiv geschriebene Gruppe der stetigen Gruppenhomomorphismen ω: $\mathbf{A}(F)/F \to T$. Es ist Ω in kanonischer Weise ein eindimensionaler F-Vektorraum. Die Multiplikation mit Skalaren $a \in F$ ist durch $(a\omega)(x) = \omega(ax)$ definiert. Zu einer diskreten oder archimedischen Primstelle $\mathfrak{p}$ bezeichne $\Omega_{\mathfrak{p}} = \Omega(F_{\mathfrak{p}})$ die Gruppe der stetigen Homomorphismen von $F_{\mathfrak{p}}$ nach T. Dann ist $\Omega_{\mathfrak{p}}$ in analoger Weise ein eindimensionaler $F_{\mathfrak{p}}$-Vektorraum und man hat einen kanonischen Isomorphismus $\Omega(F) \otimes_F F_{\mathfrak{p}} \cong \Omega(F_{\mathfrak{p}})$. Die Elemente von Ω heißen Differentiale von F. (Vgl. [2] Chap. 13 oder [18] für Einzelheiten.) Die lokalen Komponenten $\omega_{\mathfrak{p}} \in \Omega(F_{\mathfrak{p}})$ eines Elementes $\omega \in \Omega$ sind die Homomorphismen

$$F_{\mathfrak{p}} \hookrightarrow \mathbf{A}(F) \to \mathbf{A}(F)/F \xrightarrow{\omega} T.$$

E/F sei endliche algebraische Erweiterung. Man hat einen kanonischen F-linearen Einschränkungshomomorphismus

$$Tr_{E/F} \colon \Omega(E) \to \Omega(F), \qquad \omega \mapsto \omega|_{\mathbf{A}(F)/F}.$$

Indem man einer quadratischen Form q: $V \to \Omega(E)$ über E die Form $Tr_{E/F} \circ q$: $V \to \Omega(F)$ über F zuordnet, erhält man einen Verlagerungshomomorphismus

$$Tr^*_{E/F} \colon W(\Omega(E)) \to W(\Omega(F))$$

(vgl. [6, 14]). Analog hat man zu einer Primstelle $\mathfrak{p}$ von F und einer über $\mathfrak{p}$ liegenden Primstelle $\mathfrak{P}$ von E einen Einschränkungshomomorphismus $Tr_{E_{\mathfrak{P}}/F_{\mathfrak{p}}} = Tr_{\mathfrak{P}/\mathfrak{p}}$ von $\Omega(E_{\mathfrak{P}})$ nach $\Omega(F_{\mathfrak{p}})$ und dazu eine Verlagerung

$$Tr^*_{\mathfrak{P}/\mathfrak{p}} \colon W(\Omega(E_{\mathfrak{P}})) \to W(\Omega(F_{\mathfrak{p}})).$$

Lemma 3.1. *Ist E/F endliche algebraische Erweiterung und $\mathfrak{p}$ eine endliche oder unendliche Primstelle von F, so gilt für alle $\omega \in \Omega(E)$*

$$(Tr_{E/F}\,\omega)_{\mathfrak{p}} = \sum_{\mathfrak{P}/\mathfrak{p}} Tr_{\mathfrak{P}/\mathfrak{p}}\,\omega_{\mathfrak{P}}.$$

Beweis. Durch unmittelbares Nachrechnen.

Lemma 3.2. *In der Situation des letzten Lemmas gilt für alle $\Omega(E)$-wertigen quadratischen Formen Q*

$$(Tr^*_{E/F}(Q))_\mathfrak{p} \cong \bigoplus_{\mathfrak{P}/\mathfrak{p}} Tr^*_{\mathfrak{P},\mathfrak{p}}(Q_\mathfrak{P}).$$

Beweis. Unter Verwendung des letzten Lemmas durch Nachrechnen.

Für $\omega \in \Omega_\mathfrak{p}$ definiert man die Ordnung $v_\mathfrak{p}(\omega)$ als das maximale $n \in \mathbb{Z}$ mit $\omega(\mathfrak{p}^{-n}) = \{1\}$. Die Differentiale der Ordnung $\geqq 0$ bilden einen freien $A_\mathfrak{p}$-Modul $\Gamma(F_\mathfrak{p}) = \Gamma_\mathfrak{p}$ vom Rang 1. Für $\omega \in \Omega$ definieren wir $v_\mathfrak{p}(\omega) = v_\mathfrak{p}(\omega_\mathfrak{p})$. Die Differentiale von F, die überall Ordnung $\geqq 0$ haben, bilden einen projektiven A-Modul $\Gamma = \Gamma(F)$ vom Rang 1. Die Steinitz-Invariante von Γ ist die Idealklasse der Differente von $F/\mathbb{Q}$. (Vgl. [2], Chap. 13.)

Lemma 3.3. *Sei E/F endliche Erweiterung und $b: V \times V \to \Omega(E)$ symmetrische Bilinearform über E. Ist ein Gitter M $\Gamma(E)$-modular bezüglich b, so ist es $\Gamma(F)$-modular bezüglich $Tr^* b$.*

Zum Beweis benutzen wir folgendes Lemma: Es sei A ein kommutativer Ring, B eine kommutative A-Algebra, die endlich erzeugt ist als A-Modul, Γ sei ein A-Modul und Δ sei ein B-Modul.

Lemma 3.4. *Ist $b: M \times M \to \Delta$ eine nicht-singuläre symmetrische Bilinearform über B und ist $s: \Delta \to \Gamma$ eine A-lineare Abbildung, derart daß*

$$B \times \Delta \to \Gamma, \qquad (\beta, \delta) \mapsto s(\beta\delta)$$

nicht-singulär ist (d.h. Isomorphismen $B \cong \mathrm{Hom}_A(\Delta, \Gamma)$, $\Delta \cong \mathrm{Hom}_A(B, \Gamma)$ liefert), so ist

$$s \circ b: M \times M \to \Gamma$$

nicht-singuläre symmetrische Bilinearform über A.

Beweis. (Vgl. [8].) Sei $m \in M$, $m \neq 0$. Dann gibt es ein $m' \in M$ mit $b(m, m') \neq 0$. Dann gibt es ein $\beta \in B$ mit $s(\beta\, b(m, m')) = s\, b(m, m'\beta) \neq 0$. Also ist

$$M \to \mathrm{Hom}_A(M, \Gamma)$$

injektiv.

Wir beweisen nun die Surjektivität dieser Abbildung. Sei also $\varphi: M \to \Gamma$ eine A-lineare Abbildung. Jedes $m \in M$ definiert eine A-lineare Abbildung

$$B \to \Gamma, \qquad \beta \mapsto \varphi(m\beta).$$

Es gibt also ein eindeutig bestimmtes Element $\psi(m) \in \Delta$ mit

$$s(\beta\psi(m)) = \varphi(\beta m) \qquad \text{für alle } \beta \in B. \tag{*}$$

Damit haben wir eine Abbildung

$$\psi: M \to \Delta$$

definiert. Es ist trivial, daß diese Abbildung additiv ist, und es ist leicht zu sehen, daß sie auch B-linear ist. Also gibt es ein $m' \in M$ mit

$$b(m, m') = \psi(m) \qquad \text{für alle } m \in M.$$

Aus (*) ergibt sich dann mit $\beta = 1$

$$sb(m, m') = \varphi(m)$$

für alle $m \in M$, q.e.d.

Beweis von 3.3. Wir brauchen die Behauptung nur im Lokalen zu prüfen. Sei also F $\mathfrak{p}$-adischer Körper, E/F endliche algebraische Erweiterung und B der Ring der ganzen Zahlen von E mit maximalen Ideal $\mathfrak{P}$. Wir übernehmen den Beweis im wesentlichen aus [6]. Es genügt, die Fälle E/F unverzweigt und E/F rein-verzweigt zu betrachten. Nach dem letzten Lemma genügt es jeweils zu beweisen, daß

$$Tr\colon\ B \times \Gamma(E) \to \Gamma(F), \qquad (\beta, \omega) \mapsto Tr(\beta\omega)$$

nicht-singulär ist.

(i) Sei also zunächst E/F unverzweigt und $x_1, \ldots, x_n$ eine Basis von B über A. Mit s bezeichnen wir die Spur von E nach F. Sei nun $\omega_0\colon F \to T$ ein Charakter der Ordnung 0, d. h. $\omega_0(A) = \{1\}$, $\omega_0(\mathfrak{p}^{-1}) \neq \{1\}$. Dann ist $\omega = \omega_0 s$ ein Charakter der Ordnung 0 auf E. Die Matrix der Bilinearform

$$Tr\colon\ B \times \Gamma(E) \to \Gamma(F)$$

bzgl. der Basen $\{x_i\}$, $\{x_i\omega\}$, $\{\omega_0\}$ von B, $\Gamma(E)$, $\Gamma(F)$ respektive ist $(s(x_i x_j))$. Sie ist nicht-singulär, weil E/F unverzweigt ist.

(ii) Sei jetzt E/F rein-verzweigt. Dann existiert eine Uniformisierende τ von E mit Minimalgleichung $\tau^n + a_{n-1}\tau^{n-1} + \cdots + t = 0$ mit $E = F(\tau)$. Dann ist t eine Uniformisierende von F. Es sei $\omega_0\colon F \to T$ ein Charakter der Ordnung 0 mit $\omega_0(t^{-1}) \neq 1$. Definiere die F-lineare Abbildung $s\colon E \to F$ durch

$$s(1) = \cdots = s(\tau^{n-2}) = 0, \qquad s(\tau^{n-1}) = 1.$$

Für $\omega = \omega_0 s$ gilt dann $\omega(B) = \{1\}$, denn $B = A + \tau A + \cdots + \tau^{n-1}A$, und $\omega(\tau^{-1}) \neq 1$, denn

$$\tau^{-1} = -t^{-1}(a_1 + \cdots + a_{n-1}\tau^{n-2} + \tau^{n-1}).$$

Also hat ω die Ordnung 0. Die Matrix der Bilinearform $Tr\colon B \times \Gamma(E) \to \Gamma(F)$ bezüglich der Basen $\{1, \tau, \ldots, \tau^{n-1}\}$; $\{\omega, \tau\omega, \ldots, \tau^{n-1}\omega\}$, $\{\omega_0\}$ ist

$$\begin{pmatrix} 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \\ \vdots & & & & & \iddots & \\ \vdots & & & & \iddots & & \\ \vdots & & & \iddots & & & \\ \vdots & & \iddots & & & & \\ \vdots & \iddots & & * & & & \\ \iddots & & & & & & \\ 0 & & & & & & \\ 1 & & & & & & \end{pmatrix},$$

also nicht-singulär; q.e.d.

§ 4. Das Weilsche Reziprozitätsgesetz

Wir beweisen das Weilsche Reziprozitätsgesetz [17], S. 179, Proposition 5 in etwas anderer Form unter Verwendung der in [6] benutzten Methode und der lokalen Ergebnisse aus § 3.

T_8 sei die Gruppe der 8-ten Einheitswurzeln, die wir uns immer als Untergruppe von T denken. Im übrigen übernehmen wir die früheren Bezeichnungen.

Satz 4.1. *Es sei F algebraischer Zahlkörper und Ω der eindimensionale Vektorraum der Differentiale über F. Dann gibt es für alle endlichen und reellen Primstellen $\mathfrak{p}$ Homomorphismen*

$$\gamma_{\mathfrak{p}}\colon\ W(\Omega_{\mathfrak{p}}) \to T_8$$

mit folgenden Eigenschaften:

(i) *Für jedes $Q \in W(\Omega)$ gilt $\gamma_{\mathfrak{p}}(Q_{\mathfrak{p}}) = 1$ für fast alle $\mathfrak{p}$.*

(ii) *Für jedes $Q \in W(\Omega)$ gilt*

$$\prod_{\mathfrak{p}} \gamma_{\mathfrak{p}}(Q_{\mathfrak{p}}) = 1 \qquad (\textit{Reziprozitätsgesetz}).$$

(iii) *Ist $\varphi_{\mathfrak{p}}$ anisotrope vierdimensionale Form der Diskriminante 1 von $W(\Omega_{\mathfrak{p}})$, so gilt $\gamma_{\mathfrak{p}}(\varphi_{\mathfrak{p}}) = -1$.*

Korollar 4.2. (Hilbertsches Reziprozitätsgesetz.) *Ist (a, b) eine Quaternionen-Algebra über F, so ist die Anzahl der Primstellen $\mathfrak{p}$, an denen (a, b) nicht zerfällt, endlich und gerade.*

Beweis. Durch Anwendung von 4.1 auf die Normform der Quaternionen-Algebra (a, b). (Vgl. [14].)

Beweis von 4.1. Es sei zunächst $F = \mathbb{Q}$. In [14] wurde bewiesen, daß es Homomorphismen

$$\gamma'_{\mathfrak{p}}\colon\ W(\mathbb{Q}_{\mathfrak{p}}) \to T_8$$

gibt, die analoge Eigenschaften haben. Wir wiederholen die Definition der $\gamma'_{\mathfrak{p}}$: Sei $\alpha = e^{\frac{1}{4}\pi i}$. Wir definieren

$$\begin{aligned}
\gamma'_{\infty}\colon\ & W(\mathbb{R}) \to T_8, && \langle 1\rangle \mapsto \alpha,\\
\gamma'_{2}\colon\ & W(\mathbb{Q}_2) \to T_8, && \langle 1\rangle \mapsto \alpha^{-1},\\
& && \langle 1,1,1,5\rangle \mapsto 1,\\
& && \langle -1,2\rangle \mapsto 1;
\end{aligned}$$

für p ungerade Primzahl

$$\begin{aligned}
\gamma'_{p}\colon\ & W(\mathbb{Q}_p) \to T_8, && \langle \varepsilon\rangle \mapsto 1, \text{ falls } \varepsilon \text{ Einheit},\\
& && \langle p\rangle \mapsto \alpha^{p-1},\\
& && \varphi_p \mapsto -1.
\end{aligned}$$

Dadurch sind die γ'_p eindeutig bestimmt.

Offensichtlich ist Bedingung (iii) erfüllt, denn $\pm\varphi_\infty = \langle 1, 1, 1, 1\rangle$ und $\varphi_2 = \langle 1, 1, 1, 1\rangle$. Bedingung (i) ergibt sich aus der Tatsache, daß jedes $a \in \mathbb{Q}^*$ an fast allen Stellen eine Einheit ist, und (ii) ist im wesentlichen der Inhalt des Gaußschen Reziprozitätsgesetzes. Eine Familie $\{\gamma_p\}$ mit den gewünschten Eigenschaften erhalten wir, indem wir durch Wahl irgendeines Basiselementes $\omega \in \Omega(\mathbb{Q})$ die Gruppe $W(\Omega(\mathbb{Q}))$ mit $W(\mathbb{Q})$ und die Gruppen $W(\Omega(\mathbb{Q}_p))$ mit den entsprechenden $W(\mathbb{Q}_p)$ identifizieren. Es ist klar, daß dabei alle Bedingungen, insbesondere (iii), erhalten bleiben.

Sei nun $F/\mathbb{Q}$ eine endliche Erweiterung. Wir definieren $\gamma_\mathfrak{p} = \gamma_p \circ Tr^*_{\mathfrak{p}/p}$ und haben die Eigenschaften (i), (ii), (iii) nachzuprüfen.

(i) $Q \in W(\Omega(F))$ sei gegeben. An fast allen Primstellen existiert ein $\Gamma(F_\mathfrak{p})$-modulares Gitter von maximalem Rang. Nach 3.4 ist an fast allen Stellen dieses Gitter auch $\Gamma(\mathbb{Q}_p)$-modular bezüglich $Tr^*_{\mathfrak{p}/p}(Q_\mathfrak{p})$. Da der Charakter, mit dem wir die differentialwertigen und die gewöhnlichen Formen identifizieren, fast überall Ordnung 0 hat, folgt die Behauptung.

(ii) Für alle $Q \in W(\Omega(F))$ gilt unter Verwendung von 3.2 und dem schon bewiesenen Fall $F = \mathbb{Q}$:

$$\prod_\mathfrak{p} \gamma_\mathfrak{p}(Q_\mathfrak{p}) = \prod_p \Big(\prod_{\mathfrak{p}/p} \gamma_\mathfrak{p}(Q_\mathfrak{p})\Big) = \prod_p \Big(\prod_{\mathfrak{p}/p} \gamma_p \, Tr^*_{\mathfrak{p}/p}(Q_\mathfrak{p})\Big) = \prod_p \gamma_p\Big(\bigoplus_{\mathfrak{p}/p} Tr^*_{\mathfrak{p}/p}(Q_\mathfrak{p})\Big)$$
$$= \prod_p \gamma_p\big(Tr^*_{F/\mathbb{Q}}(Q)\big)_p = 1.$$

(iii) Nur der Fall $\mathfrak{p}$ endlich ist interessant. Nach einem Satz von Milnor [8] ist $Tr^*(\varphi_\mathfrak{p}) \sim \varphi_p$, also $\gamma_\mathfrak{p}(\varphi_\mathfrak{p}) = \gamma_p(\varphi_p) = -1$.

§ 5. Existenz von Reziprozitätsgesetzen. Ein Satz von Armitage

In Analogie zu den Betrachtungen in 4. untersuchen wir Familien von Homomorphismen

$$\gamma_\mathfrak{p}\colon\ W(F_\mathfrak{p}) \to T_8$$

mit folgenden Eigenschaften:

(R 1) *Für fast alle* $\mathfrak{p}$ *gilt* $\gamma_\mathfrak{p}(W(A_\mathfrak{p})) = \{1\}$. Ist insbesondere $Q \in W(F)$, so gilt also $\gamma_\mathfrak{p}(Q) = 1$ für fast alle $\mathfrak{p}$.

(R 2) *Ist* $Q \in W(F)$, *so gilt* $\prod_\mathfrak{p} \gamma_\mathfrak{p}(Q) = 1$.

Eine solche Familie nennen wir Reziprozitätsgesetz. Wir sprechen von einem erzeugenden Reziprozitätsgesetz, falls zusätzlich gilt:

(R 3) *Ist* $\varphi_\mathfrak{p}$ *die anisotrope Quaternionenform über* $F_\mathfrak{p}$, *so gilt* $\gamma_\mathfrak{p}(\varphi_\mathfrak{p}) = -1$.

Bemerkung 5.1. Gilt (R 3) für ein einziges $\mathfrak{p}$, so folgt diese Bedingung wegen (R 2) und der Existenz globaler Quaternionen-Algebren mit vorgeschriebenen Invarianten schon für alle $\mathfrak{p}$.

Ist $\mathfrak{a}$ ein gebrochenes Ideal, so sprechen wir von einem „*Reziprozitätsgesetz für* $\mathfrak{a}$", falls zusätzlich gilt:

(R $\mathfrak{a}$) Für alle $\mathfrak{p}$ ist $\gamma_\mathfrak{p}(W(\mathfrak{a}_\mathfrak{p})) = 1$.

Bemerkung 5.2. Genügt ein erzeugendes Reziprozitätsgesetz den Bedingungen (R a) und (R a') für zwei Ideale a, a', so muß $a' = a b^2$ mit einem weiteren Ideal b sein. Ist nämlich an einer diskreten Stelle p die Ordnung $v_p(a) \equiv 0(2)$, so gilt für die Normform ψ_p der unverzweigten quadratischen Erweiterung von F_p die Gleichung $\gamma_p(\psi_p) = 1$, denn $\psi_p \in W(a_p)$. Mit beliebiger Ortsuniformisierender π_p ist $\psi_p \oplus \pi_p \psi_p = \varphi_p$, also $\gamma_p(\pi_p \psi_p) = -1$. Ist hingegen $v_p(a) \equiv 1(2)$, so muß $\gamma_p(\psi_p) = -1$ und $\gamma_p(\pi_p \psi_p) = 1$ sein.

Wir stellen jetzt folgende naheliegende Frage:

Existenzproblem. Für welche Ideale a existiert ein erzeugendes Reziprozitätsgesetz?

Diese Frage wird durch den folgenden Satz beantwortet, dessen Beweis das Hauptziel dieses Paragraphen ist.

Satz 5.3. *Für* a *existiert ein erzeugendes Reziprozitätsgesetz genau dann, wenn* a *ein Quadrat in der Idealklassengruppe C von F ist.*

Dabei wird sich folgendes Resultat von Hecke ([1, 5, 18]) mitergeben:

Korollar 5.4. *Die Differente* D *von* $F/\mathbb{Q}$ *ist ein Quadrat in der Idealklassen-Gruppe.*

Es ist offensichtlich, daß für a ein erzeugendes Reziprozitätsgesetz genau dann existiert wenn für $a b^2$, b beliebig, eins existiert, oder wenn für (a) $a, a \in F^*$, eins existiert. Die Lösung des Existenzproblems hängt also nur von der Klasse von a in C/C^2 ab.

Lemma 5.5. *Die Differente* D *läßt ein erzeugendes Reziprozitätsgesetz zu.*

Beweis. Identifiziert man nach Wahl eines Basiselementes $\omega \in \Omega(F)$ den Vektorraum $\Omega(F)$ mit F, so entspricht dem Modul $\Gamma(F)$ ein Ideal D', das zur Idealklasse der Differente gehört. Nun läßt $\Gamma(F)$ ein erzeugendes Reziprozitätsgesetz zu (es ist offensichtlich, was damit gemeint ist), nämlich das Weilsche. Der Isomorphismus $\Omega(F) \cong F$ liefert Isomorphismen $\Omega(F_p) \cong F_p$, und die den Homomorphismen γ_p des Weilschen Reziprozitätsgesetzes entsprechenden Homomorphismen $W(F_p) \to T_8$ bilden ein Reziprozitätsgesetz für D', q.e.d.

Nach dem schwachen Approximationssatz kann man nicht-dyadische diskrete Primstellen $p_1, \ldots, p_c$ finden, die eine Basis von C/C^2 bilden. Es sei Δ^+ die Gruppe der unverzweigten totalpositiven Quadratklassen von F. Es besteht ein kanonischer Homomorphismus

$$\Delta^+ \to (\mathbb{Z}/2\mathbb{Z})^c, \quad d \mapsto ([F_{p_i}(\sqrt{d}) : F_{p_i}] - 1)_{i=1,\ldots,c}.$$

Der Existenzsatz der Klassenkörpertheorie besagt insbesondere (s. § 7).

Lemma 5.6. *Die eben beschriebene Abbildung* $\Delta^+ \to (\mathbb{Z}/2\mathbb{Z})^c$ *ist ein Isomorphismus.*

Wir geben im Anhang der Arbeit einen Beweis dieses Lemmas mit den hier benutzten Methoden.

Lemma 5.7. *Ist* $\mathfrak{a}$ *kein Quadrat in* C, *so läßt* $\mathfrak{a}$ *kein erzeugendes Reziprozitätsgesetz zu.*

Beweis. $\mathfrak{p}_1, \ldots, \mathfrak{p}_c$ sei wie oben Basis von C/C^2. O. B. d. A. sei $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_k, k \geqq 1$. Wir führen die Annahme „$\mathfrak{a}$ läßt ein erzeugendes Reziprozitätsgesetz zu" zum Widerspruch: Wähle nach dem letzten Lemma ein $d \in \Delta^+$, so daß d in $F_{\mathfrak{p}_1}$ kein Quadrat ist, wohl aber in $F_{\mathfrak{p}_2}, \ldots, F_{\mathfrak{p}_c}$. Dann gilt nach 5.2, daß $\gamma_{\mathfrak{p}_1}\langle 1, -d\rangle = -1$, $\gamma_{\mathfrak{p}_i}\langle 1, -d\rangle = 1$ für $i = 2, \ldots, c$ und $\gamma_{\mathfrak{p}}\langle 1, -d\rangle = 1$ an allen anderen endlichen Stellen, weil die Form dort $\mathfrak{a}$-modular (= unimodular) ist. Da d total-positiv ist, gilt auch $\gamma_{\mathfrak{p}}\langle 1, -d\rangle = 1$ an allen unendlichen Stellen, womit wir einen Widerspruch zu (R 2) haben.

Lemma 5.5 ergibt nun, daß die Differente D ein Quadrat in C ist, und dann den noch fehlenden Teil von Satz 5.3.

Durch eine Bedingung (R $\mathfrak{a}$) wird ein erzeugendes Reziprozitätsgesetz $\{\gamma_{\mathfrak{p}}\}$ nur an den diskreten Primstellen näher beschrieben. Fragestellung und Resultate dieses Paragraphen lassen sich verfeinern, indem man zu einem Ideal $\mathfrak{a}$ nach der Existenz erzeugender Reziprozitätsgesetze fragt, für die neben (R $\mathfrak{a}$) gilt:

(R∞) *An allen reellen Primstellen* $\mathfrak{p}$ *ist*

$$\gamma_{\mathfrak{p}}(\langle 1\rangle) = \alpha = e^{\frac{1}{4}\pi i}.$$

Wie eben ergibt sich, daß für die Differente ein erzeugendes Reziprozitätsgesetz, welches (R∞) *erfüllt, existiert.*

Anstelle der Klassengruppe C hat man jetzt die engere Klassengruppe C_0 (man dividiert nur durch Hauptideale mit totalpositiven Erzeugenden) zugrunde zu legen. Zu einem Charakter $\chi\colon C_0 \to \{\pm 1\}$ bezeichne $M(\chi)$ die Anzahl der reellen Primstellen $\mathfrak{p}$ mit $\chi(\mathfrak{p}) = -1$. Dabei ist unter $\chi(\mathfrak{p})$ der Wert von χ auf dem Bild von $\mathfrak{p}$ in C_0 zu verstehen, das durch ein Hauptideal (f) repräsentiert wird mit f negativ bei $\mathfrak{p}$ und positiv an den anderen reellen Stellen. Weil χ auf dem Ideal $(f) = (-f)$ zu einer totalnegativen Zahl f verschwindet, ist $M(\chi)$ eine gerade Zahl.

Satz 5.8. *Für ein Ideal* $\mathfrak{a}$ *existiert ein erzeugendes Reziprozitätsgesetz mit* (R∞) *genau dann, wenn für alle Charaktere* $\chi\colon C_0 \to \{\pm 1\}$ *der engeren Idealklassen-Gruppe* C_0 *gilt*

$$\chi(\mathfrak{a}) = i^{M(\chi)}.$$

Anwendung auf die Differente liefert einen Satz von Armitage ([1], Th. 3).

Für den Beweis von Satz 5.8 benötigen wir anstelle des Lemmas 5.6 den folgenden Spezialfall des Existenzsatzes der Klassenkörpertheorie, für den wir im Anhang der Arbeit ebenfalls einen Beweis angeben.

Lemma 5.9. *Zu jedem Charakter* $\chi\colon C_0 \to \{\pm 1\}$ *gibt es eine an allen endlichen Stellen unverzweigte Quadratklasse* (d) *von* F, *so daß für jede Primstelle* $\mathfrak{p}$ *gilt: Genau dann ist* $F_{\mathfrak{p}}(\sqrt{d}) \neq F_{\mathfrak{p}}$, *wenn* $\chi(\mathfrak{p})$ *den Wert* -1 *hat.*

Beweis von 5.8. Wir nehmen o.B.d.A. an, daß $\mathfrak{a}$ Produkt $\mathfrak{p}_1 \dots \mathfrak{p}_k$ von verschiedenen nichtdyadischen Primstellen ist. Zu dem vorgegebenen Charakter χ wählen wir eine Quadratklasse (d) wie in 5.9 angegeben. Existiert für $\mathfrak{a}$ ein erzeugendes Reziprozitätsgesetz $\{\gamma_\mathfrak{p}\}$, so gilt nach 5.2:

$$1 = \prod_{\mathfrak{p}} \gamma_\mathfrak{p}\langle 1, -d\rangle = i^{M(\chi)} \prod_{i=1}^{k} \gamma_{\mathfrak{p}_i}\langle 1, -d\rangle$$
$$= i^{M(\chi)} \prod_{i=1}^{k} \chi(\mathfrak{p}_i) = i^{M(\chi)}\, \chi(\mathfrak{a}),$$

q.e.d.

§ 6. Eindeutigkeitssätze

In diesem Abschnitt beweisen wir die Eindeutigkeit des Weilschen Reziprozitätsgesetz 4.1 im Sinne von Moore [11], Chap. II.

Dabei spielen die Elemente aus der 3. Potenz $B_0^3(F)$ des Ideals $B_0(F)$ der gerade-dimensionalen Formen über F keine Rolle, weil wir nur Charaktere mit Werten in T_8 betrachten. $B_0^3(F)$ besteht aus den Formen, die an allen diskreten Stellen hyperbolisch sind und an allen reellen Stellen durch 8 teilbare Signatur haben. Dieses Ideal ist für jedes $\mathfrak{a}$ in den Witt-Gruppen $B(\mathfrak{a})$, $W(\mathfrak{a})$ enthalten. Wir definieren

$$B'(F) = B(F)/B_0^3(F), \qquad B'(\mathfrak{a}) = B(\mathfrak{a})/B_0^3(F),$$

etc. Für eine diskrete Stelle $\mathfrak{p}$ ist $B'(F_\mathfrak{p}) = B(F_\mathfrak{p})$, für eine reelle Stelle $\mathfrak{p}$ ist

$$B'(F_\mathfrak{p}) = B(F_\mathfrak{p})/B_0^3(F_\mathfrak{p}) \cong \mathbb{Z}/8\mathbb{Z}.$$

Um die Bezeichnungen zu vereinfachen schreiben wir statt B', W' wieder B, W. Die ursprünglichen Witt-Gruppen werden überhaupt keine Rolle mehr spielen. Die neue Gruppe B ist übrigens eine Untergruppe des 2-Anteils der „graduierten Brauer-Gruppe".

Wir betrachten zunächst den lokalen Fall: Es sei F ein $\mathfrak{p}$-adischer oder reeller Körper und φ_F die Normform der nicht-trivialen Quaternionen-Algebra. $W(F) = B(F)$ ist eine endliche Gruppe; die duale Gruppe $B(F)^* := \mathrm{Hom}(B(F), T_8)$ ist ein $B(F)$-Modul vermöge

$$(b\,\chi)(b') = \chi(b \otimes b').$$

Satz 6.1. *$B(F)^*$ ist ein freier $B(F)$-Modul vom Rang* 1. *Jeder Charakter $\chi\colon B(F) \to T_8$ mit $\chi(\varphi_F) = -1$ ist ein Basiselement.*

Beweis. Da $B(F)$ und $B(F)^*$ endliche Gruppen gleicher Ordnung sind, genügt es zu beweisen, daß

$$B(F) \to B(F)^*, \qquad b \mapsto b\,\chi$$

injektiv ist, falls $\chi(\varphi_F) = -1$. Jede ungerade-dimensionale Form b ist Einheit von $B(F)$, also $b\,\chi \neq 1$. Ist b gerade-dimensionale Form der Diskriminante $d \neq 1$, so gibt es, wie man mittels [12], §63, leicht sieht, eine Form b' mit

$b \otimes b' = \varphi_F$ in $B(F)$, also $(b\chi)(b') = -1$, also $b\chi \neq 1$. Ist $b = \varphi_F$ in $B(F)$, so gilt $b\chi(1) = -1$, also $b\chi \neq 1$, q.e.d.

Es sei nun F ein algebraischer Zahlkörper und $\mathfrak{a}$ ein gebrochenes Ideal, welches ein erzeugendes Reziprozitätsgesetz zuläßt, $\mathfrak{a}$ ist also ein Quadrat in der Idealklassen-Gruppe. Es sei $\mathfrak{R}$ der Kokern der kanonischen Abbildung

$$W(F) \to \coprod_{\mathfrak{p}} W(F_{\mathfrak{p}})/W(\mathfrak{a}_{\mathfrak{p}}).$$

Hier durchläuft $\mathfrak{p}$ alle nicht-komplexen Primstellen ($W(\mathfrak{a}_{\mathfrak{p}}) = 0$ für $\mathfrak{p}$ reell). $\coprod W(F_{\mathfrak{p}})/W(\mathfrak{a}_{\mathfrak{p}})$ ist ebenso wie $W(F)$ ein $B(A)$-Modul und obige Abbildung ist $B(A)$-linear. Daher ist $\mathfrak{R}$ in kanonischer Weise $B(A)$-Modul und damit auch die Charaktergruppe $\mathfrak{R}^*$ von $\mathfrak{R}$. Offenbar entsprechen die Elemente von $\mathfrak{R}^*$ in eindeutiger Weise den Reziprozitätsgesetzen für $\mathfrak{a}$.

In Analogie zum letzten Satz gilt nun folgender Eindeutigkeitssatz:

Satz 6.2. *$\mathfrak{R}^*$ ist ein freier $B(A)$-Modul vom Rang 1. Jedes erzeugende Reziprozitätsgesetz für $\mathfrak{a}$ ist ein Basiselement.*

Beweis. $\gamma \in \mathfrak{R}^*$ sei erzeugendes Reziprozitätsgesetz. Für die lokalen Komponenten

$$\gamma_{\mathfrak{p}}\colon\ W(F_{\mathfrak{p}}) \to W(F_{\mathfrak{p}})/W(\mathfrak{a}_{\mathfrak{p}}) \to \coprod W(F_{\mathfrak{p}})/W(\mathfrak{a}_{\mathfrak{p}}) \to \mathfrak{R} \to T_8$$

gilt also $\gamma_{\mathfrak{p}}(\varphi_{\mathfrak{p}}) = -1$. Wir behaupten zunächst, daß $B(A) \to \mathfrak{R}^*$, $b \mapsto b\gamma$ eine Injektion ist. Ist $b \neq 0$ in $B(A)$, so gibt es nach Hasse-Minkowski eine Primstelle $\mathfrak{p}$ mit $b_{\mathfrak{p}} \neq 0$ in $B(A_{\mathfrak{p}})$, also $b_{\mathfrak{p}}\gamma_{\mathfrak{p}} \neq 1$ nach dem letzten Satz, womit die Behauptung bewiesen ist.

Der Hauptteil des Beweises besteht jetzt darin zu zeigen, daß $\mathfrak{R}$ und $B(A)$ endliche Gruppen gleicher Ordnung sind. Dieser Beweis wird in mehreren Hilfssätzen erbracht.

Es sei

m = Anzahl der reellen Primstellen von F,

n = Anzahl der komplexen Primstellen von F,

d = Anzahl der dyadischen Primstellen von F,

$2^c = [C : C^2]$.

Lemma 6.3. *Es sei*

$$P = \{a \in F^* \mid v_{\mathfrak{p}}(a) \equiv 0(2) \text{ für alle endlichen } \mathfrak{p}\}.$$

Dann enthält P/F^{*2} genau 2^{m+n+c} Elemente.

Beweis. Ist U die Einheiten-Gruppe von F, so hat man eine kanonische exakte Sequenz

$$1 \to U/U^2 \to P/F^{*2} \to {}_2C \to 1$$

mit

$${}_2C = \{a \in C \mid a^2 = 1\}.$$

Die Abbildung $P \to {}_2C$ ist dabei durch

$$a \mapsto \prod \mathfrak{p}^{\frac{1}{2} v_{\mathfrak{p}}(a)}$$

definiert. Nach dem Dirichletschen Einheitssatz ist $[U: U^2] = 2^{m+n}$, wegen der Endlichkeit der Klassenzahl ist $[{}_2C:1] = [C:C^2] = 2^c$, q.e.d.

Lemma 6.4. *Ist* $\mathfrak{a}$ *ein Quadrat, so enthält* $B(\mathfrak{a})$ *genau* $2^{2m+n+c+d}$ *Elemente.*

Beweis. Wegen $B(\mathfrak{a}) = B(\mathfrak{a}\,\mathfrak{b}^2) = B((a)\,\mathfrak{a})$ genügt es den Fall $\mathfrak{a} = A$ zu betrachten. Das Ergebnis ergibt sich unter Benutzung des Satzes von Hasse-Minkowski und seiner Umkehrung durch Abzählung der möglichen Invarianten: die Dimension von $b \in B(A)$ kann gerade oder ungerade sein, die Diskriminate ist ein Element von P/F^{*2}, das Hasse-Minkowski-Symbol kann nur an den reellen und dyadischen Stellen nicht verschwinden, wobei man jedoch das Reziprozitätsgesetz zu beachten hat. Auf diese Weise ergeben sich genau

$$2 \cdot 2^{m+n+c} \cdot 2^{m+d-1}$$

Elemente (vgl. [10]).

Jetzt kommt der unangenehmste Teil des Beweises:

Lemma 6.5. *Ist* $\mathfrak{a}$ *ein Quadrat, so enthält* $\mathfrak{R}$ *genau* $2^{2m+n+c+d}$ *Elemente.*

Beweis. O.B.d.A. sei wieder $\mathfrak{a} = A$. Es ist etwas bequemer, die wegen $W(\mathfrak{a}) \subset W_0(F)$ doppelt so große Ordnung des Kokernes von

$$W_0(F) \to \coprod_{\mathfrak{p}} W(F_{\mathfrak{p}})/W(A_{\mathfrak{p}})$$

zu berechnen. Wegen $W(A_{\mathfrak{p}}) \subset B(A_{\mathfrak{p}})$ hat man nach Abschnitt 2. eine kanonische surjektive Abbildung

$$\alpha: \coprod_{\mathfrak{p}} W(F_{\mathfrak{p}})/W(A_{\mathfrak{p}}) \to C/C^2.$$

Das Bild von $W_0(F)$ liegt im Kern von α. Also gilt

$$[\mathfrak{R}:1] = 2^{c-1} \text{ Ordnung } (\text{Kokern}(W_0(F) \to \text{Kern}(\alpha))).$$

Sei also $\{\bar{\eta}_{\mathfrak{p}}\}$ ein Element von Kern (α). (Der Querstrich bezeichnet die kanonische Abbildung $W(F_{\mathfrak{p}}) \to W(F_{\mathfrak{p}})/W(A_{\mathfrak{p}})$.) Dann gibt es ein $d \in F^*$ mit

$$v_{\mathfrak{p}}(d) \equiv \dim \hat{c}_{\mathfrak{p}}^2(\eta_{\mathfrak{p}}) \pmod 2$$

für alle $\mathfrak{p}$, wobei $\hat{c}_{\mathfrak{p}}^2$ die 2. Restklassenform (vgl. 1.7) bezeichnet. Die Familie $\{\bar{\zeta}_{\mathfrak{p}}\}$ mit $\zeta_{\mathfrak{p}} = \eta_{\mathfrak{p}} \oplus \langle 1, d\rangle$ repräsentiert dasselbe Element des Kokerns wie die Familie $\{\bar{\eta}_{\mathfrak{p}}\}$. An allen endlichen Stellen ist nach Wahl von d die 2. Restklassenform von $\zeta_{\mathfrak{p}}$ gerade-dimensional. Durch Addition einer geeigneten globalen Quaternionenform $\psi \in W_0(F)$ (die $\psi_{\mathfrak{p}}$ können an den dyadischen Stellen beliebig sein) ergibt sich eine Familie $\{\bar{\xi}_{\mathfrak{p}}\}$, $\xi_{\mathfrak{p}} = \zeta_{\mathfrak{p}} \oplus \psi_{\mathfrak{p}}$ mit $\bar{\xi}_{\mathfrak{p}} = 0$ für alle nicht-dyadischen Primstellen und $\hat{c}_{\mathfrak{p}}^2(\xi_{\mathfrak{p}}) = 0$ an allen dyadischen Stellen. Die Zahl dieser Familien ist

$$8^m\, 2^{m+2n+2d},$$

denn für $\mathfrak{p}$ reell enthält $W(F_\mathfrak{p})/W(A_\mathfrak{p})$ gerade 8 Elemente und für $\mathfrak{p}_i$ dyadisch und $[F_{\mathfrak{p}_i}:\mathbb{Q}_2]=N_i$ enthält $B(A_\mathfrak{p})/W(A_\mathfrak{p})$ genau 2^{N_i+2} Elemente. (Man beachte $\sum N_i=m+2n$.)

Eine solche Familie liegt nach 1.6 im Bild von $W_0(F)$, wenn sie im Bild von $B_0(A)$ liegt. Nach dem letzten Lemma ist die Ordnung von $B_0(A)$ gleich $2^{2m+n+c+d-1}$. Es bleibt jetzt noch die Anzahl der Elemente im Kern von

$$B_0(A)\to \coprod_\mathfrak{p} W(F_\mathfrak{p})/W(A_\mathfrak{p})$$

zu berechnen. Ein Element von $B_0(A)$ liegt im Kern, wenn es überall unverzweigte totalpositive Diskriminante d und an allen Stellen triviales Hasse-Minkowski-Symbol hat. Nach Lemma 5.4 gibt es 2^c solche Diskriminanten d. Die Elemente des Kernes werden durch die binären Formen $\langle 1, -d\rangle$ repräsentiert. Die Anzahl der Elemente in $\mathfrak{R}$ ergibt sich nun zu

$$2^{c-1}\,2^{3m}\,2^{m+2n+2d}(2^{2m+n+c+d-1})^{-1}\,2^c=2^{2m+n+d+c}.$$

Damit ist der Beweis des Lemmas und des Satzes 6.2 beendet.

Wir wollen jetzt einen Eindeutigkeitssatz für quadratische Reziprozitätsgesetze beweisen, ohne eine Bedingung (R α) zugrunde zu legen. Dazu definieren wir den „*Adelring*" $\mathbf{A}(B(F))=\mathbf{A}(W(F))$ als das eingeschränkte topologische Produkt

$$\prod_\mathfrak{p}(B(F_\mathfrak{p}), B(A_\mathfrak{p})),$$

wobei $B(F_\mathfrak{p})$ mit der diskreten Topologie versehen ist. In Analogie zur Definition der Differentiale sei $X(F)$ die Gruppe der stetigen Charaktere

$$\gamma\colon\ \mathbf{A}(W(F))\to T_8,$$

die auf dem Bild von $W(F)$ in $\mathbf{A}(W(F))$ verschwinden. Ist γ ein solcher Charakter, so bilden die lokalen Komponenten

$$\gamma_\mathfrak{p}\colon\ W(F_\mathfrak{p})\hookrightarrow\mathbf{A}(W(F))\xrightarrow{\gamma} T_8$$

ein Reziprozitätsgesetz. Die Bedingung (R 1) ergibt sich aus der Stetigkeit von γ. Die Bedingung (R 2) gilt, weil γ auf $W(F)$ verschwindet. Ist umgekehrt $\{\gamma_\mathfrak{p}\}$ ein Reziprozitätsgesetz und $\eta=\{\eta_\mathfrak{p}\}\in\mathbf{A}(W(F))$, so ist

$$\gamma(\eta)=\prod_\mathfrak{p}\gamma_\mathfrak{p}(\eta_\mathfrak{p})$$

wegen (R 1) wohldefiniert und wegen (R 2) ein Element von $X(F)$. Die Reziprozitätsgesetze entsprechen also umkehrbar eindeutig den Elementen von $X(F)$. Nun ist $\mathbf{A}(W(F))$ und damit auch $X(F)$ in offensichtlicher Weise ein $B(F)$-Modul, und es gilt:

Satz 6.6. *$X(F)$ ist ein freier $B(F)$-Modul vom Rang 1. Den erzeugenden Reziprozitätsgesetzen entsprechen die Basiselemente dieses Moduls.*

Beweis. Es sei $\{\gamma_\mathfrak{p}\}$ ein erzeugendes Reziprozitätsgesetz für A und γ: $\mathbf{A}(W(F))\to T_8$ der zugehörige Charakter. Die $B(F)$-lineare Abbildung

$B(F) \to X(F)$, $b \mapsto b\gamma$ ist nach demselben Argument wie früher injektiv. Wir wollen die Surjektivität zeigen. Sei also $\chi: \mathbf{A}(W(F)) \to T_8$ ein stetiger Charakter mit lokalen Komponenten $\chi_\mathfrak{p}: W(F_\mathfrak{p}) \to T_8$. Nach 6.1 gibt es eindeutig bestimmte Formen $b_\mathfrak{p} \in B(F_\mathfrak{p})$ mit

$$\chi_\mathfrak{p}(\psi) = \gamma_\mathfrak{p}(b_\mathfrak{p} \otimes \psi) \qquad (*)$$

für alle $\psi \in W(F_\mathfrak{p})$. Da $\chi_\mathfrak{p}(W(A_\mathfrak{p})) = \{1\}$ und $\gamma_\mathfrak{p}(W(A_\mathfrak{p})) = 1$ für fast alle $\mathfrak{p}$ ist, folgt $b_\mathfrak{p} \in B(A_\mathfrak{p})$ für fast alle $\mathfrak{p}$, also $\{b_\mathfrak{p}\} \in \mathbf{A}(B(F))$. Wir betrachten die Familie

$$\{\bar{b}_\mathfrak{p}\} \in \coprod_\mathfrak{p} W(F_\mathfrak{p})/W(A_\mathfrak{p}).$$

Aus $\prod \chi_\mathfrak{p}(\psi) = 1$ für alle $\psi \in B(A)$ und $(*)$ folgt nach dem letzten Satz, daß $\{\bar{b}_\mathfrak{p}\}$ unter allen Charakteren von $\mathfrak{R}$ verschwindet, d.h. $\{\bar{b}_\mathfrak{p}\}$ liegt im Bild von $B(F)$. Wir können also eine globale Form $b \in B(F)$ finden, so daß die zu $\chi + b\gamma$ gehörige Familie $\{\bar{b}_\mathfrak{p} \oplus \bar{b}\}$ gleich 0 ist. O.B.d.A. können wir also vornherein annehmen, daß $b_\mathfrak{p} \in W(A_\mathfrak{p})$ für alle $\mathfrak{p}$ ist. Dann ist χ ebenfalls ein Reziprozitätsgesetz für A, nach dem letzten Satz also von der Form $b\gamma$ für $b \in B(A)$. Damit haben wir gezeigt, daß $X(F)$ freier von γ erzeugter $B(F)$-Modul ist. Ein Element $\xi\gamma$ mit $\xi \in B(F)$ ist ein Basiselement von $X(F)$ genau dann wenn ξ eine Einheit von $B(F)$ ist, also ungerade Dimension hat. Das $\xi\gamma$ entsprechende Reziprozitätsgesetz erfüllt dann aber Bedingung (R 3), q.e.d.

Bemerkung 6.7. Sei $\gamma \in X(F)$ ein erzeugendes Reziprozitätsgesetz, das einer Bedingung (R a) genügt, und $\xi \in B(F)$ ein Element von ungerader Dimension. Es ist nicht schwer einzusehen, daß $\xi\gamma$ genau dann einer Bedingung (R a') genügt, wenn die Cliffordinvariante von ξ an allen nichtdyadischen Primstellen verschwindet.

Satz 6.6 ermöglicht uns, die Wittgruppe $W(F)$ eines algebraischen Zahlkörpers F im Sinn der Einleitung zu „berechnen". Sei ein erzeugendes Reziprozitätsgesetz $\{\gamma_\mathfrak{p}\}$ für ein Ideal $\mathfrak{c}$ von F fest vorgegeben. Seien $\mathfrak{a}$ und $\mathfrak{b}$ weitere Ideale mit $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$. Unser Reziprozitätsgesetz liefert einen Homomorphismus

$$\Phi: \bigoplus_\mathfrak{p} W(F_\mathfrak{p})/W(\mathfrak{a}_\mathfrak{p}) \to B(\mathfrak{b})^*,$$

der einem Element $\{\bar{\eta}_\mathfrak{p}\}$ den Charakter

$$\xi \mapsto \prod_\mathfrak{p} \gamma_\mathfrak{p}(\xi\eta_\mathfrak{p})$$

auf $B(\mathfrak{b})$ zuordnet, denn es ist $W(\mathfrak{a}_\mathfrak{p})B(\mathfrak{b}_\mathfrak{p}) \subset W(\mathfrak{c}_\mathfrak{p})$. Dann verschwindet Φ auf dem kanonischen Bild von $W(F)$. Wir führen die Untergruppe $W^+(\mathfrak{b})$ der $\xi \in W(\mathfrak{b})$ mit $\xi_\mathfrak{p} \sim 0$ an allen reellen $\mathfrak{p}$ ein. Analog zu Φ definiert unser Reziprozitätsgesetz einen Homomorphismus

$$\Psi: \bigoplus_\mathfrak{p} W(F_\mathfrak{p})/B(\mathfrak{a}_\mathfrak{p}) \to W^+(\mathfrak{b})^*.$$

Dabei ist an den reellen Primstellen $B(\mathfrak{a}_\mathfrak{p}) = W(F_\mathfrak{p})$ zu lesen, d.h. der Anteil der reellen Primstellen ist trivial. Nun macht man sich unter Benutzung von 5.2 und 6.1 an jeder Stelle $\mathfrak{p}$ leicht klar:

Lemma 6.8. *Die Gruppe $B(\mathfrak{a}_\mathfrak{p})$ besteht aus allen $\xi \in W(F_\mathfrak{p})$ mit $\gamma_\mathfrak{p}(\xi\,\eta)=1$ für alle $\eta \in W(\mathfrak{b}_\mathfrak{p})$. Ebenso ist $W(\mathfrak{a}_\mathfrak{p})$ die Gruppe der $\xi \in W(F_\mathfrak{p})$ mit $\gamma_\mathfrak{p}(\xi\,\eta)=1$ für alle $\eta \in B(\mathfrak{b}_\mathfrak{p})$.*

Damit erhalten wir aus Satz 6.6 unmittelbar folgendes Korollar.

Korollar 6.9. *Die Sequenzen*

$$0 \to W^+(\mathfrak{a}) \to W(F) \to \bigoplus_\mathfrak{p} W(F_\mathfrak{p})/W(\mathfrak{a}_\mathfrak{p}) \xrightarrow{\Phi} B(\mathfrak{b})^* \to 0$$

und

$$0 \to B(\mathfrak{a}) \to W(F) \to \bigoplus_\mathfrak{p} W(F_\mathfrak{p})/B(\mathfrak{a}_\mathfrak{p}) \xrightarrow{\Psi} W^+(\mathfrak{b})^* \to 0$$

sind exakt.

Die Ordnungen der endlichen Gruppen $B(\mathfrak{a})$ lassen sich leicht berechnen (vgl. Lemma 6.4). Die Ordnungen der $W^+(\mathfrak{a})$ ergeben sich z. B. aus einem Vergleich der zweiten Sequenz aus Korollar 6.9 mit den in Satz 2.2 betrachteten Sequenzen, unter Berücksichtigung des Existenzsatzes 5.3:

$$[W^+(\mathfrak{b}):1]=[C:C^2],$$

falls $\mathfrak{b}$ ein Quadrat in C ist, und

$$[W^+(\mathfrak{b}):1]=\tfrac{1}{2}[C:C^2]$$

sonst. Die erste dieser Gleichungen hatten wir natürlich schon im Beweis von Lemma 6.5 benutzt.

In Korollar 6.9 können die Wittgruppen auch im ursprünglichen Sinne gelesen werden, also nicht mod $(B_0)^3$ reduziert. Unter $B(\mathfrak{b})^*$ ist dann die Gruppe $\mathrm{Hom}(B(\mathfrak{b}), T_8)$ zu verstehen.

§ 7. Anhang. Zum Existenzsatz der globalen Klassenkörpertheorie für quadratische Erweiterungen

Wir betrachten zu der Gruppe Δ^+ der unverzweigten totalpositiven Quadratklassen von F und der Gruppe $\mathrm{Div}(F)$ der Divisoren (= multiplikative Gruppe der gebrochenen Ideale) von F die biadditive Abbildung

$$\rho\colon\ \Delta^+ \times \mathrm{Div}(F) \to \mathbb{Z}/2\mathbb{Z},$$

die einer Quadratklasse d und einem Primideal $\mathfrak{p}$ den Wert $(F_\mathfrak{p}(\sqrt{d}):F_\mathfrak{p})-1$ mod 2 zuordnet. Unter dieser Paarung liefert ein Element $(d)\neq(1)$ von Δ^+ eine von 0 verschiedene Abbildung von $\mathrm{Div}(F)$ nach $\mathbb{Z}/2\mathbb{Z}$. Weiter besagt das Weilsche Reziprozitätsgesetz, angewandt auf eine Form $\langle 1, -f\rangle \otimes \langle 1, -d\rangle \otimes \langle\omega\rangle$ mit $\omega \in \Omega(F)$, $\omega \neq 0$, $f \in F^*$, $(d) \in \Delta^+$ (also Hilberts Reziprozitätsgesetz), daß $\rho(d,(f))=0$ ist. ρ faktorisiert somit über eine Paarung

$$\Delta^+ \times C/C^2 \to \mathbb{Z}/2\mathbb{Z}, \tag{1}$$

die im Argument Δ^+ nicht ausgeartet ist. Lemma 5.6 bedeutet gerade, daß diese Paarung eine perfekte Dualität ist. (Dazu genügt es, $[\Delta^+:1] \geqq [C:C^2]$ zu zeigen.) Dies ist ein Spezialfall des Existenzsatzes der Klassenkörpertheorie (vgl. z. B. [3], Chap. VIII).

Analog erhält man zu der Gruppe Δ der an allen diskreten Primstellen unverzweigten Quadratklassen eine im 1. Argument nicht ausgeartete Paarung

$$\Delta \times C_0/C_0^2 \to \mathbb{Z}/2\mathbb{Z}. \tag{2}$$

Lemma 5.9 bedeutet, daß diese Paarung eine perfekte Dualität ist, ein anderer Spezialfall des Existenzsatzes der Klassenkörpertheorie.

Wir beweisen jetzt die Ungleichung $[\Delta:1] \geqq [C_0:C_0^2]$ unter Benutzung des Satzes von Hasse-Minkowski und seiner Umkehrung mit den Methoden aus § 6. Dann wissen wir, daß (2) eine perfekte Dualität ist. Die Gruppe $\bar{\mathfrak{H}}$ der Bilder aller Hauptdivisoren in C_0 wird von den „reellen Primdivisoren" erzeugt. $\bar{\mathfrak{H}}$ hat also unter (2) in Δ den Annullator Δ^+. Andererseits ist $C_0/\bar{\mathfrak{H}} \cong C$. Somit wissen wir nach Beweis von $[\Delta:1] \geqq [C_0:C_0^2]$, daß auch (1) eine perfekte Dualität ist.

Wie in § 6 bezeichnen wir mit m, n, d die Anzahl der reellen bzw. komplexen bzw. dyadischen Primstellen von F und schreiben $[C:C^2] = 2^c$. Wie in § 6 betrachten wir nur mod B_0^3 reduzierte Witt-Gruppen. Sei $\mathfrak{a}$ ein (evtl. gebrochenes) Ideal von A, für das es ein erzeugendes Reziprozitätsgesetz $\{\gamma_\mathfrak{p}\}$ gibt, etwa die Differente von $F/\mathbb{Q}$ (s. 5.5). $\mathfrak{L}(\mathfrak{a})$ bezeichne den Kokern der kanonischen Abbildung

$$B(F)/B_0(F)^2 \to \coprod_\mathfrak{p} B(F_\mathfrak{p})/(W(\mathfrak{a}_\mathfrak{p}) + B_0(F_\mathfrak{p})^2),$$

wobei $\mathfrak{p}$ jetzt *nur die diskreten* Primstellen durchläuft. $B^+(A)$ bezeichne die Gruppe aller $\xi \in B(A)$ von gerader Dimension mit $\xi_\mathfrak{p} \sim 0$ an allen reellen Stellen. (Ist $m > 0$, so braucht man „gerade Dimensionen" natürlich nicht extra zu fordern.) Unser Reziprozitätsgesetz gibt eine wohldefinierte Paarung

$$B^+(A) \times \mathfrak{L}(\mathfrak{a}) \to T, \tag{3}$$

die einem $\xi \in B^+(A)$ und einem durch eine Familie $\{\eta_\mathfrak{p}\}$ mit $\eta_\mathfrak{p} \in B(F_\mathfrak{p})$ repräsentierten Element von $\mathfrak{L}(\mathfrak{a})$ die Einheitswurzel $\prod \gamma_\mathfrak{p}(\xi \eta_\mathfrak{p})$ zuordnet. Ähnlich wie zu Anfang des Beweises von 6.2 sieht man, daß diese Paarung im Argument $B^+(A)$ nicht ausgeartet ist. Wir erhalten somit

Lemma 7.1. $[\mathfrak{L}(\mathfrak{a}):0] \geqq [B^+(A):0]$.

Wir werden jetzt $[B^+(A):0]$ berechnen und dann $[\mathfrak{L}(\mathfrak{a}):0]$ nach oben abschätzen.

Lemma 7.2. *Die Ordnung der Gruppe* $B^+(A)$ *ist gleich* $2^{n+d-1}[C_0:C_0^2]$.

Beweis. Wie im Beweis von 6.4 sieht man, daß die Ordnung von $B^+(A)$ gleich

$$2^{d-1}[P^+:F^{*2}]$$

ist, wobei P^+ die Gruppe der totalpositiven $a \in F^*$ mit $v_\mathfrak{p}(a) \equiv 0 \bmod 2$ für alle endlichen $\mathfrak{p}$ bezeichnet. Sei U^+ die Gruppe der totalpositiven Einheiten von A und $\bar{\mathfrak{H}} = \mathfrak{H}/\mathfrak{H}^+$ das Bild der Gruppe $\mathfrak{H}$ der Hauptdivisoren in der engeren Klassengruppe $C_0 = \mathrm{Div}(F)/\mathfrak{H}^+$. Analog zum Beweis von 6.3 erhalten wir

eine exakte Sequenz

$$1 \to U^+/U^2 \to P^+/F^{*2} \to {}_2(C_0)/\bar{\mathfrak{H}} \to 0,$$

indem wir einem $a \in P^+$ die Klasse von $\prod \mathfrak{p}^{\frac{1}{2}v_\mathfrak{p}(a)}$ zuordnen. Also ist

$$[P^+ : F^{*2}] = [U^+ : U^2][C_0 : C_0^2][\mathfrak{H} : \mathfrak{H}^+]^{-1}.$$

Andererseits haben wir trivialerweise eine exakte Sequenz

$$1 \to U/U^+ \to F^*/F^+ \to \mathfrak{H}/\mathfrak{H}^+ \to 1,$$

wobei F^+ die Gruppe der totalpositiven Zahlen aus F^* bezeichnet. Daher ist

$$[\mathfrak{H} : \mathfrak{H}^+][U : U^+] = 2^m.$$

Insgesamt erhalten wir

$$[P^+ : F^{*2}] = 2^{-m}[U : U^2] \cdot [C_0 : C_0^2],$$

also mit dem Dirichletschen Einheitensatz die Behauptung, q.e.d.

Wir wollen jetzt die Ordnung von $\mathfrak{Q}(\mathfrak{a})$ möglichst weitgehend berechnen. Sie ist doppelt so groß wie die Ordnung des Kokerns der kanonischen Abbildung

$$\lambda\colon\ B^0(F)/B_0(F)^2 \to \coprod_\mathfrak{p} B(F_\mathfrak{p})/(W(\mathfrak{a}_\mathfrak{p}) + B_0(F_\mathfrak{p})^2).$$

Offensichtlich liegt das Bild von λ im Kern der natürlichen Surjektion

$$\beta\colon\ B(F_\mathfrak{p})/(W(\mathfrak{a}_\mathfrak{p}) + B_0(F_\mathfrak{p})^2) \to \coprod_\mathfrak{p} B(F_\mathfrak{p})/(B(\mathfrak{a}_\mathfrak{p}) + B_0(F_\mathfrak{p})^2) \to C/C^2,$$

wobei der zweite Pfeil von der in §2 betrachteten Abbildung stammt. Wir bezeichnen den Kokern der aus λ durch Einschränkung des Bildbereiches entstehenden Abbildung von $B_0(F)/B_0(F)^2$ nach $\mathrm{Ker}(\beta)$ mit $\mathfrak{Q}_1(\mathfrak{a})$. Es ist

$$[\mathfrak{Q}(\mathfrak{a}) : 0] = 2^{c-1}[\mathfrak{Q}_1(\mathfrak{a}) : 0]. \tag{4}$$

Man sieht nun, mit weniger Mühe als im Beweis von 6.5, daß alle Elemente von $\mathfrak{Q}_1(\mathfrak{a})$ schon durch Familien aus

$$\mathfrak{Q}_2(\mathfrak{a}) := \coprod_{\mathfrak{p}\,|\,2} B(\mathfrak{a}_\mathfrak{p})/(W(\mathfrak{a}_\mathfrak{p}) + B_0(F_\mathfrak{p})^2)$$

repräsentiert werden. Damit erhält man eine natürliche exakte Sequenz

$$\begin{aligned} 0 \to W(\mathfrak{a})/(W(\mathfrak{a}) \cap B_0(F)^2) &\to (B(\mathfrak{a}) \cap B_0(F))/(B(\mathfrak{a}) \cap B_0(F))^2 \\ &\to \mathfrak{Q}_2(\mathfrak{a}) \to \mathfrak{Q}_1(\mathfrak{a}) \to 0. \end{aligned} \tag{5}$$

Man verifiziert (vgl. Beweis von 6.5)

$$[\mathfrak{Q}_2(\mathfrak{a}) : 0] = 2^{m+2n+d}. \tag{6}$$

Die Elemente des ersten und zweiten Terms aus (5) werden durch ihre Diskriminante klassifiziert. Diese muß beim ersten Term in Δ liegen, kann jedoch beim 2. Term jedes Element der in 6.3 betrachteten Menge P/F^{*2} sein.

Also ist

$$[W(\mathfrak{a}):(W(\mathfrak{a})\cap B_0(F)^2)]\leqq[\Delta:1] \tag{7}$$

und nach 6.3

$$[(B(\mathfrak{a})\cap B_0(F)):(B(\mathfrak{a})\cap B_0(F)^2)]=2^{m+n+c}. \tag{8}$$

Aus (4), (5), (6), (7), (8) erhält man

Lemma 7.3. $[\mathfrak{L}(\mathfrak{a}):0]\leqq 2^{n+d-1}[\Delta:1]$.

Diese drei Hilfssätze ergeben zusammen die Behauptung $[\Delta:1]\geqq[C_0:C_0^2]$. Es sei noch angemerkt, daß die jetzt bewiesene Gleichheit $[\Delta:1]=[C_0:C_0^2]$ auch bedeutet, daß die Paarung (3) eine perfekte Dualität ist. Das ist eine Abschwächung von Satz 6.6.

Literatur

1. Armitage, J.V.: On a theorem of Hecke in number fields and function fields. Inventiones math. **2**, 238 – 246 (1967).
2. Artin, E.: Algebraic numbers and algebraic functions. Lecture Notes Princeton 1951. New York-London-Paris: Gordon & Breach 1967.
3. – Tate, J.: Class field theory. Princeton Lecture notes 1951.
4. Fröhlich, A.: On the K-theory of unimodular forms over rings of algebraic integers. Preprint 1970.
5. Hecke, E.: Vorlesungen über die Theorie der algebraischen Zahlen. Leipzig: Akad. Verlag 1923 u. 1954.
6. Geyer, W.D., Harder, G., Knebusch, M., Scharlau, W.: Ein Residuensatz für symmetrische Bilinearformen. Inventiones math. **11**, 319 – 328 (1970).
7. Knebusch, M.: Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen. S.-ber. Heidelberger Akad. Wiss. 1969 70. 3. Abh., auch als Einzelheft bei Springer, Berlin-Göttingen-Heidelberg 1970.
8. Milnor, J.: On isometries of inner product spaces. Inventiones math. **8**, 83 – 97 (1969).
9. – Algebraic K-theory and quadratic forms. Inventiones math. **9**, 318 – 344 (1970).
10. – Symmetric inner product spaces over a Dedekind domain. Preprint 1970.
11. Moore, C.C.: Group extensions of p-adic and adelic linear groups. Publ. Math. I.H.E.S. **35**, 157 – 222 (1968).
12. O'Meara, O.T.: Introduction to quadratic forms. Berlin-Göttingen-Heidelberg: Springer 1963.
13. Scharlau, W.: Quadratic forms. Queen's papers in pure and applied mathematics No. 22, 1969.
14. – Quadratic reciprocity laws. To appear in J. Number Theory.
15. Serre, J.P.: Corps locaux. Paris: Hermann 1962.
16. Springer, T.A.: Quadratic forms over a field with a discrete valuation. Indagationes Math. **17**, 352 – 362 (1955).
17. Weil, A.: Sur certains groupes d'operateurs unitaires. Acta math. **111**, 143 – 211 (1964).
18. – Basic number theory. Berlin-Heidelberg-New York: Springer 1967.
19. Witt, E.: Theorie der quadratischen Formen in beliebigen Körpern. J. Reine Angew. Math. **176**, 31 – 44 (1937).

Dr. M. Knebusch
Mathematisches Institut der Universität
BRD-6600 Saarbrücken
Deutschland

Dr. W. Scharlau
Mathematisches Institut der Universität
BRD-4400 Münster, Roxeler Straße 64
Deutschland

(Eingegangen am 26. Mai 1971)