数理解析研究所講究録
第 603 巻 1987 年 152-168

Binary Quadratic Forms, Dihedral Fields and Decomposition Laws

Franz Halter-Koch

The connections between rational decomposition laws for dihedral fields and the representations of primes by binary quadratic forms have been considered by many authors. Whereas the subject has been treated in a systematically and satisfactory way from the field theoretic point of view (see e. g. [24], [9], [18], [6], [7]) no equally satisfactory treatment of the subject from the point of view of quadratic forms seems to be available in the literature.

Recently I have given a systematic theory of spinor genus characters of binary quadratic forms in the sense of [5] using dihedral fields [13]; the results obtained there cover all (or at least almost all) known special representation theorems for binary quadratic forms and rational biquadratic reciprocity laws published recently (e. g. [2], [3], [5], [16], [17], [19], [20], [22], [28], [9], [6]) as well as the classical results of Rédei [24] and Scholz [26].

This paper parallels [13] in a very strict sense. Though the Main Theorems are stated in a slightly more general form than there, they are proved in the same manner, and thus a I shall not repeat here the lengthy calculations which are necessary for the proofs of the Theorems in § 2; I also refer to [13] for examples. Instead of this I shall derive the connections of my spinor genus symbol with the symbols of Rédei [24] and Furuta [7] in § 3.

§ 1 Notations and Representation Theorems.

The notations introduced in this chapter will be used in the whole paper without further reference.

Let $\Delta \in \mathbb{Z}$ be a discriminant of integral non-degenerated binary quadratic forms, so $\Delta \equiv 0$ or $1 \bmod 4$ and $\Delta = \Delta_o f^2$ with a fundamental discriminant $\Delta_o \neq 0,1$. Let $C(\Delta)$ be the composition class group of integral primitive (in case $\Delta < 0$ positive definite) binary quadratic forms of discriminant Δ, and let $k_\Delta = \mathbb{Q}(\sqrt{\Delta})$ be the associated quadratic number field, whose discriminant is Δ_o. I use the symbol $[a,b,c]$ to denote the class of the form $aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]$ in $C(\Delta)$; thus $[a,b,c] \in C(\Delta)$ iff $a,b,c \in \mathbb{Z}$, $(a,b,c) = 1$, $\Delta = b^2 - 4ac$ and $a > 0$ if $\Delta < 0$.

There is a canonical isomorphism

$$\lambda: C(\Delta) \xrightarrow{\sim} \mathcal{I}(\Delta)$$

of $C(\Delta)$ with the ring class group modulo f in the narrow sense of k_Δ: for $A = [a,b,c]$ with $a > 0$, $\lambda(A)$ is the class containing the ideal generated by a and $\frac{1}{2}(b-\sqrt{\Delta})$ (see [1; Kap. II, § 7] in connection with [14; § 10]).

If $A \in C(\Delta)$ represents primitively some $\kappa \in \mathbb{Z}$, I write $A \to \kappa$; then, for $\kappa > 0$, $A \to \kappa$ iff $\lambda(A)$ contains an integral ideal $\mathfrak{a}$ with $N(\mathfrak{a}) = \kappa$.

Let

$$C(\Delta)' = \mathrm{Hom}(C(\Delta), \{\pm 1\})$$

be the group of genus characters of $C(\Delta)$. To $1 \neq \phi \in C(\Delta)'$ there belongs a unique field

$$K_\phi = \mathbb{Q}(\sqrt{e_\phi}, \sqrt{\tilde{e}_\phi}) \supsetneqq k_\Delta$$

with fundamental discriminants e_ϕ, $\tilde{e}_\phi$ such that $\phi \circ \lambda^{-1}$ is the ideal character attatched to K_ϕ/k_Δ. I set

$$e_\phi \tilde{e}_\phi = \Delta_o \cdot f_\phi^2$$

with $f_\phi \in \mathbb{N}$, which is the finite part of the conductor of K_ϕ/k_Δ; obviously, $f_\phi | f$ and ϕ factors in the form $\phi: C(\Delta) \xrightarrow{\nu} C(\Delta_o f_\phi^2) \to \{\pm 1\}$ where ν is the canonical epimorphism. If $Q \in C(\Delta)$ and p is a prime with $p \nmid f_\phi$ and $Q \to p$, then

$$\phi(Q) = \left(\frac{K_\phi/k_\Delta}{\mathfrak{p}}\right)$$

for prime ideals $\mathfrak{p}$ of k_Δ dividing p , and thus, if $p \nmid \Delta$, p splits completely in K_ϕ iff $\phi(Q) = 1$. More generally, if $\mathfrak{a} \in \lambda(Q)$ is an integral ideal prime to 2Δ and $a = N(\mathfrak{a})$, then

$$\phi(Q) = \left(\frac{K_\phi/k_\Delta}{\mathfrak{a}}\right) = \left(\frac{e_\phi}{a}\right) = \left(\frac{\tilde{e}_\phi}{a}\right)$$

(with ordinary Jacobi symbols).

The significance of genus characters for the representation problem becomes clear from the following theorem, which in principle is well known, but for which I will include a proof for lack of a suitable reference.

Theorem 1 *(Representation Theorem by Means of Genus Characters). Suppose* $\kappa \in \mathbb{Z}$, $(\kappa, 2\Delta) = 1$ *and that there is a class* $Q \in C(\Delta)$ *with* $Q \to \kappa$ *. Then, for* $A \in C(\Delta)$ *, the following assertions are equivalent:*

i) *There is a class* $A' \in A \cdot C(\Delta)^2$ *(in the genus of* A *) such that* $A' \to \kappa$ *.*

ii) $\phi(A) = \left(\frac{e_\phi}{\kappa}\right) = \left(\frac{\tilde{e}_\phi}{\kappa}\right)$ *for all* $\phi \in C(\Delta)'$ *; here* $\left(\frac{e_\phi}{\kappa}\right)$ *is the usual Jacobi symbol if* $\kappa > 0$ *, and* $\left(\frac{e_\phi}{\kappa}\right) = \mathrm{sgn}(e_\phi) \cdot \left(\frac{e_\phi}{|\kappa|}\right)$ *if* $\kappa < 0$ *.*

Proof. Suppose first that $A' = AB^2$ with $B \in C(\Delta)$ and $A' \to \kappa$. If $\kappa > 0$ there is an integral ideal $\mathfrak{a} \in \lambda(A')$ with $N(\mathfrak{a}) = \kappa$, and then $\phi(A') = \phi(A) = \left(\frac{K_\phi/k_\Delta}{\mathfrak{a}}\right) = \left(\frac{e_\phi}{\kappa}\right) = \left(\frac{\tilde{e}_\phi}{\kappa}\right)$. Now assume $\kappa < 0$; then $\Delta > 0$, and there is a unique class

$J \in C(\Delta)$ such that $J \to -1$; for this I have $\phi(J) = \mathrm{sgn}(e_\phi) = \mathrm{sgn}(\tilde{e}_\phi)$, and from $JA' \to |\kappa|$ I derive as before $\phi(JA') = (\frac{e_\phi}{|\kappa|}) = (\frac{\tilde{e}_\phi}{|\kappa|})$ and thus $\phi(A) = \phi(J)\cdot\phi(JA') = (\frac{e_\phi}{\kappa}) = (\frac{\tilde{e}_\phi}{\kappa})$.

Let now ii) be satisfied and suppose $Q \to \kappa$ for some $Q \in C(\Delta)$; if $Q \notin A\cdot C(\Delta)^2$ then $\phi(Q) \neq \phi(A)$ for some $\phi \in C(\Delta)'$, but by the part just proved I have $\phi(Q) = (\frac{e_\phi}{\kappa}) = (\frac{\tilde{e}_\phi}{\kappa})$, a contradiction, q. e. d.

Now I am going to introduce so-called spinor genus characters which will enable me to go one step behind Theorem 1. To do this, let $\mathfrak{X}(\Delta)$ be the group of all $\phi \in C(\Delta)'$ which are of the form $\phi = \chi^2$ for some character $\chi: C(\Delta) \to \mathbb{C}^\times$; $\mathfrak{X}(\Delta)$ is a subgroup of $C(\Delta)'$ whose rank is the number of invariants of $C(\Delta)$ divisible by 4. As $\phi\circ\lambda^{-1}$ is the ideal character belonging to K_ϕ/k_Δ I obtain the following field-theoretical characterization of genus characters ϕ in $\mathfrak{X}(\Delta)$:

<u>Lemma.</u> *A genus character* $1 \neq \phi \in C(\Delta)'$ *belongs to* $\mathfrak{X}(\Delta)$ *iff* K_ϕ *can be imbedded in a dihedral field* L_ϕ *of degree* 8 *over* $\mathbb{Q}$, *cyclic over* k_Δ , *such that the conductor of* L_ϕ/k_Δ *devides* $f\cdot\infty$.

For $1 \neq \phi \in \mathfrak{X}(\Delta)$ the dihedral field L_ϕ is not unique; but for L_ϕ as in the Lemma the finite part of the conductor of L_ϕ/k_Δ is generated by a unique positive rational integer f_ϕ^* [10; Satz 7]. I choose L_ϕ such that f_ϕ^* is minimal and fix it in the sequel. Let $\chi_\phi^*: \mathfrak{I}(\Delta) \to \mathbb{C}^\times$ be the ideal character attatched to L_ϕ/k_Δ ; then $\chi_\phi = \chi_\phi^*\circ\lambda$ is a character of $C(\Delta)$ which factors in the form $\chi_\phi: C(\Delta) \overset{\nu}{\to} C(\Delta_o f_\phi^{*2}) \to \mathbb{C}^\times$ and satisfies $\chi_\phi^2 = \phi$. The integer f_ϕ^* can also be characterized to be the least positive integer f_1 for which there is a character $\chi: C(\Delta) \to \mathbb{C}^\times$ which factors in the form $\chi: C(\Delta) \overset{\nu}{\to} C(\Delta_o f_1^2) \to \mathbb{C}^\times$ and satisfies $\chi^2 = \phi$.

If $1 \neq \phi \in \mathfrak{X}(\Delta)$, $Q \in C(\Delta)$, and if $\mathfrak{a} \in \lambda(Q)$ is an integral ideal prime to f_ϕ^* then

$$\chi_\phi(Q) = \left(\frac{L_\phi/k_\Delta}{\mathfrak{a}}\right) .$$

To become independent of the choice of L_ϕ let $\mathbb{P}(\Delta)$ be the set of all rational primes $p \nmid 2\Delta$ which are represented by a class in the principal genus of $C(\Delta)$, i. e. for which there is a class $Q \in C(\Delta)$ such that $Q^2 \to p$. Obviously $\mathbb{P}(\Delta)$ consists of all primes p which split completely in the genus field of the ring class field modulo f of k_Δ in the narrow sense [11] (which is the compositum of all fields K_ϕ for $1 \neq \phi \in C(\Delta)'$). Let $\mathbb{R}(\Delta)$ be the set of all square free positive rational integers composed only of primes $p \in \mathbb{P}(\Delta)$.

For $p \in \mathbb{P}(\Delta)$, $\phi \in \mathfrak{X}(\Delta)$ define

$$\sigma_\phi(p) = \begin{cases} 1 , \text{ if } \phi = 1 \text{ or } p \text{ splits completely in } L_\phi , \\ -1 \quad \text{otherwise,} \end{cases}$$

and extend σ_ϕ to $\mathbb{R}(\Delta)$ by multiplicativity, i. e. for $a = p_1 \cdot \ldots \cdot p_n \in \mathbb{R}(\Delta)$ set

$$\sigma_\phi(a) = \sigma_\phi(p_1) \cdot \ldots \cdot \sigma_\phi(p_n) .$$

Now suppose $a \in \mathbb{R}(\Delta)$ and $1 \neq \phi \in \mathfrak{X}(\Delta)$; then there is an integral ideal $\mathfrak{A}$ in K_ϕ with $N(\mathfrak{A}) = a$, and by definition, for any such $\mathfrak{A}$,

$$\sigma_\phi(a) = \left(\frac{L_\phi/K_\phi}{\mathfrak{A}}\right) ;$$

if $\mathfrak{a}$ is any integral ideal of k_Δ with $N(\mathfrak{a}) = a$, then it is of the form $\mathfrak{a} = N_{K_\phi/k_\Delta}(\mathfrak{A})$ for an integral ideal $\mathfrak{A}$ of K_ϕ , and thus also

$$\sigma_\phi(a) = \left(\frac{L_\phi/k_\Delta}{\mathfrak{a}}\right) .$$

Furthermore, as $a \in \mathbb{R}(\Delta)$ there is a class $Q \in C(\Delta)$ with $Q^2 \to a$ (there is such one for each prime factor of a) and so there is an integral ideal $\mathfrak{a} \in \lambda(Q^2)$ with $N(\mathfrak{a}) = a$, whence $\left(\frac{L_\phi/k_\Delta}{\mathfrak{a}}\right) = \chi_\phi(Q^2) = \chi_\phi^2(Q) = \phi(Q)$, so

$\sigma_\phi(a) = \phi(Q)$,

which proves the independence of $\sigma_\phi(a)$ from the choice of L_ϕ .

Characters of degree 4 of $C(\Delta)$ are called *spinor genus characters* in accordance with [5], and because of the formula $\sigma_\phi(a) = \chi_\phi(Q^2)$ proved above I call $\sigma_\phi(a)$ the *spinor genus symbol*. Now I can prove:

<u>Theorem 2</u> (*Representation Theorem by Means of Spinor Genus Symbols*). *Let* $A = A_o^2 \in C(\Delta)^2$ *be a class in the principal genus of* $C(\Delta)$ *and* $a \in \mathbb{R}(\Delta)$. *Then the following assertions are equivalent:*

<u>i)</u> *There is a class* $A' \in A\cdot C(\Delta)^4$ ("*in the spinor genus of* A") *such that* $A' \to a$.

<u>ii)</u> $\sigma_\phi(a) = \phi(A_o)$ *for all* $\phi \in \mathfrak{X}(\Delta)$.

<u>Proof.</u> Suppose first $A' = AB^4 \to a$ with some $B \in C(\Delta)$; then $A' = (A_oB^2)^2$, and as already shown above, $\sigma_\phi(a) = \phi(A_oB^2) = \phi(A_o)$ for all $\phi \in \mathfrak{X}(\Delta)$.

Now suppose $A' \to a$ with $A' = A_o'^2 \in C(\Delta)^2$, $A' \notin A\cdot C(\Delta)^4$; then $A'A^{-1} = B^2$ for some $B \in C(\Delta)\setminus C(\Delta)^2$ such that 4 divides the order of B in $C(\Delta)$. So there is a character $\chi: C(\Delta) \to \mathbb{C}^\times$ of degree 4 with $\chi(B) = \sqrt{-1}$; if I set $\chi^2 = \phi$, then $\phi \in \mathfrak{X}(\Delta)$ and, by the above, $\sigma_\phi(a) = \phi(A_o')$. Therefore $\phi(A_o) = \phi(A_o')$ and $1 = \phi(A_o'A_o^{-1}) = \chi^2(A_o'A_o^{-1}) = \chi(A'A^{-1}) = \chi(B^2) = -1$, a contradiction, q. e. d.

<u>Corollary 1.</u> *Let* $A = A_o^2 \in C(\Delta)^2$ *be a class in the principal genus of* $C(\Delta)$, $\kappa \in \mathbb{N}$, $(\kappa, 2\Delta) = 1$ *and* $a \in \mathbb{R}(\Delta)$ *such that* $A \to \kappa^2 a$. *Then*

$$\sigma_\phi(a) = \left(\frac{e_\phi}{\kappa}\right)\cdot\phi(A_o) = \left(\frac{\tilde{e}_\phi}{\kappa}\right)\cdot\phi(A_o)$$

for all $\phi \in \mathfrak{X}(\Delta)$.

Proof. Choose $Q = Q_o^2 \in C(\Delta)^2$ with $Q \to a$ such that $A_o Q_o^{-1} \to \kappa$; then, for all $\phi \in \mathfrak{X}(\Delta)$, $\phi(A_o Q_o^{-1}) = (\frac{e_\phi}{\kappa}) = (\frac{\tilde{e}_\phi}{\kappa})$, and as $\sigma_\phi(a) = \phi(Q_o) = \phi(A_o Q_o^{-1}) \cdot \phi(A_o)$ the assertion follows, q. e. d.

Corollary 2. *Let* $I \in C(\Delta)$ *be the principal class,* $a \in \mathbb{R}(\Delta)$ *and* $b \in \mathbb{N}$ *with* $(b, 2\Delta) = 1$ *and* $I \to b^2 a$. *Then*

$$\sigma_\phi(a) = (\frac{e_\phi}{b}) = (\frac{\tilde{e}_\phi}{b})$$

for all $\phi \in \mathfrak{X}(\Delta)$.

Proof. Obvious from Corollary 1.

As the principal form $I \in C(\Delta)$ is well known, Corollary 2 gives a first method to calculate the spinor genus symbol, similarly to the calculations of prime decomposition symbols in [7], [6] and [9].

In order to make Theorem 2 and its Corollary 1 applicable for concrete representation problems for binary quadratic forms one has to solve the following two problems:

A) Decide whether or not a given genus character $\phi \in C(\Delta)'$ belongs to $\mathfrak{X}(\Delta)$.

B) Calculate $\sigma_\phi(a)$ as explicitely as possible.

It is possible to define higher spinor genus characters of order 2^t for $t \geq 3$ and to use them to prove a Representation Theorem analoguos to Theorem 2; but then the problems corresponding to A) and B) above have no known explicit solutions.

§ 2 Criteria for $\phi \in \mathfrak{X}(\Delta)$ and computation of $\sigma_\phi(a)$.

In this section I state three Theorems which solve Problems A and B stated at the end of § 1. For proofs I refer to [13];

though the Theorems stated there concern only $\sigma_\phi(p)$ for $p \in \mathbb{P}(\Delta)$, they are valid for $\sigma_\phi(a)$ for arbitrary $a \in \mathbb{R}(\Delta)$ as one may easy see by multiplicativity. I shall use Jacobi's symbol $(\frac{a}{b})$ and Hilbert's symbol $(\frac{a,b}{p})$ as in [15] and the quadratic symbol $(\frac{\alpha}{a})$ as defined in [4; "Exercises"].

I keep all notations of § 1; especially $\Delta = \Delta_0 f^2$ is always a discriminant (not a square), $k_\Delta = \mathbb{Q}(\sqrt{\Delta})$, for $\phi \in C(\Delta)'$ $e_\phi \tilde{e}_\phi = \Delta_0 f_\phi^2$, $K_\phi = \mathbb{Q}(\sqrt{e_\phi}, \sqrt{\tilde{e}_\phi})$, and if $\phi \in \mathfrak{X}(\Delta)$, L_ϕ, f_ϕ^* and σ_ϕ are defined as there.

<u>Theorem A)</u> *For a genus character* $1 \neq \phi \in C(\Delta)'$ *the following assertions are equivalent:*

I. $\phi \in \mathfrak{X}(\Delta)$.

II. *There is an* $\alpha \in \mathbb{Q}(\sqrt{e_\phi})$ *which satisfies the following three conditions:*

1. α *is integral and not divisible by a rational prime.*
2. $N_{\mathbb{Q}(\sqrt{e_\phi})/\mathbb{Q}}(\alpha) = \tilde{e}_\phi \cdot h^2$ *for some* $h \in \mathbb{Q}^\times$;
3. *The relative discriminant* $\mathfrak{d}$ *of* $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}(\sqrt{e_\phi})$ *satisfies* $N(\mathfrak{d}) \cdot e_\phi | \Delta$.

III. *The following two conditions are satisfied:*

1'. $(\frac{e_\phi, \tilde{e}_\phi}{p}) = 1$ *for all* $p \in \mathbb{P} \cup \{\infty\}$;

2'. $f_\phi \cdot z_\phi | f$, *where*

$z_\phi = 1$, if $2 \nmid f_\phi$ *and not* $(e_\phi, \tilde{e}_\phi) \equiv (4,5)$ *or* $(5,4) \bmod 8$;

$z_\phi = 2$ *otherwise.*

If these conditions are fullfilled then $f_\phi^* = f_\phi z_\phi$.

In the field theoretic setting, Theorem A) can be viewed as an imbedding theorem for biquadratic fields into dihedral fields of degree 8 with restricted ramification. As such one it strengthens the known theorems on this subject (see [25], [24; § 1.3] and [23 ; Théorème 12]).

<u>Theorem B)</u> *Suppose* $1 \neq \phi \in \mathfrak{X}(\Delta)$, $a \in \mathbb{R}(\Delta)$, *and let* $\alpha \in \mathbb{Q}(\sqrt{e_\phi})$ *satisfy the conditions* 1., 2. *and* 3. *of Theorem* A), II.

<u>i)</u> *If* $a = N(\mathfrak{a})$ *for an integral ideal* $\mathfrak{a}$ *of* $\mathbb{Q}(\sqrt{e_\phi})$ *then*

$$\sigma_\phi(a) = \left(\frac{\alpha}{\mathfrak{a}}\right) .$$

<u>ii)</u> *If, for some rationals choice of* $\sqrt{e_\phi}$ *modulo* a, $\alpha \equiv b \bmod a$ *with* $b \in \mathbb{Z}$, *then*

$$\sigma_\phi(a) = \left(\frac{b}{a}\right) .$$

<u>iii)</u> *If* $\tilde{\alpha} \in \mathbb{Q}(\sqrt{\tilde{e}_\phi})$ *is integral such that* $\tilde{\alpha}\xi^2 = $ $= \mathrm{Tr}_{\mathbb{Q}(\sqrt{e_\phi})/\mathbb{Q}}(\alpha) + h\cdot\sqrt{\tilde{e}_\phi}$ *with some* $\xi \in \mathbb{Q}(\sqrt{\tilde{e}_\phi})$ *and* $h \in \mathbb{Q}$, *and if* $a = N(\tilde{\mathfrak{a}})$ *with an integral ideal* $\tilde{\mathfrak{a}}$ *of* $\mathbb{Q}(\sqrt{\tilde{e}_\phi})$, *then*

$$\sigma_\phi(a) = \left(\frac{\tilde{\alpha}}{\tilde{\mathfrak{a}}}\right) .$$

<u>iv)</u> *If* $\tilde{\alpha}$ *is as in* <u>iii)</u>, *and if, for some rational choice of* $\sqrt{\tilde{e}_\phi}$ *modulo* a, $\tilde{\alpha} \equiv \tilde{b} \bmod a$ *with* $\tilde{b} \in \mathbb{Z}$, *then*

$$\sigma_\phi(a) = \left(\frac{\tilde{b}}{a}\right) .$$

<u>Theorem B')</u> *Suppose* $1 \neq \phi \in \mathfrak{X}(\Delta)$, $a \in \mathbb{R}(\Delta)$ *and let* e *resp.* $\tilde{e}$ *be the square free kernels of* e_ϕ *resp.* $\tilde{e}_\phi$; *let* e^* *be the product of the odd primes dividing* $\tilde{e}$. *Suppose*

$$\pi = \frac{M+N\sqrt{e}}{w} \in \mathbb{Q}(\sqrt{e_\phi})$$

with $M, N \in \mathbb{Z}$, $M > 0$, $(M,N) = 1$, $w \in \{1,2\}$, $M+N \equiv w \bmod 2$ *and* $w = 1$ *if* $e \not\equiv 1 \bmod 8$, *such that*

$$M^2 - eN^2 = w^2H^2a$$

with $H \in \mathbb{N}$, $(H,2\Delta) = 1$. *Then*

$$\sigma_\phi(a) = \sigma_\phi'(a)\cdot\sigma_\phi''(a)$$

with an "odd" part $\sigma_\phi'(a)$ *and an "even" part* $\sigma_\phi''(a)$, *which can be calculated as follows:*

<u>i)</u> *Let* $\mathfrak{d}^*$ *be an integral ideal of* $\mathbb{Q}(\sqrt{e_\phi})$ *with* $N(\mathfrak{d}^*) = e^*$; *then*

$$\sigma_\phi'(a) = \left(\frac{\pi}{\mathfrak{d}^*}\right) .$$

ii) Suppose $(e,e^*) = 1$ *; then for fixed rational choices of* $\sqrt{e}$ *and* $\sqrt{a}$ *modulo* e^* *I have*

$$\sigma_\phi'(a) = \left(\frac{M+N\sqrt{e}}{e^*}\right)\cdot\left(\frac{w}{e^*}\right) = \left(\frac{M+wH\sqrt{a}}{e^*}\right)\cdot\left(\frac{2w}{e^*}\right) .$$

iii) For the determination of $\sigma_\phi''(a)$ *I distinguisch 9 cases:*

1. $e \equiv \tilde{e} \equiv 1 \bmod 4$: $\sigma_\phi''(a) = 1$.

2. $e \equiv 1 \bmod 4$, $\tilde{e} \equiv 3 \bmod 4$: $\sigma_\phi''(a) = (-1)^{\frac{M+N-1}{2}}$.

3. $e \equiv 1 \bmod 4$, $\tilde{e} \equiv 2 \bmod 4$:

$$\sigma_\phi''(a) = \left(\frac{2}{M+Nt}\right)\cdot(-1)^{\frac{M+N-1}{2}\cdot\frac{\tilde{e}-2}{2}} ,$$ *where* $t \in \mathbb{N}$ *is such that* $t \equiv \frac{e+1}{2} \bmod 8$.

4. $e \equiv 3 \bmod 4$, $\tilde{e} \equiv 1 \bmod 8$: $\sigma_\phi''(a) = 1$.

5. $e \equiv 3 \bmod 4$, $\tilde{e} \equiv 5 \bmod 8$: $\sigma_\phi''(a) = (-1)^N$.

6. $e \equiv 3 \bmod 4$, $\tilde{e} \equiv 2 \bmod 8$: *Putting* $s = \left(\frac{2}{e}\right)$ *I have*

$$\sigma_\phi''(a) = \begin{cases} (-1)^{\frac{1}{8}(e+\tilde{e}-1)}\cdot\left(\frac{2s}{M+N}\right) , & \textit{if } M \equiv 0 \bmod 2 , \\ \left(\frac{2s}{M+N}\right) , & \textit{if } M \equiv 1 \bmod 3 . \end{cases}$$

7. $e \equiv 2 \bmod 4$, $\tilde{e} \equiv 1 \bmod 4$: $\sigma_\phi''(a) = 1$.

8. $e \equiv 2 \bmod 4$, $\tilde{e} \equiv 3 \bmod 4$: $\sigma_\phi''(a) = (-1)^{\frac{M+N-1}{2}}$.

9. $e \equiv \tilde{e} \equiv 2 \bmod 4$: *If* $e \equiv 2\varepsilon \bmod 8$, $\varepsilon \in \{\pm 1\}$,

$$\sigma_\phi''(a) = \begin{cases} \left(\frac{2\varepsilon}{M}\right) , & \textit{if } N \equiv 0 \bmod 4 , \\ \left(\frac{2\varepsilon}{3M}\right) , & \textit{if } N \equiv 2 \bmod 4 . \end{cases}$$

§ 3 Comparasion with the symbols of Rédei and Furuta

As already mentioned in the introduction, the spinor genus symbol $\sigma_\phi(a)$ is closely connected with the symbols defined by

Rédei [24] and Furuta [7]; this section is devoted to a detailed analysis of this connection. The three symbols have different domains of definition neither of which contains the other. The spinor genus symbol and Rédei's symbol coincide on their common domain of definition; the spinor genus symbol and Furuta's symbol coincide on a suitable subdomain of their common domain of definition to be specified.

a) Rédei's symbol

Rédei's symbol $\{a_1,a_2,a_3\}$ is defined for $a_1,a_2,a_3 \in \mathbb{Z}$ which satisfy the following five conditions:

1. a_1 and a_2 are fundamental discriminants, not both negative and not both even.

2. a_3 is positive and square-free; set $a_3 = a_3' a_3''$ where a_3'' is the product of all $p \mid a_3$ with $(\frac{a_1}{p}) = -1$.

3. For all $p \mid a_1 a_2 a_3'$ I have

$$(\frac{a_j}{p}) = 1 \ , \quad \text{if} \quad j \in \{1,2\} \quad \text{and} \quad p \nmid a_j \ ^{1)} \ ,$$

$$(\frac{a_3'}{p}) = 1 \ , \quad \text{if} \quad p \nmid 2a_3 \ .$$

4. $(\frac{-a_1a_2}{p}) = 1$ for all $p \mid (a_1,a_2)$.

5. $(\frac{-a_ja_3'}{p}) = 1$ for $j \in \{1,2\}$ and all odd $p \mid (a_j,a_3')$.

If 1. to 5. are fullfilled then

$$\{a_1,a_2,a_3\} = (\frac{a_2}{a_3''}) \cdot (\frac{\alpha_2}{\mathfrak{a}_3})$$

where $\alpha_2 \in \mathbb{Q}(\sqrt{a_1})$ is such that $N_{\mathbb{Q}(\sqrt{a_1})/\mathbb{Q}}(\alpha_2) = h^2 a_2$ for some $h \in \mathbb{Q}^{\times}$ and the relative discriminant $\mathfrak{d}$ of $\mathbb{Q}(\sqrt{\alpha_2})/\mathbb{Q}(\sqrt{a_1})$

---

1) $(\frac{a}{2}) = 1$ means $a \equiv 1 \bmod 8$

satisfies $N(\mathfrak{d}) = |a_2|$, and $\mathfrak{a}_3$ is an integral ideal of $\mathbb{Q}(\sqrt{a_1})$ with $N(\mathfrak{a}_3) = a_3'$.

From this description I obtain:

Proposition 1. *For* $1 \neq \phi \in C(\Delta)'$ *the following assertions are equivalent:*

i) *Rédei's symbol* $\{e_\phi, \tilde{e}_\phi, a\}$ *is defined for some* $a \in \mathbb{N}$;

ii) $\phi \in \mathfrak{X}(\Delta)$, $2 \nmid f_\phi$, *and* $(e_\phi, \tilde{e}_\phi) \not\equiv (4,5) \bmod 8$, $(e_\phi, \tilde{e}_\phi) \not\equiv (5,4) \bmod 8$.

If these conditions are fullfilled, then, for $a \in \mathbb{R}(\Delta)$, $\sigma_\phi(a) = \{e_\phi, \tilde{e}_\phi, a\}$.

Proof. If $\{e_\phi, \tilde{e}_\phi, a\}$ is defined, then, by 1., 3. and 4., $\left(\frac{e_\phi, \tilde{e}_\phi}{p}\right) = 1$ for all $p \in \mathbb{P} \cup \{\infty\}$ and $(e_\phi, \tilde{e}_\phi) \not\equiv (4,5) \bmod 8$, $(e_\phi, \tilde{e}_\phi) \not\equiv (5,4) \bmod 8$; as e_ϕ and $\tilde{e}_\phi$ are not both even, I have $2 \nmid f_\phi$. Theorem A now implies $\phi \in \mathfrak{X}(\Delta)$ ($z_\phi = 1$, and, obviously, $f_\phi | f$).

If the conditions ii) are fullfilled, then, by Theorem A, $\left(\frac{e_\phi, \tilde{e}_\phi}{p}\right) = 1$ for all $p \in \mathbb{P} \cup \{\infty\}$; thus e_ϕ, $\tilde{e}_\phi$ are not both negative, $\left(\frac{e_\phi}{p}\right) = 1$ for all odd p with $p | \tilde{e}_\phi$, $p \nmid e_\phi$, $\left(\frac{\tilde{e}_\phi}{p}\right) = 1$ for all odd p with $p | e_\phi$, $p \nmid \tilde{e}_\phi$ and $\left(\frac{-e_\phi \tilde{e}_\phi}{p}\right) = 1$ for all odd $p | (e_\phi, \tilde{e}_\phi)$; but as $2 \nmid f_\phi$, e_ϕ and $\tilde{e}_\phi$ are not both even, and as further $(e_\phi, \tilde{e}_\phi) \not\equiv (4,5) \bmod 8$, $(e_\phi, \tilde{e}_\phi) \not\equiv (5,4) \bmod 8$, the above formulae are also valid for $p = 2$; if now $a \in \mathbb{R}(\Delta)$, then $\{e_\phi, \tilde{e}_\phi, a\}$ is defined.

Suppose now $a \in \mathbb{R}(\Delta)$ and that $\{e_\phi, \tilde{e}_\phi, a\}$ is defined. To prove $\sigma_\phi(a) = \{e_\phi, \tilde{e}_\phi, a\}$, let $\alpha \in \mathbb{Q}(\sqrt{e_\phi})$ be as in Theorem A, and let $\mathfrak{d}$ be the relative discriminant of $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}(\sqrt{e_\phi})$. Then, for the discriminant D of $\mathbb{Q}(\sqrt{\alpha})$ I have $|D| = N(\mathfrak{d}) \cdot e_\phi^2$ and also $|D| = \Delta_o e_\phi f_\phi^{*2}$ [10; Satz 24], so $N(\mathfrak{d}) = \frac{\Delta_o f_\phi^{*2}}{e_\phi} =$

$= \tilde{e}_\phi \cdot (\frac{f^*_\phi}{f_\phi}) = \tilde{e}_\phi$ as $f^*_\phi = z_\phi f_\phi = f_\phi$ (by Theorem A). Therefore $\{e_\phi, \tilde{e}_\phi, a\} = (\frac{\alpha}{\mathfrak{a}})$ if $\mathfrak{a}$ is an integral ideal of $\mathbb{Q}(\sqrt{e_\phi})$ with $N(\mathfrak{a}) = a$, and this proves $\{e_\phi, \tilde{e}_\phi, a\} = \sigma_\phi(a)$ by Theorem B), i), q. e. d.

From Proposition 1 it follows, that $\sigma_\phi(a)$ may be defined even if $\{e_\phi, \tilde{e}_\phi, a\}$ is not (namely, when $z_\phi = 2$); on the other hand there are many cases in which $\{e_\phi, \tilde{e}_\phi, a\}$ is defined, but $a \notin \mathbb{R}(\Delta)$.

b) Furuta's symbol

The definition of Furuta's symbol uses the notation of genus fields and central class fields as follows:

Let L be a finite abelian and M a finite normal algebraic number field such that $L \subset M$; then L^* denotes the maximal absolutely abelian number field containing L such that L^*/L is unramified outside infinity ("absolute genus field in the narrow sense"); L^*_M denotes the maximal absolutely abelian subfield of M ("genus field of L/M "); L'_M denotes the maximal normal subfield of M containing L for which $Gal(L'_M/L)$ lies in the center of $Gal(L'_M/Q)$ ("central class field of L/M ").

Furuta's symbol $[d_1, d_2, a]$ is defined for rational integers d_1, d_2, a such that $L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ is a biquadratic field and there is a full ray class field in the narrow sense R of L such that the following conditions are satisfied:

1. $R/\mathbb{Q}$ is normal;
2. $L^*_R \subsetneq L'_R$ (if this is the case, then $[L'_R : L^*_R] = 2$);
3. a is square free, positive, and all primes $p|a$ split completely in L^*_R .

If 1., 2. and 3. are fullfilled then

$$[d_1, d_2, a] = (\frac{L'_R/L^*_R}{\mathfrak{a}})$$

with an integral ideal $\mathfrak{a}$ of L^*_R such that $N(\mathfrak{a}) = a$.

<u>Proposition 2.</u> *Suppose* $\phi \in \mathfrak{X}(\Delta)$ *and* $a \in \mathbb{N}$.

<u>i)</u> *Let Furuta's symbol* $[e_\phi, \tilde{e}_\phi, a]$ *be defined and assume* $p \equiv 1 \bmod 8$ *for all primes* $p|a$ *if* $e_\phi \equiv \tilde{e}_\phi \equiv 0 \bmod 8$ *and* $\Delta_o \equiv 1 \bmod 4$ *; then* $a \in \mathbb{R}(\Delta)$.

<u>ii)</u> *Suppose* $a \in \mathbb{R}(\Delta)$ *; then there is a unique integer* F_ϕ *with* $F_\phi | f^*_\phi$ *such that* $[e_\phi, \tilde{e}_\phi, a]$ *is defined iff* $p \equiv 1 \bmod F_\phi$ *for all primes* $p|a$.

<u>iii)</u> *Let* $[e_\phi, \tilde{e}_\phi, a]$ *be defined and suppose* $a \in \mathbb{R}(\Delta)$ *and* $p \equiv 1 \bmod g$ *for all* $p|a$ *where*

$$g = \begin{cases} f_\phi , & \text{if } e_\phi \equiv \tilde{e}_\phi \equiv 0 \bmod 8 \text{ and } \Delta_o \equiv 0 \bmod 4 , \\ f^*_\phi & \text{otherwise;} \end{cases}$$

then $\sigma_\phi(a) = [e_\phi, \tilde{e}_\phi, a]$.

<u>Proof.</u> <u>i)</u> Let R be a ray class field over $L = K_\phi = \mathbb{Q}(\sqrt{e_\phi}, \sqrt{\tilde{e}_\phi})$ defining the symbol $[e_\phi, \tilde{e}_\phi, a]$, i. e. $R/\mathbb{Q}$ is normal, $L^*_R \subsetneq L'_R$, all primes $p|a$ split completely in L^*_R and $[e_\phi, \tilde{e}_\phi, a] = \left(\frac{L'_R/L^*_R}{\mathfrak{a}}\right)$ for an integral ideal $\mathfrak{a}$ of L^*_R with $N(\mathfrak{a}) = a$. Let $\bar{K}_\phi$ be the genus field of the ring class field modulo f_ϕ over $k_\Delta = \mathbb{Q}(\sqrt{\Delta_o})$. Then, by [11], $\bar{K}_\phi/L$ is unramified (so $\bar{K}_\phi \subset L^*_R$) unless $\Delta_o \equiv 1 \bmod 4$ and $2^3 | f_\phi$ in which case $\bar{K}_\phi \subset L^* \cdot \mathbb{Q}^{(8)}$ [1]) (so $\bar{K}_\phi \subset L^*_R \cdot \mathbb{Q}^{(8)}$). Thus all primes $p|a$ split in $\bar{K}_\phi$, i. e. $a \in \mathbb{R}(\Delta)$.

<u>ii)</u>, <u>iii)</u> Let S be the ray class field (in the narrow sense) modulo f^*_ϕ over $k_\Delta = \mathbb{Q}(\sqrt{\Delta_o})$ and $L = K_\phi = \mathbb{Q}(\sqrt{e_\phi}, \sqrt{\tilde{e}_\phi})$. Then, as $L_\phi/\mathbb{Q}$ is dihedral and f^*_ϕ is the conductor of L_ϕ/k_Δ , $L_\phi \subset L'_S$ and $L_\phi \not\subset L^*_S$, so $L^*_S \subsetneq L'_S$, and by [7; Prop. 2.1] the symbol $[e_\phi, \tilde{e}_\phi, a]$ is defined if every prime $p|a$ splits completely in L^*_S , and moreover, if this is the case, then

$$[e_\phi, \tilde{e}_\phi, a] = \left(\frac{L'_S/L^*_S}{\mathfrak{A}}\right) = \left(\frac{L_\phi/L}{\mathfrak{a}}\right) = \sigma_\phi(a)$$

---

[1]) $\mathbb{Q}^{(n)}$ is the field of n-th roots of unity.

(by the Translation Theorem of class field theory) if $\mathfrak{A}$ resp. $\mathfrak{a}$ is an integral ideal of L_S^* resp. $L = K_\phi$ such that $N(\mathfrak{A}) = N(\mathfrak{a}) = a$. But $L_S^* = K_S^* = K^* \cdot \mathbb{Q}^{(g)}$ by [7; Theorem 4.3] and thus every prime $p|a$ splits completely in L_S^* ; this proves iii).

To obtain ii), let R be an arbitray ray class field in the narrow sense over $L = K_\phi = \mathbb{Q}(\sqrt{e_\phi}, \sqrt{\tilde{e}_\phi})$ for which $R/\mathbb{Q}$ is normal and $L_R^* \subsetneq L_R'$. By [7; Theorem 4.2], $L_R^* = L^* \cdot \mathbb{Q}^{(F)}$ for some $F \in \mathbb{N}$; by [21], L^*/Q is elementary abelian and therefore contained in the genus field of the ring class field modulo f_ϕ over $k_\Delta = \mathbb{Q}(\sqrt{\Delta_o})$ [11] whence all $p \in \mathbb{P}(\Delta)$ split completely in L^* . Thus R can be used to define $[e_\phi, \tilde{e}_\phi, a]$ iff all primes $p|a$ satisfy $p \equiv 1 \bmod F$; if F_ϕ denotes the minimal possible F , the assertion follows, q. e. d.

It seems to be difficult to determine the exact range of coincidence of Furuta's symbol with the spinor genus symbol, even if one restricts the considerations to strictly defined symbols in the sense of [7; Def. 4.2]. But there are cases in which both symbols are defined and take different values, i. e.: $\Delta = -192$, $e_\phi = -8$, $\tilde{e}_\phi = 24$, $a = 73$, where $\sigma_\phi(a) = -1$ and $[-8,24,73] = +1$, as the representations $73 \cdot 1^2 = 5^2 + 48 \cdot 1^2$, $73 \cdot 13^2 = 103^2 + 192 \cdot 3^2$ show (use [7; Theorem 5.1] and § 1, Corollary 2).

In [8] the results of [12] concerning the quadratic resp. biquadratic characters of quadratic units are rephrased in terms of Furuta's symbol; to do this it is necessary to restrict the considerations in the case $t = 2$ to $q \equiv 1 \bmod 16$ (in the terminology of [8]) as done there. This restriction however comes from the method and not from the problem and it can be dropped if one uses the spinor genus symbol $\sigma_\phi(q)$ for $e_\phi = dt$, $\tilde{e}_\phi = -et$ instead of the symbol $[dt,-et,q]$; it is not difficult to work out the details.

LITERATURE

[1] I. Borevič, I. R. Shafarevič, Zahlentheorie. Birkhäuser 1966

[2] E. Brown, Biquadratic reciprocity laws, Proc. Amer. Math. Soc. 37 (1973), 374 - 476

[3] E. Brown, A theorem on biquadratic reciprocity, Proc. Amer. Math. Soc. 30 (1971), 220 - 222

[4] J. W. S. Cassels, A. Fröhlich, Algebraic Number Theory. Academic Press 1967

[5] D. R. Estes, G. Pall, Spinor Genera of Binary Quadratic Forms, J. Number Theory 5 (1973), 421 - 432

[6] Y. Furuta, Note on class number factors and prime decompositions, Nagoya Math. J. 66 (1977), 167 - 182

[7] Y. Furuta, A prime decomposition symbol for a non abelian central extension which is abelian over a bicyclic biquadratic field, Nagoya Math. J. 79 (1980), 79 - 109

[8] Y. Furuta, P. Kaplan, On Quadratic and Quartic Characters of Quadratic Units, Sci. Rep. Kanazawa Univ. 26 (1981), 27 - 30

[9] A. Fröhlich, A prime decomposition symbol for certain non Abelian number fields, Acta Sci. Math. 21 (1960), 229 - 246

[10] F. Halter-Koch, Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe, J. Number Theory 3 (1971), 412 - 443

[11] F. Halter-Koch, Geschlechtertheorie der Ringklassenkörper, J. f. reine u. angew. Math. 250 (1971), 107 - 108

[12] F. Halter-Koch, P. Kaplan, K. S. Williams, An Artin character and representations of primes by binary quadratic forms II, Manuscr. math. 37 (1982), 357 - 381

[13] F. Halter-Koch, Binäre quadratische Formen und Diederkörper, to appear

[14] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I. Physika-Verlag, Würzburg 1965

[15] H. Hasse, Number Theory. Springer 1980

[16] P. Kaplan, Representations of prime numbers by classes of binary quadratic forms, Proc. Intern. Symp. on Alg. Number

Theory, Kyoto 1976

[17] P. Kaplan, K. S. Williams, Y. Yamamoto, An application of dihedral fields to representations of primes by binary quadratic forms, Acta Arithmetica 44 (1984), 407 - 413

[18] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern, J. Math. Soc. Japan 3 (1951), 148 - 156

[19] P. A. Leonard, K. S. Williams, A representation problem involving binary quadratic forms, Arch. Math. 36 (1981), 53 - 56

[20] P. A. Leonard, K. S. Williams, An Observation on Binary Quadratic Forms of Discriminant -32q , Abh. Math. Inst. d. Univ. Hamburg 53 (1983), 39 - 40

[21] H. W. Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr. 9 (1953), 350 - 362

[22] J. B. Muskat, On Simultaneous Representations of Primes by Binary Quadratic Forms, J. Number Theory 19 (1984), 263 - 282

[23] B. Perrin-Riou, Plongement d'une extension diédrale dans une extension diédrale ou quaternionienne. Ann. Inst. Gourier 30 (1980), 19 - 33

[24] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, J. f. reine u. angew. Math. 180 (1939), 1 - 43

[25] L. Rédei, H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. f. reine u. angew. Math. 170 (1933), 69 - 74

[26] A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Zeitschr. 39 (1934), 95 - 111

[27] J.-P. Serre, Local Class Field Theory, in "Algebraic Number Theory", ed. by J. W. S. Cassels and A. Fröhlich, Academic Press 1967 (see [4])

[28] H. C. Williams, The quadratic character of a certain quadratic surd, Utilitas math. 5 (1974), 49 - 55

Franz Halter-Koch
Institut für Mathematik
Karl-Franzens-Universität

Halbärthgasse 1/1
A-8010 Graz
Austria