A prime decomposition symbol for certain non Abelian number fields

By A. FRÖHLICH in London

Dedicated to Professor L. Rédei on his 60th birthday

In a recent paper (cf. [4])[1] I gave a rational description of normal[2] fields Λ of prime power degree l^{n+1} which contain an Abelian subfield K of degree l^n. This made it possible in particular to determine in purely rational terms the group extensions of a group of order l by the Galois group of K which are realised by such fields Λ, and the relative ramification types of $\Lambda/$K which will occur.

In the present paper we shall consider normal non cyclic fields Λ of degree 8. Every such field will contain a biquadratic field[3] $\mathrm{P}(\sqrt{d_1}, \sqrt{d_2})$ and so the theory of [4] can be applied. We shall principally be concerned with a new symbol $[a_1, a_2, a]_c$; the variable c is a factor system class of the "Vierer-gruppe" in the group of square roots of unity, and the variables a_1, a_2, a are non zero rational numbers satisfying certain conditions. In the significant cases a_1, a_2 coincide with the independent quadratic discriminants d_1, d_2. When a is then a rational prime which is total norm residue of $\mathrm{P}(\sqrt{d_1}, \sqrt{d_2})$, the value of the symbol will determine the decomposition of (a) in a field Λ, belonging to the factor system class c. Though we are of course principally interested in non Abelian fields, it will be useful for a proper theoretical understanding to treat simultaneously all fields containing $\mathrm{P}(\sqrt{d_1}, \sqrt{d_2})$. In order to keep this paper at a reasonable length we shall however make at some stage (cf. (2.15)) the restriction that d_1, d_2 be odd.

It will be seen that the symbol $[a_1, a_2, a]_c$ is unrestrictedly multiplicative in a and c, and partially multiplicative in a_1, a_2. It moreover admits two basic inversion laws. For the first of these we shall interpret the symmetric

[1] Numbers in square brackets refer to the literature list.

[2] Terms such as "normal", "Abelian", "degree" are to be understood in the absolute sense, i. e. with respect to the rational field, unless otherwise qualified.

[3] P is the rational field.

group of permutations on three symbols simultaneously as group of permutations of the three quadratic discriminants associated with the field $P(\sqrt{d_1}, \sqrt{d_2})$ and as a group of automorphisms of the "Vierer-gruppe". Each permutation then gives rise to an inversion formula. The second inversion law on the other hand is closely connected with quadratic reciprocity in quadratic fields.

We shall also give explicit expressions for the new symbol in terms of values of rational residue characters associated with certain rational ternary quadratic forms, and thus obtain rational prime-decomposition criteria for a class of non Abelian fields. Some of the multiplication laws and inversion formulae will then have interesting interpretations in terms of the explicit expressions given.

Decomposition criteria for certain non Abelian fields of degree 8[1]) were found for the first time by S. KURODA (cf. [7]), whose results where subsequently extended by FURUTA to the relative case (cf. [5], [6]). The class of fields covered by S. KURODA was discussed again in a paper of the author's (cf. [3]), in conjunction with a general theory of the restricted biquadratic residue symbol. In view of our present restriction to odd quadratic discriminants there is no overlap between the class of fields considered here and that considered in the quoted papers. The results of [3] can however easily be rephrased in terms of suitable symbols $[a_1, a_2, a]_c$.

Our symbol has a "restricted" argument domain. It was L. RÉDEI who first saw the importance of such restricted symbols when dealing with problems of a "non-Abelian" nature (cf. [10], [11]). Altogether our subject matter is closely related to L. RÉDEI's work on quadratic fields (cf. [8], [9], [11]), and in particular to the symbol defined by him in [9], and applied to a number of problems. L. RÉDEI's symbol is in fact essentially the same as ours for a certain fixed value of the variable c, and the multiplication and inversion laws for this case can already be found in his original paper.

§ 1.

P is throughout the rational field. The Galois group of a normal extension Λ of an algebraic number field K will be denoted by $\Gamma(\Lambda/K)$. We shall use the results of class field theory in a finite number field K as formulated in terms of idèle class characters (cf. [1]), i. e. of continuous characters of the idèle group of K which take trivial value on the principal idèles. To each Abelian extension Λ/K there will then correspond a group $\Phi(\Lambda/K)$ of such characters; $\Phi(\Lambda/K)$ can also be considered as the group of

[1]) And of course for composites of such fields with Abelian fields.

continuous characters of $\Gamma(A/K)$. If φ is an idèle class character in K we denote by K_φ the associated class field; thus $\Phi(K_\varphi/K)$ is a cyclic group with generator φ.

If Ω is a subfield of K we can associate with every idèle class character ψ in Ω, a character[5]) $R_{K/\Omega}\psi$ in K by the rule (cf. [4])

$$R_{K/\Omega}\psi(\mathfrak{m}) = \psi(N_{K/\Omega}\mathfrak{m}) \tag{1.1}$$

for all idèles $\mathfrak{m}$ in K, $N_{K/\Omega}$ being the norm mapping. $R_{K/\Omega}$ is a homomorphism.

Denote by Q_φ the group of ideals in K which are integral for and prime to the conductor[6]) $\mathfrak{f}(\varphi)$ of the character φ in K. For $\mathfrak{a} \in Q_\varphi$ choose any idèle $\mathfrak{m}$ with contents $(\mathfrak{m}) = \mathfrak{a}$, whose components $\mathfrak{m}_\mathfrak{p}$ have value 1 whenever $\mathfrak{p}$ divides $\mathfrak{f}(\varphi)$ or is an infinite prime. $\varphi(\mathfrak{m})$ is then independent of the particular choice of $\mathfrak{m}$ within the stated conditions so that we may write

$$\varphi(\mathfrak{m}) = \theta_\varphi(\mathfrak{a}). \tag{1.2}$$

θ_φ is a character of the ideal group Q_φ; $\theta_\varphi(\mathfrak{a}) = 1$ if and only if we have for the Artin symbol of $\mathfrak{a}$, $(K_\varphi/K; \mathfrak{a}) = 1$. For characters φ_1, φ_2 we get

$$\theta_{\varphi_1\varphi_2}(\mathfrak{a}) = \theta_{\varphi_1}(\mathfrak{a})\theta_{\varphi_2}(\mathfrak{a}) \tag{1.3}$$

whenever $\mathfrak{a} \in Q_{\varphi_1} \cap Q_{\varphi_2}$.

Let Q_φ^* be the group of non zero elements α of K with $(\alpha) \in Q_\varphi$. We write for $\alpha \in Q_\varphi^*$

$$\chi_\varphi(\alpha) = \Pi \varphi_\mathfrak{p}(\alpha) \tag{1.4}$$

the product extending over the finite prime divisors ramified at φ. χ_φ is a residue character, and again

$$\chi_{\varphi_1\varphi_2}(\alpha) = \chi_{\varphi_1}(\alpha)\chi_{\varphi_2}(\alpha) \tag{1.5}$$

for $\alpha \in Q_{\varphi_1}^* \cap Q_{\varphi_2}^*$. As $\varphi(\alpha) = 1$ we also get

$$\theta_\varphi((\alpha)) = \chi_\varphi^{-1}(\alpha)\varphi_\infty(\alpha) \tag{1.6}$$

where φ_∞ is the product of the infinite components of φ.

Assume now K to be normal over a subfield Ω. An ideal $\mathfrak{A}$ in K is said to be *primitive* (with respect to Ω) if in its prime power decomposition

$$\mathfrak{A} = \prod_i \mathfrak{P}_i^{r_i}$$

[5]) The term "character" without further qualification will be used as synonymous with "idèle class character".

[6]) $\mathfrak{f}(\varphi)$ is considered as an ideal, i.e. the prime divisors of $\mathfrak{f}(\varphi)$ are the finite ramified prime divisors (prime ideals).

no two of the prime ideals $\mathfrak{P}_i$ occurring non trivially are conjugate over Ω. Let φ be a character in K such that K_φ is a *central extension* of K over Ω, i.e. that K_φ is normal over Ω and $\Gamma(K_\varphi/K)$ lies in the centre of $\Gamma(K_\varphi/\Omega)$. Such a character φ is characterised by the equations

$$(1.7) \qquad \varphi^\gamma = \varphi \quad \text{for all} \quad \gamma \in \Gamma(K/\Omega).$$

Let $N(K/\Omega)$ be the group of ideals in Ω which are norms of ideals in K. Every ideal $\mathfrak{a}$ in $N(K/\Omega)$ is then also the norm of a primitive ideal $\mathfrak{A}$ in K; if $\mathfrak{a}$ is integral for and prime to the conductor $\mathfrak{f}(\varphi)$ then so is $\mathfrak{A}$. Hence $\theta_\varphi(\mathfrak{A})$ is defined; in view of (1.7) its value will not depend on $\mathfrak{A}$ but solely on $\mathfrak{a}$. We may thus write

$$(1.8) \qquad \theta_\varphi(\mathfrak{A}) = (N_{K/\Omega}\theta_\varphi)(\mathfrak{a}).$$

If $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are ideals in $N(K/\Omega)$ then they are norms of primitive ideals $\mathfrak{A}_1$ and $\mathfrak{A}_2$ so that $\mathfrak{A}_1\mathfrak{A}_2$ is again primitive. Hence

$$(1.9) \qquad (N_{K/\Omega}\theta_\varphi)(\mathfrak{a}_1\mathfrak{a}_2) = (N_{K/\Omega}\theta_\varphi)(\mathfrak{a}_1)\cdot(N_{K/\Omega}\theta_\varphi)(\mathfrak{a}_2).$$

On the other hand we have by (1.3)

$$(1.10) \qquad (N_{K/\Omega}\theta_{\varphi_1\varphi_2})(\mathfrak{a}) = (N_{K/\Omega}\theta_{\varphi_1})(\mathfrak{a})\cdot(N_{K/\Omega}\theta_{\varphi_2})(\mathfrak{a}).$$

Both in (1.9) and in (1.10) the left hand side is defined provided that the right hand side is.

§ 2.

Throughout Γ is a fixed, non cyclic group of order 4 with γ_1, γ_2 as a given, ordered pair of generators. F is the group of factor system classes of Γ in the group E of square roots of unity. For any factor system $\bar{c}$ in a given class c the elements

$$(2.1) \qquad \begin{cases} \bar{c}(\gamma_i, 1)\,\bar{c}(\gamma_i, \gamma_i) = (-1)^{c(\gamma_i)} \\ \bar{c}(\gamma_1, \gamma_2)\,\bar{c}(\gamma_2, \gamma_1)^{-1} = (-1)^{c(\gamma_1, \gamma_2)} \end{cases} \qquad (i = 1, 2)$$

depend only on c and will in turn determine c uniquely. Accordingly we represent the elements of F as sequences

$$(2.2) \qquad c = [c(\gamma_1), c(\gamma_2), c(\gamma_1, \gamma_2)]$$

of integers mod 2, multiplication in F being given by component-wise addition mod 2. Each such sequence will in fact represent an element of F. It will be useful to write

$$(2.3) \qquad \gamma_1\gamma_2 = \gamma_3, \quad c(\gamma_3) \equiv c(\gamma_1) + c(\gamma_2) + c(\gamma_1, \gamma_2) \pmod 2.$$

We shall find it convenient to consider the $c(\gamma_i)$, and $c(\gamma_1, \gamma_2)$ actually as integers, normalised to the values 0 or 1.

Let d_1, d_2 be an ordered pair of independent quadratic discriminants. Then

$$\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2}) \tag{2.4}$$

is a non cyclic, biquadratic field. We shall repeatedly use the symbols

$$\left\{\begin{array}{l} d_3 = d_1 d_2/(d_1, d_2)^2, \\ f_1 = (d_2, d_3), \quad f_2 = (d_3, d_1), \quad f_3 = (d_1, d_2), \end{array}\right. \tag{2.5}$$

where (a, b) is always taken to be positive. With the given pair d_1, d_2 we associate the isomorphism

$$g_{d_1, d_2} = g \colon \quad \Gamma \cong \Gamma(\mathsf{K}/\mathsf{P})$$

uniquely determined by

$$\sqrt{d_i}^{\,g(\gamma_j)-1} = (-1)^{\delta_{ij}} \qquad (i, j = 1, 2), \tag{2.6}$$

δ_{ij} being the Kronecker symbol.

Let Σ be the symmetric group of permutations on the symbols 1, 2, 3. For each $\pi \in \Sigma$ we have then $\mathsf{K} = \mathsf{P}(\sqrt{d_{\pi(1)}}, \sqrt{d_{\pi(2)}})$ and there exists a unique isomorphism

$$g_\pi \colon \quad \Gamma \cong \Gamma(\mathsf{K}/\mathsf{P})$$

such that

$$\sqrt{d_{\pi(i)}}^{\,g_\pi(\gamma_j)-1} = (-1)^{\delta_{ij}} \qquad (i, j = 1, 2). \tag{2.7}$$

There will then exist a unique automorphism π' of Γ such that

$$g_\pi = g \circ \pi'. \tag{2.8}$$

The characters φ in K with

$$\varphi^2 = 1 = \varphi^{\gamma-1} \tag{2.9}$$

for all $\gamma \in \Gamma(\mathsf{K}/\mathsf{P})$ form a group which we shall here denote by Φ_K. The fields K_φ $(\varphi \in \Phi_\mathsf{K})$ are precisely those cyclic extensions of K of relative degree 2 (or 1) which are central extensions of K over P, i. e. which are (absolutely) normal. For each φ $\Gamma(\mathsf{K}_\varphi/\mathsf{P})$ is a group extension of $\Gamma(\mathsf{K}_\varphi/\mathsf{K})$ by $\Gamma(\mathsf{K}/\mathsf{P})$ and thus determines a class b_φ in the group $F(\mathsf{K}, \varphi)$ of factor system classes of $\Gamma(\mathsf{K}/\mathsf{P})$ in $\Gamma(\mathsf{K}_\varphi/\mathsf{K})$. To describe this extension in terms of the fixed group F we only have to note that the isomorphism $g\colon \Gamma \cong \Gamma(\mathsf{K}/\mathsf{P})$ together with the homomorphism $\varphi\colon \Gamma(\mathsf{K}_\varphi/\mathsf{K}) \to E$ gives rise to a homomorphism

$$g^* \colon \quad F(\mathsf{K}, \varphi) \to F. \tag{2.10}$$

If $\varphi \neq 1$, then φ is an isomorphism, and so g^* is an isomorphism. On replacing g by g_π we get

$$(2.11) \qquad g^*_\pi = \pi^* \circ g^*$$

where π^* is the automorphism of F induced by π'.

For fixed d_1, d_2 we shall write

$$(2.12) \qquad g^*(b_\varphi) = c_\varphi .$$

Explicitly we have for $c = c_\varphi$, for any representatives $\bar{\gamma}_i$ of $g(\gamma_i)$ in $\Gamma(\mathsf{K}_\varphi/\mathsf{P})$ $(i = 1, 2)$, and for ω as generator of $\Gamma(\mathsf{K}_\varphi/\mathsf{K})$ the relations [7]

$$(2.13) \qquad \bar{\gamma}_i^2 = \omega^{c(\gamma_i)} \ (i = 1, 2), \quad (\bar{\gamma}_1, \bar{\gamma}_2) = \omega^{c(\gamma_1, \gamma_2)}.$$

Thus K_φ is non Abelian if and only if $c(\gamma_1, \gamma_2) = 1$.

The c_φ are those classes in F which in terms of the given isomorphism g are *realised arithmetically* by actual extensions of K. By [4] (Theorem 1) we have

Theorem 1. *$\varphi \rightarrow c_\varphi$ is a homomorphism whose kernel is the group of characters $R_{\mathsf{K}/\mathsf{P}}\psi$ with $\psi^2 = 1$.*

The classes c_φ will thus form a subgroup $A(d_1, d_2)$ of F. As a special case of the general criterion in [4] (Theorem 7) we get

Theorem 2. *An element c in F will lie in $A(d_1, d_2)$ if and only if*

$$\left(\frac{-1, d_1}{p}\right)^{c(\gamma_1)} \left(\frac{-1, d_2}{p}\right)^{c(\gamma_2)} \left(\frac{d_1, d_2}{p}\right)^{c(\gamma_1, \gamma_2)} = 1$$

for all rational prime divisors p.

It will of course always suffice to consider only the prime factors p of d_1, d_2.

Those characters φ in Φ_K whose conductor $\mathfrak{f}(\varphi)$ contains only such prime ideals which are also contained in $d_1 d_2$ form a subgroup Φ^*_K of $\Phi_\mathsf{K} \cdot \mathfrak{f}(\varphi)$ is always the relative discriminant of $\mathsf{K}_\varphi/\mathsf{K}$. The element φ of Φ^*_K are thus characterised in Φ_K by the property that every rational discriminant prime divisor of K_φ is already a discriminant prime divisor of K. The importance of the group Φ^*_K was exhibited in Theorems 5 (Corollary 1) and 11 in [4].

Let K^* be the genus field of K (in the narrow sense) i.e. the maximal (absolutely) Abelian field which contains K and has relative discriminant (1) over K. $\Phi(\mathsf{K}^*/\mathsf{K})$ is then the subgroup of Φ^*_K of those characters satisfying the equations

$$(2.14) \qquad \chi_\varphi = 1, \quad c_\varphi = 1.$$

[7] In (2. 13) $(\bar{\gamma}_1, \bar{\gamma}_2)$ is the commutator.

From now on, and for the remainder of this paper it will be assumed that

(2.15) $$d_1 \equiv d_2 \equiv 1 \pmod 4.$$

Then we have (cf. [4], Theorems 8, 11):

Theorem 3. *For each $c \in A(d_1, d_2)$ $\exists \varphi \in \Phi_K^*$ with $c = c_\varphi$, and the characters $\varphi \in \Phi_K^*$ with this property form a coset $\Phi^*(c) = \Phi^*(d_1, d_2, c)$ of*[8] *Φ_K^* mod $\Phi(K^*/K)$.*

From the last assertion it follows that for each $c \in A(d_1, d_2)$ we have a unique residue character

(2.16) $$\chi_c = \chi_\varphi \qquad (\varphi \in \Phi^*(d_1, d_2, c)),$$

and so a unique conductor

(2.17) $$\mathfrak{d}_c = \mathfrak{f}(\varphi).$$

$\mathfrak{d}_c$ is the relative discriminant over K of all fields K_φ with $\varphi \in \Phi^*(c)$.

For an explicit description of χ_c we note firstly that in view of (2.9) conjugate prime ideals in K have the same ramification behaviour in K_φ. In the second place as "even" prime ideals can be neglected the only possible non trivial prime components of χ_c are those given by the quadratic residue symbols $\left(\frac{\cdot}{\mathfrak{P}}\right)$. It will thus suffice to find those rational prime factors of $d_1 d_2$ which are coprime to $\mathfrak{d}_c$. Every rational prime factor p of $d_1 d_2$ divides one and only one of the integers f_i defined in (2.5). Assume, say $p | f_1$. Then the inertia group of p in K/P is generated by $g(\gamma_2)$, and so by (2.13) $\omega^{c(\gamma_2)}$ will generate the inertia group in K_φ/K of the prime divisors of p in K. In this manner we have proved the

Proposition 2.1. $(p, \mathfrak{d}_c) = 1$ *if and only if*

$$(p, f_1^{c(\gamma_2)} f_2^{c(\gamma_1)} f_3^{c(\gamma_3)}) = 1.$$

Next we consider criteria for K_φ to be real, assuming now that K is real. If first $\left(\frac{-1, d_i}{p}\right) = -1$ for some i and some p, then K^* is imaginary. It follows easily from Theorem 3 that there will be both real and imaginary fields K_φ with $\varphi \in \Phi^*(c)$.

Now assume that $\left(\frac{-1, d_i}{p}\right) = 1$ for all p and for $i = 1, 2$. In this case the restricted biquadratic residue symbols $\left[\frac{-1}{d_i}\right]$, $\left[\frac{-1}{f_i}\right]$ are defined (cf. [3]),

[8] $\Phi^*(c)$ will actually depend on the ordered pair d_1, d_2. Whenever this is to be stressed the symbol $\Phi^*(d_1, d_2, c)$ will be used.

and the criterion of Theorem 2 reduces to

$$\left(\frac{d_1, d_2}{p}\right)^{c(\gamma_1, \gamma_2)} = 1.$$

Thus if $c(\gamma_1, \gamma_2) = 1$ then for $p | f_i$ we have $\left(\frac{p}{d_i}\right) = 1$; therefore the symbols $\left[\frac{f_i}{d_i}\right]$ are defined. We then have

Theorem 4. *Assume d_1, d_2 to be products of primes* $\equiv 1 \pmod 4$, *and that $c \in A(d_1, d_2)$. The property of $K_\varphi(\varphi \in \Phi^*(c))$ to be real or imaginary will then solely depend on c.*

For $c(\gamma_1, \gamma_2) = 0$, K_φ is real if and only if

$$\left[\frac{-1}{d_1}\right]^{c(\gamma_1)} \cdot \left[\frac{-1}{d_2}\right]^{c(\gamma_2)} = 1.$$

For $c(\gamma_1, \gamma_2) = 1$, K_φ is real if and only if

$$\left[\frac{-1}{d_1}\right]^{c(\gamma_1)} \left[\frac{-1}{d_2}\right]^{c(\gamma_2)} \left[\frac{f_1}{d_1}\right] \left[\frac{f_2}{d_2}\right] \left[\frac{f_3}{d_3}\right] \left[\frac{-1}{f_3}\right] \left(\frac{f_2}{f_3}\right) = 1.$$

We shall not give a proof of this theorem. Such a proof would follow the line of argument in [2] p. 248—249. For $(d_1, d_2) = 1$, $c(\gamma_1) = c(\gamma_2) = 0$, $c(\gamma_1, \gamma_2) = 1$ the criterion is effectively due to L. Rédei (cf. [8]).

There is an apparent asymmetry in the factor $\left(\frac{f_2}{f_3}\right)$ occurring in the last formula of the theorem. The hypothesis however implies that $\left(\frac{f_2}{f_3}\right) = \left(\frac{f_1}{f_3}\right)$, and in fact more generally that $\left(\frac{f_2}{f_3}\right) = \left(\frac{f_i}{f_j}\right)$ for all $i, j = 1, 2, 3$; $i \neq j$.

§ 3.

We consider triplets

$$\{d_1, d_2, c\}$$

where d_1, d_2 *are square free integers* $\equiv 1 \pmod 4$ with $d_i = 1$ as possible values and where $c \in F$. The following postulates are to be satisfied:

A. (i) *Whenever d_1, d_2 are independent quadratic discriminants* (i. e. $1 \neq d_1 \neq d_2 \neq 1$) *then $c \in A(d_1, d_2)$,* i. e. *for all p*

$$\left(\frac{-1, d_1}{p}\right)^{c(\gamma_1)} \left(\frac{-1, d_2}{p}\right)^{c(\gamma_2)} \left(\frac{d_1, d_2}{p}\right)^{c(\gamma_1, \gamma_2)} = 1.$$

(ii) *Whenever* $d_1 = d_2$ *then for all* p

$$\left(\frac{-1, d_2}{p}\right)^{c(\gamma_2)+c(\gamma_1,\gamma_2)} = 1.$$

A triplet $\{d_1, d_2, c\}$ with d_1, d_2 independent quadratic discriminants will be called *non-degenerate.* The degenerate triplets are thus those for which $d_i = 1$ for some i or $d_1 = d_2$. In the non degenerate case we shall for fixed d_1, d_2 adopt the notation of § 2.

With each triplet $\{d_1, d_2, c\}$ we associate a multiplicative group $S\{d_1, d_2, c\}$ of non zero rational numbers. We consider separately three cases (i) $\{d_1, d_2, c\}$ is non degenerate; (ii) $\{d_1, d_2, c\}$ is degenerate, $d_1 = d_2 \neq 1$ and $c(\gamma_2) + c(\gamma_1, \gamma_2) \equiv 1 \pmod 2$; (iii) $\{d_1, d_2, c\}$ is degenerate but the other conditions in (ii) are not both satisfied. In all cases $S\{d_1, d_2, c\}$ is generated by its integral elements. It will therefore suffice to give the conditions for an integer a to lie in this group.

B. *Case* (i):

$$\left(\frac{a, d_i}{p}\right) = 1 \text{ *for* } i = 1, 2 \text{ *and for all* } p, \quad (a, f_1^{c(\gamma_2)} f_2^{c(\gamma_1)} f_3^{c(\gamma_3)}) = 1,$$

also $a > 0$ *whenever* $d_1 d_2$ *has a prime divisor* $p \equiv 3 \pmod 4$.

Case (ii):

$$\left(\frac{a, d_1}{p}\right) = 1 \text{ *for all* } p, \; (a, d_1) = 1.$$

Case (iii): *a always lies in* $S\{d_1, d_2, c\}$.

The defining condition in case (i) apart from the sign condition can be restated in the form

B′. (a) *is prime to the relative discriminant* $\mathfrak{d}_c$. *Also* (a) *is norm of some ideal* $\mathfrak{A}$ *in* K, *and for every such* $\mathfrak{A}$, $(K^*/K; \mathfrak{A}) = 1$.

For every triplet $\{d_1, d_2, c\}$ and for all $a \in S(d_1, d_2, c)$ we now define the symbol

$$[d_1, d_2, a]_c$$

as follows. In case (iii)

(3. 1) $$[d_1, d_2, a]_c = 1.$$

In case (ii)

(3. 2) $$[d_1, d_2, a]_c = \left[\frac{a}{d_1}\right]\left[\frac{-1}{d_1}\right]^{(\operatorname{sign} a-1)/2}$$

where we note that by **B** the restricted biquadratic residue symbols $\left[\frac{a}{d_1}\right], \left[\frac{-1}{d_1}\right]$ are defined (cf. [3]).

In the non degenerate case (a) will be ideal norm of K. Also we see that the ideal (a) is integral for and prime to $\mathfrak{d}_c$ so that the symbol $\big(N_{\mathsf{K}/\mathsf{P}}\,\theta_\varphi)\,(a)\big)$ (cf. § 1. (1.8)) is defined for all $\varphi \in \Phi^*(d_1, d_2, c)$. Let $\mathfrak{A}$ be a primitive ideal in K with norm (a). By $\mathbf{B}'$ $(\mathsf{K}^*/\mathsf{K}; \mathfrak{A}) = 1$. If $\varphi, \varphi_1 \in \Phi^*(d_1, d_2, c)$ then $\varphi_1\varphi^{-1} \in \Phi(\mathsf{K}^*/\mathsf{K})$, whence $\theta_{\varphi_1}(\mathfrak{A}) = \theta_\varphi(\mathfrak{A})$. Thus $(N_{\mathsf{K}/\mathsf{P}}\,\theta_\varphi)\big((a)\big)$ solely depends on c and not on the actual choice of φ, and we can write

$$[d_1, d_2, a]_c = (N_{\mathsf{K}/\mathsf{P}}\,\theta_\varphi)\big((a)\big). \tag{3.3}$$

One can extend the definition of the new symbol by writing

$$[b_1^2 d_1, b_2^2 d_2, a]_c = [d_1, d_2, a]_c \tag{3.4}$$

whenever b_1, b_2 are non zero rationals. We may however always restrict our attention to the case $b_1 = b_2 = 1$.

Directly from the definitions we have

Theorem 5 (First Decomposition Theorem). *The domain of values of $[d_1, d_2, a]_c$ is ± 1. — If $\{d_1, d_2, c\}$ is non degenerate, and if $a \in S(d_1, d_2, c)$ then*

$$[d_1, d_2, a]_c = 1$$

if and only if for some (for every) $\varphi \in \Phi^*(d_1, d_2, c)$ and for some (for every) primitive ideal $\mathfrak{A}$ in K with norm (a)

$$(\mathsf{K}_\varphi/\mathsf{K}; \mathfrak{A}) = 1.$$

In particular if a is a prime power then (a) is ideal norm of K_φ if and only if

$$[d_1, d_2, a]_c = 1.$$

In view of this Theorem we shall refer to the symbol $[d_1, d_2, a]_c$ in all cases as the *decomposition symbol*. Together with ordinary quadratic residue symbols it will in the non degenerate case suffice to provide a decomposition criterion in $S(d_1, d_2, c)$ for every normal field of degree 8 containing $\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2})$. We recall that every such field is of form K_φ with $\varphi \in \Phi_{\mathsf{K}}$.

Theorem 6 (Second Decomposition Theorem). *Let d_1, d_2 be independent quadratic discriminants, $\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2})$. To every normal field K_φ $(\varphi \in \Phi_{\mathsf{K}})$ there belongs a triplet $\{d_1, d_2, c\}$ and a rational quadratic residue character χ with conductor $\mathfrak{f}(\chi)$ prime to $d_1 d_2$, and to every triplet $\{d_1, d_2, c\}$ and every such residue character χ there belongs a field K_φ $(\varphi \in \Phi_{\mathsf{K}})$ in the following sense:*

For every prime power $p^r \in S(d_1, d_2, c)$ prime to $\mathfrak{f}(\chi)$, (p^r) is ideal norm of K_φ if and only if

$$\chi(p^r)\,[d_1, d_2, p^r]_c = 1.$$

Proof. Let M be the group of rational idèle class characters μ with $\mu^2 = 1$ of conductor prime to $d_1 d_2$. Every character

$$\varphi = \varphi' R_{K/P}\mu \qquad (\varphi' \in \Phi_K^*, \mu \in M) \tag{3.5}$$

lies in Φ_K, and every character $\varphi \in \Phi_K$ has a representation (3.5) (cf. [4], Theorem 5). The theorem now follows by observing that when p^r satisfies the hypothesis of Theorem 6 then by (1.10)

$$(N_{K/P}\theta_\varphi)((p^r)) = (N_{K/P}\theta_{\varphi'})((p^r))(N_{K/P}\theta_{\varphi''})((p^r)),$$

with $\varphi'' = R_{K/P}\mu$. The first factor on the right is $[d_1, d_2, p^r]_c$ for $c = c_{\varphi'} = c_\varphi$ by Theorem 5. For the second factor we have from the definition of the mappings $N_{K/P}$, $R_{K/P}$ the equation $N_{K/}\ \theta_{\varphi''} = \theta_\mu$, and then by (1.6), $\theta_\mu((p^r)) = = \chi_\mu(p^r)$. Finally we note that every rational quadratic residue character χ of conductor prime to $d_1 d_2$ is of form χ_μ for some $\mu \in M$.

Theorem 7 (First Uniqueness Theorem). *The ordered pair d_1, d_2 together with the character φ determine the class c and the character χ in Theorem 6 uniquely. Two characters $\varphi_1, \varphi_2 \in \Phi_K$ will determine the same class c and the same character χ if and only if $\varphi_1\varphi_2^{-1} \in \Phi(K^*/K)$.*

Proof. The first part follows by the uniqueness of φ' and μ in (3.5) for given $\varphi \in \Phi_K$ (cf. [4] Theorem 5).

For the second part we first note that the prime power ideals $\mathfrak{P}^r$ for which $|N_{K/P}\mathfrak{P}^r|$ lies in $S(d_1, d_2, c)$ are precisely those which split completely in K^*, disregarding powers of factors of $\mathfrak{d}_c$. Two characters φ_1, φ_2 will then determine the same class c and the same character χ if and only if for all such prime powers $\mathfrak{P}^r$, $\theta_{\varphi_1}(\mathfrak{P}^r) = \theta_{\varphi_1}(\mathfrak{P}^r)$ i. e. $\theta_{\varphi_1\varphi_2^{-1}}(\mathfrak{P}^r) = 1$ i. e. $\varphi_1\varphi_2^{-1} \in \in \Phi(K^*/K)$.

From our discussion we also obtain another characterisation of the symbol $[d_1, d_2, a]_c$.

Let $\{d_1, d_2, c\}$ be a non degenerate triplet and let χ be a quadratic residue character of conductor prime to $d_1 d_2$. There exists a unique field $\bar{\Lambda}$ of degree 2 (or 1) over K^*, which is absolutely normal such that

(i) *the prime powers p^r, prime to $\mathfrak{f}(\chi)$, which lie in $S(d_1, d_2, c)$ are precisely those rational prime powers for which (p^r) is ideal norm of K^* and which are prime to the relative discriminant of $\bar{\Lambda}/K^*$;*

(ii) *the prime powers p^r for which in addition $\chi(p^r)[d_1, d_2, p^r]_c = 1$ are precisely those for which (p^r) is an ideal norm of $\bar{\Lambda}$.*

§ 4.

We recall the definition of the isomorphisms g_π: $\Gamma(\mathsf{K}/\mathsf{P})$, and of automorphism π^* in § 2. From equation (2.11) and from the definitions in § 3 we have

Theorem 8 (First Inversion Law). *Let $\pi \in \Sigma$ and let $\{d_1, d_2, c\}$ be non degenerate. Then $\{d_{\pi(1)}, d_{\pi(2)}, \pi^*(c)\}$ is non degenerate and $[d_1, d_2, a]_c = [d_{\pi(1)}, d_{\pi(2)}, a]_{\pi^*(c)}$ where the right hand side is defined whenever the left hand side is.*

Let $\varkappa$ be the permutation (1, 2). Then

$$(4.1) \qquad \varkappa^* c(\gamma_1) = c(\gamma_2), \quad \varkappa^* c(\gamma_2) = c(\gamma_1), \quad \varkappa^* \check{c}(\gamma_1, \gamma_2) = c(\gamma_1, \gamma_2).$$

From Theorem 8 we have thus in particular

$$(4.2) \qquad [d_1, d_2, a]_c = [d_2, d_1, a]_{\varkappa^*(c)}.$$

When $c(\gamma_1) = c(\gamma_2) = 0$, $c(\gamma_1, \gamma_2) = 1$ our symbol can be shown to coincide essentially with that defined by L. Rédei in [9]. In this case $c = \varkappa^*(c)$, and so

$$(4.3) \qquad [d_1, d_2, a]_c = [d_2, d_1, a]_c.$$

This is one of the inversion formulae found by L. Rédei in [9].

On the basis of the first inversion law the uniqueness theorem 7 can now in the non Abelian case be strengthened to

Theorem 9 (Second Uniqueness Theorem). *Let $\{d_1, d_2, c\}$ be a non degenerate triplet with $c(\gamma_1, \gamma_2) = 1$. If χ is a rational quadratic residue character and $\{d_1', d_2', c'\}$ a triplet such that for all primes $p \in S(d_1, d_2, c) \cap \cap S(d_1', d_2', c')$ with $(p, \mathfrak{f}(\chi)) = 1$*

$$\chi(p)\,[d_1', d_2', p]_{c'} = [d_1, d_2, p]_c,$$

then for all such primes p, $\chi(p) = 1$, $\mathfrak{f}(\chi)$ is a divisor of $d_1 d_2$, and $\exists \pi \in \Sigma$ such that $d_i' = d_{\pi(i)}$ $(i = 1, 2)$, $c' = \pi^*(c)$.

Proof. We shall troughout restrict ourselves to primes which are not divisors of $d_1 d_2 d_1' d_2' \mathfrak{f}(\chi)$. We can write $\chi = \chi' \chi''$ where χ', χ'' are quadratic residue characters, $(\mathfrak{f}(\chi'), d_1 d_2) = 1$, $\mathfrak{f}(\chi'') | d_1 d_2$. For the primes in $S(d_1, d_2, c)$, $\chi'(p) = \chi(p)$. We may thus assume already that $(\mathfrak{f}(\chi), d_1 d_2) = 1$.

The primes in $R = S(d_1 d_2, c) \cap S(d_1' d_2', c')$ are precisely those which split (completely) in some Abelian field $\bar{\mathsf{K}}$. Let $\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2})$, $\varphi \in \Phi^*(d_1, d_2, c)$. Then those primes in R for which $[d_1, d_2, p]_c = 1$ are precisely those splitting in $\mathsf{K}_\varphi \bar{\mathsf{K}}$. Note that K_φ and so $\mathsf{K}_\varphi \bar{\mathsf{K}}$ is non Abelian, but normal.

On the other hand the primes in R for which $\chi(p)[d_1', d_2', p]_{c'} = 1$ are those splitting in some normal field $\bar{\Lambda}$. When $\{d_1', d_2', c'\}$ is degenerate this follows directly from the definition, otherwise by Theorem 6. In the degenerate case $\bar{\Lambda}$ will be Abelian.

Assume now the hypothesis of the Theorem to hold. Then $\bar{\Lambda} = \bar{\mathsf{K}}\mathsf{K}_\varphi$. Hence $\bar{\Lambda}$ is non Abelian, and so $\{d_1', d_2', c'\}$ is non degenerate. Let $\mathsf{K}' = \mathsf{P}(\sqrt{d_1'}, \sqrt{d_2'})$ and choose a character $\varphi' \in \Phi_{\mathsf{K}'}$ so that $\mathsf{K}'_{\varphi'}$ belongs to $\{d_1', d_2', c'\}$ and χ in the sense[9]) of Theorem 6. Then $\Lambda = \bar{\mathsf{K}}\mathsf{K}'_{\varphi'} = \bar{\mathsf{K}}\mathsf{K}_\varphi$. Hence in the first place $\mathsf{K}'_{\varphi'}$ is non Abelian and so $c'(\gamma_1, \gamma_2) = 1$. Moreover on inspecting the Galois group $\Gamma(\bar{\Lambda}/\mathsf{P})$ we find that K as the maximal Abelian subfield of K_φ belongs to the centre of $\Gamma(\bar{\Lambda}/\mathsf{P})$; the same is true for K', i. e. $\mathsf{K} = \mathsf{K}'$. On applying a suitable permutation $\pi \in \Sigma$ we may assume that $d_1' = d_1$, $d_2' = d_2$. By the first uniqueness theorem it follows then that $c' = c$ and $\chi = 1$.

Theorem 10 (First Multiplication Law).

With $\{d_1, d_2, c_1\}$, $\{d_1, d_2, c_2\}$ also $\{d_1, d_2, c_1c_2\}$ is a triplet, and

$$[d_1, d_2, a]_{c_1}[d_1, d_2, a]_{c_2} = [d_1, d_2, a]_{c_1 c_2},$$

where all symbols are defined, provided that two of them are defined.

Proof. By the definitions and by Theorem 1.

Theorem 11 (Second Multiplication Law).

$$[d_1, d_2, a]_c[d_1, d_2, b]_c = [d_1, d_2, ab]_c,$$

where all symbols are defined, provided that two of them are defined.

Proof. By the definitions and by (1. 9).

§ 5.

In this section we shall state a number of Theorems, whose proofs are to be given in a second paper.

We consider the quadratic subfield

$$\Omega = \mathsf{P}(\sqrt{d_1}) \tag{5. 1}$$

of the biquadratic field $\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2})$. The generating automorphism of Ω will be denoted by τ. We have

$$\mathsf{K} = \Omega_\mu \tag{5. 2}$$

for a certain idèle class character μ in Ω. The set of characters ψ in Ω

[9]) Note that we may now also assume $(\mathfrak{f}(\chi), d_1'd_2') = 1$.

for which

$$R_{K/\Omega}\psi \in \Phi^*(d_1, d_2, c)$$

will be denoted by $\Psi^*(d_2, c)$.

We shall consider the residue characters in Ω associated with idèle class characters (cf. (1.4)). We write

$$\chi_\mu = \eta. \tag{5.3}$$

For any residue character χ we denote by χ_p the product of its $\mathfrak{p}$-components, $\mathfrak{p}$ running through the prime divisors of p in Ω. Then we have

Theorem 12 (Criterion for Residue Characters). *Let $c \in A(d_1, d_2)$. A residue character χ in Ω will be of form χ_ψ, $\psi \in \Psi^*(d_2, c)$, if and only if*

(i) *for all p: $\chi_p^2 = \eta_p^{c(\gamma_2)}$, $\chi_p^{\tau-1} = \eta_p^{c(\gamma_1, \gamma_2)}$;*

(ii) *for $(p, f_1) = 1$: $\chi_p \neq 1$ if and only if $p | f_2^{c(\gamma_1)} f_3^{c(\gamma_3)}$.*

In the case $c(\gamma_1) = c(\gamma_2) = 0$, $c(\gamma_1, \gamma_2) = 1$ it follows that the characters $\chi_\psi(\psi \in \Psi^*(d_2, c))$ are precisely the quadratic residue symbols whose denominator is a primitive ideal with norm (d_2). From this it follows that for the given value of c our symbol coincides essentially with that of L. Rédei (cf. [9]). Moreover one gets in analogy to L. Rédei's result:

Theorem 13 (Second Inversion Law). *Let $\{d_1, d_2, c\}$, $\{d_1, d, c\}$ be triplets with $c(\gamma_1, \gamma_2) = 1$, $c(\gamma_1) = c(\gamma_2) = 0$. If both decomposition symbols are defined then*

$$[d_1, d_2, d]_c = [d_1, d, d_2]_c t$$

where $t = 1$ unless d_1, d_2, d are all distinct from 1, and either $d_2 < 0$ or $d < 0$. In this latter case we may assume without loss of generality that $d < 0$ and that $\left(\frac{-1, d_i}{p}\right) = 1$ for all p and for $i = 1, 2$. Then

$$t = \left[\frac{-1}{d_1}\right] \text{ if } d_2 = d_1; \quad t = \left[\frac{f_1}{d_1}\right]\left[\frac{f_2}{d_2}\right]\left[\frac{f_3}{d_3}\right]\left[\frac{-1}{f_3}\right]\left(\frac{f_2}{f_3}\right) \text{ if } d_1 \neq d_2.$$

Theorem 14 (Third Multiplication Law). *Let $c(\gamma_1) = 0$. If $\{d_1, d_2, c\}$, $\{d_1, d_2', c\}$, are triples, and if $d_2'' = d_2 d_2'/(d_2, d_2')^2$ then also $\{d_1, d_2'', c\}$ is a triplet, and*

$$[d_1, d_2, a]_c [d_1, d_2', a]_c = [d_1, d_2'', a]_c,$$

where all symbols are defined provided that two of them are defined.

By combining the stated multiplication and inversion laws one can derive further such laws, and in particular a multiplication law for the first argument d_1.

In conclusion we give explicit expressions for the decomposition symbol. For completeness sake we first deal with the case when the fields belonging to the given triplet are Abelian. Throughout all that follows $\{d_1, d_2, c\}$ is a given, non-degenerate triplet.

Theorem 15 (Explicit Form in the Abelian Case). *Let* $c(\gamma_1, \gamma_2) = 0$. *Then*

$$[d_1, d_2, a]_c = \begin{cases} \left[\frac{a}{d_1}\right]\left[\frac{-1}{d_1}\right]^{(\operatorname{sign} a-1)/2} & \text{if} \quad c(\gamma_1) = 1,\ c(\gamma_2) = 0, \\ \left[\frac{a}{d_2}\right]\left[\frac{-1}{d_2}\right]^{(\operatorname{sign} a-1)/2} & \text{if} \quad c(\gamma_1) = 0,\ c(\gamma_2) = 1, \\ \left[\frac{a}{d_3}\right]\left[\frac{-1}{d_3}\right]^{(\operatorname{sign} a-1)/2} & \text{if} \quad c(\gamma_1) = c(\gamma_2) = 1, \\ 1 & \text{if} \quad c(\gamma_1) = c(\gamma_2) = 0. \end{cases}$$

For the non Abelian case we first observe that every element in $S(d_1, d_2, c)$ is the product of elements a^r and p^{2s} of the following types:

(i) a is a square free integer in $S(d_1, d_2, c)$.

(ii) p is a prime, $p \notin S(d_1, d_2, c)$ but $p^2 \in S(d_1, d_2, c)$. By Theorem 11 it will thus suffice to give explicit forms for elements of these two types only.

Theorem 16 (Explicit Form for Prime Squares). *Let* $c(\gamma_1, \gamma_2) = 1$ *and let* p^2 *be of type* (ii).

(a) *If* $(p, d_1 d_2) = 1$ *then*

$$[d_1, d_2, p^2]_c = \begin{cases} \left(\frac{p}{d_i}\right)^{c(\gamma_2)} (i = 2, 3) & \textit{when} \quad \left(\frac{p}{d_1}\right) = 1, \\ \left(\frac{p}{d_i}\right)^{c(\gamma_1)} (i = 1, 3) & \textit{when} \quad \left(\frac{p}{d_2}\right) = 1, \\ \left(\frac{p}{d_i}\right)^{c(\gamma_3)} (i = 1, 2) & \textit{when} \quad \left(\frac{p}{d_3}\right) = 1. \end{cases}$$

(b) *If* $p | d_1 d_2$ *then* $[d_1, d_2; p^2]_c = 1$.

For square free integers we shall use a representation by ternary quadratic forms, which is easily derived from the theory of quadratic fields.

Proposition 5.1. *For every square free integer* a *with* $\left(\frac{a, d_1}{p}\right) = 1$ *for all* p, *there exist rational integers* $2x, 2y, z$ *such that*

(i) $x^2 - y^2 d_1 - z^2 a = 0$,

(ii) $x - y$ *is an integer and* $(2x, 2y, x - y) = 1$,

(iii) $z > 0$, $(z, a d_1 d_2) = 1$ *and* $\left(\frac{z, d_1}{p}\right) = 1$ *for all* $p | z$.

Assume now that $a \in S(d_1, d_2, c)$, $c(\gamma_1, \gamma_2) = 1$. Then we get:

Proposition 5.2. *Let* $p | f_1$. *If* $p^{c(\gamma_2)} \equiv 3 \pmod 4$ *then*

$$\left(\frac{d_1}{p}\right) = -1, \quad (a, p) = 1, \quad \left(\frac{a}{p}\right) = 1. \tag{5.4}$$

If $p^{c(\gamma_2)} \equiv 1 \pmod 4$ *then* $\left(\frac{d_1}{p}\right) = 1$ *so that* $\exists e$ *with*

$$d_1 \equiv e^2 \pmod p. \tag{5.5}$$

Moreover if x, y, z *give a representation of* a *as in Proposition 5.1 then* e *can be chosen so that*

$$(x + ye, p) = 1. \tag{5.6}$$

If $(p, a) = 1$, (5.6) of course will hold for all possible values of (5.5); the existence of a suitable e when $p | a$ follows from a more detailed analysis of the conditions in Proposition 5.1. The remainder of Proposition 5.2 is immediate from the definitions.

Let now $2x, 2y, z$ give a representation of a as in Proposition 5.1 and let $p | f_1$. We define a symbol

$$\left\{\frac{x, y}{p}\right\}_{d_1}.$$

In the second case possible by Proposition 5.2, namely when $\left(\frac{d_1}{p}\right) = 1$, we write

$$\left\{\frac{x, y}{p}\right\}_{d_1} = \left(\frac{x + ye}{p}\right) \tag{5.7}$$

with e satisfying (5.5), (5.6). If $p | a$ then e is uniquely determined mod p. If $p \nmid a$ then $\left(\frac{a}{p}\right) = 1$ and so the value of the right hand side in (5.7) will remain unaltered if e is replaced by $-e$. Thus in all cases the left hand side is not affected by the possible choices of e.

The other possible case is (5.4). Then

$$\left(\frac{x^2 - y^2 d_1}{p}\right) = 1$$

and so there exist integers u, v such that

$$u^2 + v^2 d_1 \equiv x, \quad 2uv \equiv y \pmod p. \tag{5.8}$$

The value of the symbol

$$\left\{\frac{x, y}{p}\right\}_{d_1} = \left(\frac{u^2 - v^2 d_1}{p}\right) \tag{5.9}$$

is then independent of the particular choice of u and v.

We shall write f_1' for the product of the primefactors of f_1 which are $\equiv 1 \pmod 4$. Then we have

Theorem 17 (Explicit Form for Square Free Integers). *Let* $c(\gamma_1, \gamma_2) = 1$ *and let a be a square free integer in* $S(d_1, d_2, c)$. *Then for every representation of a as in Proposition 5.1*

$$[d_1, d_2, a]_c = rs$$

is the product of a "residue factor" r and a "signature factor" s.

The residue factor is given by

$$r = \begin{cases} \left(\dfrac{x}{f_3}\right) \prod\limits_{p|f_1} \left\{\dfrac{x, y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = c(\gamma_2) = 0, \\ \left(\dfrac{x}{f_2}\right) \prod\limits_{p|f_1} \left\{\dfrac{x, y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = 1,\ c(\gamma_2) = 0, \\ \left(\dfrac{z}{d_2}\right) \left[\dfrac{az^2}{f_1'}\right] \prod\limits_{p|f_1} \left\{\dfrac{x, y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = 0,\ c(\gamma_2) = 1, \\ \left(\dfrac{x}{d_1}\right) \left(\dfrac{z}{d_2}\right) \left[\dfrac{az^2}{f_1'}\right] \prod\limits_{p|f_1} \left\{\dfrac{x, y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = c(\gamma_2) = 1. \end{cases}$$

The signature factor is given by

$$s = \left\{ \left[\frac{-1}{d_1}\right]^{c(\gamma_1)} \left[\frac{-1}{d_2}\right]^{c(\gamma_2)} \left[\frac{f_1}{d_1}\right] \left[\frac{f_2}{d_2}\right] \left[\frac{f_3}{d_3}\right] \left[\frac{-1}{f_3}\right] \left(\frac{f_2}{f_3}\right) \right\}^{(\mathrm{sign}\, a-1)/2}$$

when all prime divisors of $d_1 d_2$ are $\equiv 1 \pmod 4$, *by* $s = (-1)^{(\mathrm{sign}\, x-1)/2}$ *when* $d_1 > 0$, $d_2 < 0$, *and by* $s = 1$ *in all other cases.*

An important feature of this theorem is the *invariance of value* of the explicit expressions given for rs; though these involve functions of x, y, z they are in fact quite independent of the particular choice of these parameters. Moreover the inversion laws, and in particular the second inversion law and the special formula (4. 2) arising out of the first inversion law lead now to *reciprocity formulae* for the explicit expressions given in the theorem. Both these phenomena were already noted in a similar context in [3]. Finally the multiplication laws for the decomposition symbol, and in particular Theorem 11 exhibit a multiplicative property of the expressions given in the last theorem. Conversely of course some of the earlier theorems (e. g. Theorem 10) can in turn be derived from Theorem 15—17.

References

[1] C. Chevalley, Théorie du corps de classes, *Annals of Math.*, (2) **41** (1940), 394—418.

[2] A. Fröhlich, On fields of class two, *Proc. London Math. Soc.*, (3) **4** (1954), 235—256.

[3] A. Fröhlich, The restricted biquadratic residue symbol, *Proc. London Math. Soc.*, (3) **9** (1959), 189—207.

[4] A. Fröhlich, The rational characterization of certain sets of relatively Abelian extensions, *Philosophical Transactions Royal Soc. London,* (A) **251** (1959), 385 425.

[5] Y. Furuta, A reciprocity law of the power residue symbol, *Journ. Math. Soc. Japan,* **10** (1958), 46—54.

[6] Y. Furuta, On meta-abelian fields of a certain type, *Nagoya Math. Journal,* **14** (1959), 193 - 199.

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

[8] L. Rédei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *Journal f. d. reine u. angew. Math.,* **171** (1934), 131—148.

[9] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, *Journal f. d. reine u. angew. Math.*, **180** (1939), 1—43.

[10] L. Rédei, Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie, *Acta Math. Acad. Sci. Hung.*, **4** (1953), 1—29.

[11] L. Rédei, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, *Acta Math. Acad. Sci. Hung.*, **4** (1953), 31—87.

KING'S COLLEGE,
LONDON

(Received February 11, 1960)