Redei reciprocity, governing fields and negative Pell

BY PETER STEVENHAGEN

Mathematisch Instituut, Universiteit Leiden,
Postbus 9512, 2300 *RA Leiden, The Netherlands*
e-mail: psh@math.leidenuniv.nl

Abstract

We discuss the origin, an improved definition and the key reciprocity property of the trilinear symbol introduced by Rédei [**16**] in the study of 8-ranks of narrow class groups of quadratic number fields. It can be used to show that such 8-ranks are 'governed' by Frobenius conditions on the primes dividing the discriminant, a fact used in the recent work of A. Smith [**18**, **19**]. In addition, we explain its impact in the progress towards proving my conjectural density for solvability of the negative Pell equation $x^2 - dy^2 = -1$.

2020 Mathematics Subject Classification: Primary 11R11, 11R37; Secondary 11R16.

1. *Introduction*

In a 1939 Crelle paper [**16**], the Hungarian mathematician László Rédei introduced a trilinear quadratic symbol $[a, b, c] \in \{\pm 1\}$ for quadratic discriminants $a, b \in \mathbf{Z}$ and positive squarefree integers c satisfying a number of conditions. He used his symbol to describe 8-ranks of quadratic class groups, much in the way he had described the 4-ranks of these class groups in terms of Legendre symbols in his earlier work [**15**]. His definition of the symbol, as a Jacobi symbol in the quadratic field $\mathbf{Q}(\sqrt{a})$, is somewhat involved, and seems to depend on many choices. Moreover, it only allows for a limited 'symmetry' of the symbol in its arguments, as infinite primes are disregarded in his definition.

An improved definition in class field theoretic terms was proposed in 2007 by Jens Corsman [**5**]. He imposes fewer conditions on the arguments of the symbol, which are most conveniently taken in the group $\mathbf{Q}^*/\mathbf{Q}^{*2}$ of non-zero rational numbers modulo squares, requiring them to have relative quadratic Hilbert symbols

$$(a, b)_p = (a, c)_p = (b, c)_p = 1 \tag{1}$$

at all primes p, and to satisfy the coprimality condition

$$\gcd(\Delta(a), \Delta(b), \Delta(c)) = 1 \tag{2}$$

for the discriminants of the associated quadratic fields, with $\Delta(1) = 1$. The Rédei symbol is then defined as a product $[a, b, c] = \prod_{p|c}[a, b, c]_p$ of 'local' symbols at the primes p dividing the squarefree integer representing c. It is essential to include the infinite prime

$p = \infty$ in the product, with $\infty | c$ having the meaning $c < 0$. A correct definition of $[a, b, c]_p$ leads to a striking feature that we baptise *Rédei's reciprocity law*.

THEOREM 1·1. *For $a, b, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ satisfying* (1) *and* (2)*, the Rédei symbol $[a, b, c]$ is linear in each of its arguments, and satisfies the reciprocity law*

$$[a, b, c] = [b, a, c] = [a, c, b].$$

The Rédei symbol traditionally has its values in $\{\pm 1\}$, as it may be computed as a Jacobi symbol in a quadratic field. Moreover, it has a definition as a product of local symbols that in (48) turn out to be quadratic Hilbert symbols, which invariably have values in $\{\pm 1\}$, and satisfy a *product* formula on which the proof of Theorem 1·1 is based. However, the Rédei symbol is typically used in a linear algebra setting over the field of two elements $\mathbf{F}_2$. It therefore makes sense to take its value in $\mathbf{F}_2$, as we will do in our formal Definition 7·8.

Part of the perfect symmetry of the symbol $[a, b, c]$ in its arguments is immediate from the definition, as $[a, b, c]$ is the Artin symbol depending on c in a cyclic quartic extension $K = \mathbf{Q}(\sqrt{ab}) \subset F_{a,b}$ that depends symmetrically on a and b. Symmetry involving c is a true reciprocity: we may swap b and c in the symbol by a (non-obvious) application of quadratic reciprocity over $\mathbf{Q}(\sqrt{a})$.

The auxiliary field $F_{a,b}$ occurring in the definition of $[a, b, c]$, which is only unique up to twisting by a finite group $T_{a,b}$ of quadratic characters (43), is the most complicated ingredient in the definition. Corsman failed to notice that $K \subset F_{a,b}$ may be ramified over 2, and that one has to require *minimal* ramification at 2 for $K \subset F_{a,b}$ in order for $[a, b, c]$ to be well-defined, independently of the choice of $F_{a,b}$.

In the case of prime arguments $a, b, c \equiv 1 \bmod 4$, no dyadic ramification subtleties arise, and the symbol has been interpreted by Morishita [13, section 8·2] as an arithmetic Milnor invariant, leading to a description as a triple Massey product that is useful in the study of pro-2-extensions of $\mathbf{Q}$ with given ramification locus [8].

Although Galois cohomology does play a role in Corsman's approach to the Rédei symbol, its relation to Massey products and the applications of Rédei reciprocity to the *average* behavior of the 2-part of imaginary quadratic class groups in the recent work of Smith [18, 19], neither the definition of the symbol nor the proof of its symmetry properties needs it, and we do not use it in this paper. Galois cohomology may be needed to find generalisations of the Rédei symbol. In fact, the linearity properties of the symbol make it one of the rare trilinear maps that 'naturally occur' in mathematics, and it is an interesting question whether the symbol has variants having properties of cryptographic interest in the sense of [1].

In this paper we approach Rédei's symbol along historical lines, showing how it arises in the study of the 2-part of the narrow class group C of a quadratic field K of discriminant D. Starting from old results in Section 2 on the 2-rank of C, we describe the 4-rank of C in terms of the *Rédei matrix* $R_4 = R_4(D)$, a matrix over the field $\mathbf{F}_2$ of 2 elements with entries that are essentially $\mathbf{F}_2$-valued relative Legendre symbols of the primes dividing D (Theorem 3·1). Linear algebra also gives the 8-rank of C in terms of a matrix $R_8 = R_8(D)$ over $\mathbf{F}_2$ (Theorem 4·1), but this time its entries are ($\mathbf{F}_2$-valued) *Rédei symbols* $[d_1, d_2, m]$, given in Definition 4·4 as the Artin symbol of an ambiguous ideal in K of norm m in an unramified cyclic quartic extension $K = \mathbf{Q}(\sqrt{d_1 d_2}) \subset F_{d_1, d_2}$ having $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ as its intermediate

quadratic extension. In Section 5, we explicitly compute $[d_1, d_2, m]$ in a field F_{d_1,d_2} obtained by twisting the field $F(x, y, z)$ in (33) associated to a primitive integral point on the conic

$$x^2 - d_1 y^2 - d_2 z^2 = 0$$

by a quadratic character to ensure that $K \subset F_{d_1,d_2}$ is unramified at 2.

Section 6 shows how Rédei's reciprocity law is suggested by the behaviour of small examples, and indicates how the general symbol $[a, b, c]$ should be defined in order to obtain reciprocity. The precise definitions are in Section 7, leading to a proof of Theorem 1·1 in Section 8.

As an immediate application of Rédei reciprocity, Section 9 shows, following Corsman, how it yields the existence of *governing fields* for the 8-rank of class groups in 1-parameter families $\mathbf{Q}(\sqrt{dp})$, with d a fixed integer and p a variable prime, a result that was originally obtained by different means in 1988 in [**20**], and that is at the basis of Smith's work. Section 10 discusses its impact on my now classical Conjecture 3·2 on the number of real quadratic fields with fundamental unit of norm -1 or, equivalently, the asymptotic number of squarefree $d \in \mathbf{Z}_{>1}$ for which the *negative Pell equation*

$$x^2 - dy^2 = -1 \tag{3}$$

is solvable in integers $x, y \in \mathbf{Z}$.

2. *The 2-rank*

Let $d \neq 1$ be a squarefree integer, $K = \mathbf{Q}(\sqrt{d})$ the corresponding quadratic field, $D \in \{d, 4d\}$ the discriminant of K, and $C = \mathrm{Cl}_K^+ = \mathrm{Cl}^+(\mathcal{O}_K)$ the *narrow* class group of K, i.e., the quotient $C = I/P^+$ of the group I of fractional $\mathcal{O}_K$-ideals by the subgroup of principal ideals $(x) = x\mathcal{O}_K$ with generator of *positive* norm $N(x)$. The narrow class group maps surjectively to the ordinary class group Cl_K of K, and we have an exact sequence

$$0 \longrightarrow \langle F_\infty \rangle \longrightarrow C \longrightarrow \mathrm{Cl}_K \to 0 \tag{4}$$

in which F_∞, the *Frobenius at* ∞, denotes the ideal class $[(\sqrt{d})] \in C$. This is the trivial element in C if K is imaginary quadratic, and also if K is real quadratic with fundamental unit ε_d of norm $N(\varepsilon_d) = -1$. If K is real quadratic with $N(\varepsilon_d) = 1$, then F_∞ is of order 2, and C has twice the size of Cl_K.

Describing the 2-part $C[2^\infty] \subset C$ consisting of all 2-power torsion elements in C can be done by specifying, for $k \geq 1$, the 2^k-rank

$$r_{2^k} = r_{2^k}(D) = \dim_{\mathbf{F}_2} C[2^k]/C[2^{k-1}] = \dim_{\mathbf{F}_2} 2^{k-1}C/2^k C.$$

The sequence of non-negative integers $r_2, r_4, r_8, \ldots$ is non-increasing, and we have $r_{2^k} = 0$ for k sufficiently large.

The 2-rank $r_2 = \dim_{\mathbf{F}_2} C[2] = \dim_{\mathbf{F}_2} C/2C$ was already determined by Gauss, who defined C in terms of binary quadratic forms. To state his result, we factor D as a product

$$D = \prod_{i=1}^{t} p_i^* = t_D \prod_{p | D \text{ odd}} p^* \tag{5}$$

of signed odd prime discriminants $p^* = (-1)^{(p-1)/2} p \equiv 1 \bmod 4$ and a discriminantal 2-part $t_D \in \{1, -4, \pm 8\}$ that we sloppily denote by 2^* in case D is even. We let $\mathfrak{p}_i | p_i$ be the prime of K lying over p_i. It satisfies $\mathfrak{p}_i^2 = (p_i)$, so we have $[\mathfrak{p}_i] \in C[2]$.

THEOREM 2·1. *We have $r_2 = t - 1$, with t the number of prime divisors of D.*

Proof. There are two fundamentally different proofs of this result, describing $C[2]$ and $C/2C$, respectively. The first uses the t *ambiguous ideal classes* $[\mathfrak{p}_i] \in C[2]$ coming from the ramifying primes $\mathfrak{p}_i | p_i$ of K, the second the t *genus characters* $\chi_{p_i^*} \in \widehat{C}[2]$ corresponding to the discriminantal divisors p_i^* in (5).

In the first proof, one exploits the Galois action on C of $\mathrm{Gal}(K/\mathbf{Q}) = \langle \sigma \rangle$, noting that σ acts by inversion as the norm map $N = 1 + \sigma$ annihilates C. A little Galois cohomology shows that the 2-torsion subgroup $C[2] = C[\sigma - 1]$ is generated by the t classes $[\mathfrak{p}_i]$, subject to a single relation. This yields $r_2 = t - 1$.

For the second proof, one views $C = \mathrm{Gal}(H/K)$ under the Artin isomorphism as the Galois group over K of the narrow Hilbert class field H of K. Then H is Galois over $\mathbf{Q}$ with dihedral Galois group

$$\mathrm{Gal}(H/\mathbf{Q}) \cong \mathrm{Gal}(H/K) \rtimes \mathrm{Gal}(K/\mathbf{Q}) = C \rtimes \langle \sigma \rangle,$$

as the surjection $\mathrm{Gal}(H/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q}) = \langle \sigma \rangle$ is split and σ acts by inversion. The *genus field* $H_2 \subset H$ of K, which is defined as the maximal subfield of H that is abelian over $\mathbf{Q}$, has as its Galois group over $\mathbf{Q}$ the elementary abelian 2-group

$$\mathrm{Gal}(H_2/\mathbf{Q}) = \mathrm{Gal}(H/\mathbf{Q})^{\mathrm{ab}} = C/2C \times \langle \sigma \rangle. \tag{6}$$

One can generate H_2 explicitly over $\mathbf{Q}$ by t independent square roots as

$$H_2 = \mathbf{Q}(\{\sqrt{p_i^*} : i = 1, 2, \ldots, t\}), \tag{7}$$

so $\mathrm{Gal}(H_2/\mathbf{Q})$ is naturally an $\mathbf{F}_2$-vector space of dimension t, in which the subspace $C/2C = \mathrm{Gal}(H_2/K) \subset \mathrm{Gal}(H_2/\mathbf{Q})$ has dimension $r_2 = t - 1$. □

The second proof of Theorem 2·1 shows that the prime power discriminants $p_i^* | D$ in (5) yield an $\mathbf{F}_2$-basis of the quadratic characters on $\mathrm{Gal}(H_2/\mathbf{Q})$, with

$$\chi_{p_i^*} : \mathrm{Gal}(H_2/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\sqrt{p_i^*})/\mathbf{Q}) \cong \mathbf{F}_2 \tag{8}$$

giving the Galois action on $\sqrt{p_i^*}$. Even though this Galois action is given by multiplication by ± 1, it is convenient for our linear algebra purposes to have *additive* characters with values in $\mathbf{Q}/\mathbf{Z}$, and define the quadratic characters $\chi_{p_i^*}$ with values in $\frac{1}{2}\mathbf{Z}/\mathbf{Z} = \mathbf{F}_2$.

The character $\chi_{d_1} = \sum_{i \in S} \chi_{p_i}$ for a subset $S \subset \{1, 2, \ldots, t\}$ corresponding to the *discriminantal divisor* $d_1 = \prod_{i \in S} p_i^*$ of D gives the action on $\sqrt{d_1}$. When restricted to $C/2C = \mathrm{Gal}(H_2/K) \subset \mathrm{Gal}(H_2/\mathbf{Q})$, it yields a quadratic character in the character group

$$\widehat{C} = \mathrm{Hom}(C, \mathbf{Q}/\mathbf{Z}) \tag{9}$$

of C that coincides with the character χ_{d_2} corresponding to the complementary divisor $d_2 = D/d_1 = \prod_{i \notin S} p_i^*$. Rédei calls an unordered pair (d_1, d_2) of quadratic discriminants satisfying

$$D = d_1 d_2 \tag{10}$$

a *discriminantal decomposition* of D. It 'is' the *genus character* $\chi_{d_1} = \chi_{d_2} \in \widehat{C}[2]$, and the corresponding finitely unramified quadratic extension $K \subset E$ inside H is

$$E = K(\sqrt{d_1}) = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2}) = K(\sqrt{d_2}). \tag{11}$$

3. *The 4-rank and negative Pell*

The ambiguous ideal proof of Theorem 2·1 describes the subgroup $C[2] \subset C$ as a quotient of $\mathbf{F}_2^t$ by a surjection

$$\alpha : \mathbf{F}_2^t \longrightarrow C[2] \tag{12}$$

that sends the jth basis vector to the class $[\mathfrak{p}_j]$. The generator $A_D \in \mathbf{F}_2^t$ of its 1-dimensional kernel encodes the unique non-trivial relation that exists between the t classes of the ramifying primes $\mathfrak{p}_j | D$ of K. In particular, it tells us whether the element $F_\infty = [(\sqrt{d})] \in C[2]$ in (4) is trivial. In the interesting case $D > 0$, this amounts to the fundamental unit of $K = \mathbf{Q}(\sqrt{D})$ having norm $N(\varepsilon_d) = -1$.

The genus theory proof of Theorem 2·1 describes the quotient $C/2C = \mathrm{Gal}(H_2/K)$ of C as a subspace of $\mathrm{Gal}(H/\mathbf{Q}) = \mathbf{F}_2^t$ under the inclusion map

$$\gamma : C/2C = \mathrm{Gal}(H_2/K) \longrightarrow \mathrm{Gal}(H_2/\mathbf{Q}) = \mathbf{F}_2^t, \tag{13}$$

with the ith coordinate of $\gamma(\mathfrak{a}) \in \mathbf{F}_2^t$ for $[\mathfrak{a}] \in C$ describing the action of the Artin symbol $\mathrm{Art}(\mathfrak{a}, H/K) \in \mathrm{Gal}(H/K)$ on $\sqrt{p_i^*}$. As elements of $\mathrm{Gal}(H_2/K)$ fix the product $\prod_{i=1}^t \sqrt{p_i^*} = \sqrt{D}$, the map γ embeds $C/2C$ as the 'sum-zero-hyperplane' in $\mathbf{F}_2^t$. Equivalently, one can formulate this as in (12) by saying that the subgroup $\widehat{C}[2] \subset \widehat{C}$ of quadratic characters on C is generated by the t characters $\chi_{p_i^*}$, subject to the relation that their sum

$$\chi_D = \sum_{i=1}^t \chi_{p_i^*}, \tag{14}$$

the Dirichlet character corresponding to K, is the character on $\mathrm{Gal}(H_2/\mathbf{Q})$ in (6) that has kernel $C/2C$ and is trivial as an element of $\widehat{C}$. This time, the relation holds no deeper information as it is 'the same' for all quadratic fields.

The 4-rank of C is the $\mathbf{F}_2$-dimension of the kernel $C[2] \cap 2C$ of the natural map

$$\varphi_4 : C[2] \longrightarrow C/2C,$$

and we can find it by combining φ_4 with the surjection α and the injection γ from (12) and (13) into a single $\mathbf{F}_2$-linear *Rédei map*

$$R_4 : \quad \mathbf{F}_2^t \xrightarrow{\alpha} C[2] \xrightarrow{\varphi_4} C/2C \xrightarrow{\gamma} \mathrm{Gal}(H_2/\mathbf{Q}) = \mathbf{F}_2^t. \tag{15}$$

We have

$$1 + r_4 = 1 + \dim_{\mathbf{F}_2} \ker \varphi_4 = \dim_{\mathbf{F}_2} \ker R_4 = t - \mathrm{rank}_{\mathbf{F}_2} R_4,$$

and writing $r_2 = t - 1$ as in Theorem 3·1, we obtain the following result.

THEOREM 3·1. *The 4-rank of C equals $r_4 = r_2 - \mathrm{rank}_{\mathbf{F}_2} R_4$.* □

Explicit entries for the matrix $R_4 = (\varepsilon_{ij})_{i,j} \in \text{Mat}_{t \times t}(\mathbf{F}_2)$ can easily be given. The entry ε_{ij} describes the action of the Artin symbol $\text{Art}(\mathfrak{p}_j, H/K)$ on $\sqrt{p_i^*} \in H_2 \subset H$. For $i \neq j$, it is an $\mathbf{F}_2$-valued Legendre (or for $p_j = 2$ Kronecker) symbol:

$$\varepsilon_{ij} = \chi_{p_i^*}([\mathfrak{p}_j]) = \left(\frac{p_i^*}{p_j} \right) \in \mathbf{F}_2. \tag{16}$$

The diagonal entries $\varepsilon_{jj} = \sum_{i \neq j} \varepsilon_{ij}$ of R_4 follow from the sum-zero-property of γ: the rows of R_4 add up to $0 \in \mathbf{F}_2^t$. This simple description of r_4 in terms of the relative quadratic behavior of the primes p_i dividing D goes back to Rédei [15].

The somewhat hybrid notation in (16) uses an identification '$\{\pm 1\} = \mathbf{F}_2$' of multiplicative and additive value groups of quadratic symbols and characters. The same notational ambiguity inevitably occurs for Rédei symbols, which are quadratic symbols in quadratic fields, with values that are traditionally taken in $\{\pm 1\}$, but that also occur as entries of matrices over $\mathbf{F}_2$. We have mostly chosen additive values of characters and symbols in this paper, but multiplicative values are used in the proof of Rédei's reciprocity law in Section 8, which relates Rédei symbols to quadratic Hilbert symbols.

For $K = \mathbf{Q}(\sqrt{d})$ real quadratic of discriminant $D \in \{d, 4d\}$, the fundamental unit has norm $N(\varepsilon_d) = -1$ if and only if the *negative Pell equation*

$$x^2 - dy^2 = -1 \tag{17}$$

is solvable in *integers* x, $y \in \mathbf{Z}$. If it exists, the smallest solution to (17) can be found from the continued fraction expansion of $\sqrt{d}$, which then needs to have *odd* period length, or from general unit finding algorithms in number rings [9]. For $d = D \equiv 5 \bmod 8$, this solution corresponds to the *cube* of ε_d in case the fundamental unit $\varepsilon_d \in \mathcal{O}_K = \mathbf{Z}[(1 + \sqrt{d})/2]$ does not lie in $\mathbf{Z}[\sqrt{d}]$. Conjecturally [22], this happens for a fraction $2/3$ of squarefree $D \equiv 5 \bmod 8$.

For solvability of (17) in *rational numbers*, which amounts to K having elements of norm -1 or, equivalently, having quadratic Hilbert symbols

$$(d, -1)_p = (D, -1)_p = 1 \qquad \text{for all primes } p \leq \infty, \tag{18}$$

there is an easy criterion: solvability occurs if and only if d (or D) is positive and without prime factors $p \equiv 3 \bmod 4$. By [17, Satz 3], the set $\mathcal{D}$ of such D is a thin set, asymptotically containing $cX/\sqrt{\log X}$ elements $D < X$, for some explicit $c \approx .348 \in \mathbf{R}_{>0}$. For $D \in \mathcal{D}$ we have $t_D \in \{1, 8\}$ and $p^* = p$ in (5), and by (7)

$$D \in \mathcal{D} \quad \Longleftrightarrow \quad H_2 \text{ is totally real.} \tag{19}$$

The class field theoretic implication of (4) is that the set $\mathcal{D}^- \subset \mathcal{D}$ of discriminants for which the negative Pell equation (17) is solvable in integers has a similar description:

$$D \in \mathcal{D}^- \quad \Longleftrightarrow \quad H \text{ is totally real.} \tag{20}$$

Indeed, the narrow Hilbert class field H of $K = \mathbf{Q}(\sqrt{d})$ is totally real if and only if the Frobenius at infinity $F_\infty \in C$ at the real primes of $K = \mathbf{Q}(\sqrt{d})$ is trivial on H.

Assume $D \in \mathcal{D}$. Then the map $\alpha : \mathbf{F}_2^t \to C[2]$ in (12) describes $F_\infty = [(\sqrt{d})]$ as

$$F_\infty = \alpha[(1)_{i=1}^t] \in C[2] \cap 2C,$$

and $V = \alpha^{-1}(C[2] \cap 2C) \subset \mathbf{F}_2^t$ is an $(r_4 + 1)$-dimensional subspace containing $(1)_{i=1}^t$. The linear map $\alpha|_V : V \to C[2] \cap 2C$ is surjective with kernel $\mathbf{F}_2 \cdot A_D$, and numerical evidence [2] suggests that A_D behaves like a 'random' non-zero element in V. As $D \in \mathcal{D}$ satisfies

$$D \in \mathcal{D}^- \iff A_D = (1)_{i=1}^t,$$

we expect that for the discriminants $D \in \mathcal{D}$ having 4-rank $r_4 = e$, the negative Pell equation (17) will be solvable with 'probability' $(\#V - 1)^{-1} = (2^{r_4+1} - 1)^{-1}$.

To heuristically find the density for $\mathcal{D}^-$ in $\mathcal{D}$, write $\mathcal{D} = \bigcup_{e=0}^{\infty} \mathcal{D}(e)$, with $\mathcal{D}(e)$ the subset of $D \in \mathcal{D}$ having 4-rank $r_4 = e$. By Theorem 3·1, a discriminant $D \in \mathcal{D}$ is in $\mathcal{D}(e)$ if and only if its Rédei matrix $R_4 \in \text{Mat}_t(\mathbf{F}_2)$ has corank $e + 1$. Quadratic reciprocity for the entries (16) implies that the matrix R_4 is *symmetric*, with rows and columns adding up to 0. The $(1, 1)$-minor of R_4, which determines the full matrix R_4, behaves as a random symmetric $(t - 1) \times (t - 1)$-matrix. As the average number t of primes factors of D tends to infinity with D, albeit very slowly, as $\log \log D$, we expect the density of $\mathcal{D}(e)$ in $\mathcal{D}$ to equal $P(e) = \lim_{n \to \infty} P_n(e)$, with $P_n(e)$ the fraction of the $\binom{n+1}{2}$ symmetric $n \times n$-matrices over $\mathbf{F}_2$ having corank e. In terms of the infinite product

$$\alpha = \prod_{j \text{ odd}} (1 - 2^{-j}) = \prod_{j=1}^{\infty} (1 + 2^{-j})^{-1} \approx .419422441, \qquad (21)$$

we have $P(0) = \alpha$, and more generally $P(e) = \alpha \cdot \prod_{j=1}^e (2^j - 1)^{-1}$ for $e \geq 0$.

By the probability argument above, we expect the natural density of $\mathcal{D}^-(e)$ in $\mathcal{D}(e)$ to be $1/(2^{e+1} - 1)$ for all $e \in \mathbf{Z}_{\geq 0}$. This leads to my 1992 conjecture for the solvability of the negative Pell equation [21].

CONJECTURE 3·2. *The set $\mathcal{D}^-$ of discriminants of quadratic fields with fundamental unit of norm -1 has natural density*

$$\sum_{e=0}^{\infty} \frac{P(e)}{2^{e+1} - 1} = 1 - \alpha \approx .580577559$$

inside the set $\mathcal{D}$ of discriminants of quadratic fields containing elements of norm -1.

Fouvry and Klüners proved in 2010 [6] that $\mathcal{D}(e)$ does indeed have the expected density $P(e)$ in $\mathcal{D}$. For $e = 0$ we have $2^{e+1} - 1 = 1$ and $\mathcal{D}(0) \subset \mathcal{D}^-$, as in the case $r_4 = 0$ the narrow Hilbert class field H is totally real, being a normal number field of *odd* degree over the totally real genus field H_2. This immediately implies that $P(0) = \alpha$ is a lower bound for the lower density of $\mathcal{D}^-$ in $\mathcal{D}$. To get better bounds, one needs control over the archimedean character of H for $e \geq 1$. We will address this in Section 10.

4. *The 8-rank*

The 8-rank r_8 of C equals the $\mathbf{F}_2$-dimension of the kernel of the natural map

$$\varphi_8 : C[2] \cap 2C \longrightarrow 2C/4C$$

between r_4-dimensional vector spaces over $\mathbf{F}_2$. Under the Artin isomorphism, the group $2C/4C$ is the Galois group $\text{Gal}(H_4/H_2)$, with $H_4 \subset H$ the narrow 4-Hilbert class field of K.

We can restrict α in (12) to the kernel of the 4-rank map R_4 from (15) and compose with φ_8 to obtain an $\mathbf{F}_2$-linear map

$$R_8: \quad \ker R_4 \xrightarrow{\alpha} C[2] \cap 2C \xrightarrow{\varphi_8} 2C/4C = \mathrm{Gal}(H_4/H_2) \cong \mathbf{F}_2^{r_4} \tag{22}$$

defined on the $(r_4 + 1)$-dimensional space $\ker R_4$. Here we write $\mathrm{Gal}(H_4/H_2) \cong \mathbf{F}_2^{r_4}$, in contrast to the equality $\mathrm{Gal}(H_2/\mathbf{Q}) = \mathbf{F}_2^t$ in (15), as we no longer have an obvious choice for the basis of this $\mathbf{F}_2$-vector space. As $r_8 = \dim_{\mathbf{F}_2} \ker \varphi_8$ is the codimension of the image of φ_8 in $2C/4C$, we obtain the following analogue of Theorem 3·1.

THEOREM 4·1. *The 8-rank of C equals $r_8 = r_4 - \mathrm{rank}_{\mathbf{F}_2} R_8$.* $\qquad\square$

In order to obtain a matrix representing R_8, we want to represent $\mathrm{Gal}(H_4/H_2)$ in (22) as explicitly as we represented $\mathrm{Gal}(H_2/\mathbf{Q})$ in (15). Rédei had already achieved this in a 1934 paper with Reichardt [14], which computed r_4 not as in Theorem 3·1 but by an explicit construction of $H_2 \subset H_4$ in terms of r_4 cyclic quartic extensions $K \subset F$ inside H that are K-linearly disjoint. For such unramified F, the group $\mathrm{Gal}(F/\mathbf{Q})$ is dihedral of order 8, and the intersection $E = F \cap H_2$ equals $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ for a discriminantal decomposition $D = d_1 d_2$ as in (10) and (11).

Rédei calls the decompositions $D = d_1 d_2$ defining those $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ that arise as $F \cap H_2$ *zweiter Art*, 'of the second kind'. For the corresponding quadratic character $\chi \in \widehat{C} = \mathrm{Hom}(C, \mathbf{Q}/\mathbf{Z})$, it means that we have $\chi = 2\psi$ for a quartic character ψ defining $K \subset F$. By the duality of finite abelian groups, we have $\chi \in 2\widehat{C}$ if and only if χ vanishes on the 2-torsion subgroup $C[2]$. This leads to the following characterization of these quadratic characters.

LEMMA 4·2. *For a quadratic character $\chi \in \widehat{C}[2]$ defining $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ as in (10) and (11), having $\chi \in 2\widehat{C}$ is equivalent to each of the following*:

(i) *there exists a cyclic quartic extension $K \subset F$ inside H containing E;*
(ii) $\chi_{d_1} \circ R_4 = \chi_{d_2} \circ R_4$ *is the zero map;*
(iii) *all ramified primes of K split completely in $K \subset E$;*
(iv) *for $i = 1, 2$ and $p | d_i$ prime we have $\left(\frac{D/d_i}{p}\right) = 1$.*

Proof. Having $\chi = 2\psi$ for a quartic character $\psi \in \widehat{C}$ defining F as in (i) is equivalent to χ vanishing on the subgroup $C[2]$ of ambiguous ideal classes generated by the classes of the ramifying primes $\mathfrak{p} | D = d_1 d_2$ of K as in (12). One can phrase this using the map R_4 from (15) as in (ii), or in terms of the splitting of the ramifying primes in $K \subset E$ as in (iii). A ramifying prime of K divides exactly one of d_1, d_2. A prime $\mathfrak{p} | p$ in K dividing, say, d_1 splits completely in $K \subset E = K(\sqrt{d_2})$ if and only if the Legendre (or Kronecker) symbol $\left(\frac{d_2}{p}\right)$ equals 1, as in (iv). $\qquad\square$

Remark 4·3. The identity $\chi = 2\psi$ determines $\psi \in \widehat{C}$ up to a quadratic character, as an element of $\widehat{C}[4]/\widehat{C}[2]$, and this means that the quadratic extension $E \subset F$ it gives rise to in (i) is determined by χ only up to 'twisting' by an unramified quadratic character. In other words: not $E \subset F$, but the quadratic extension $H_2 \subset H_2 F$ it generates over the genus field H_2 is unique.

In order to compute the 8-rank in Theorem 4·1 from the rank of an explicit matrix describing the map R_8 in (22), we *choose* an $\mathbf{F}_2$-basis for the $(r_4 + 1)$-dimensional subspace $\ker R_4 \subset \mathbf{F}_2^t$, and write

$$[\mathfrak{m}_j] \in C[2] \cap 2C \qquad (j = 1, 2, \ldots, r_4 + 1)$$

for the images of these basis vectors under the map α from (12). The classes $[\mathfrak{m}_j]$ span $C[2] \cap 2C$, subject to a single relation encoded in A_D, and their Artin symbols $\mathrm{Art}(\mathfrak{m}_j, H/K)$ are the identity on the genus field H_2.

Similarly, we *choose* quartic characters ψ_i for $i = 1, 2, \ldots, r_4$ spanning $\widehat{C}[4]/\widehat{C}[2]$, and let $K \subset F_{4,i}$ be the corresponding unramified quartic extensions. By condition (ii) of Lemma 4·2, the quadratic characters $\chi_i = 2\psi_i \in \widehat{C}[2]$ come from vectors in $\mathbf{F}_2^t$ that, together with $(1)_{i=1}^t$, span the kernel of the *transpose* R_4^T of the Rédei matrix in (15). The r_4 quadratic extensions $H_2 \subset H_2 F_{4,i}$ span $H_2 \subset H_4$, and the map R_8 is represented by a matrix $R_8 = (\eta_{ij})_{i,j} \in \mathrm{Mat}_{r_4 \times (r_4+1)}(\mathbf{F}_2)$ with entries

$$\eta_{ij} = \psi_i[\mathfrak{m}_j] = \mathrm{Art}(\mathfrak{m}_j, H_2 F_{4,i}/K) \in \mathrm{Gal}(H_2 F_{4,i}/H_2) = \mathbf{F}_2 . \qquad (23)$$

In cases where we know the kernel of α in (12), i.e., the non-trivial relation A_D between the ramified primes of K in C, we can use it to leave out a column of R_8 corresponding to a 'superfluous' generator $[\mathfrak{m}_j]$ of $C[2] \cap 2C$, and work with an $(r_4 \times r_4)$-matrix to describe φ_8 in (22).

A product $\mathfrak{m}$ of distinct ramified primes of K is characterized by the squarefree divisor $m | D$ arising as its norm, and the residue class of a quartic character ψ in $\widehat{C}[4]/\widehat{C}[2]$ by the invariant field $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ of the quadratic character 2ψ corresponding to a decomposition $D = d_1 d_2$ 'of the second kind'. This leads to a classical notation for the entries $\psi([\mathfrak{m}])$ in (23) as *Rédei symbols*.

Definition 4·4. Let $D = d_1 d_2$ be a decomposition of the second kind, $K \subset F$ a corresponding extension as in condition (i) of Lemma 4·2, and $m | D$ the squarefree norm of an integral ideal $\mathfrak{m}$ in K with $[\mathfrak{m}] \in C[2] \cap 2C$. Then the Rédei symbol associated to d_1, d_2, and m is the Artin symbol

$$[d_1, d_2, m] = \mathrm{Art}(\mathfrak{m}, H_2 F/K) \in \mathrm{Gal}(H_2 F/H_2) = \mathbf{F}_2 .$$

It is convenient to take the value of Rédei symbols in $\mathbf{F}_2$, as we do in Definition 4·4. After all, they arise as entries η_{ij} of an $\mathbf{F}_2$-matrix R_8 in (23). However, they describe the Galois action on certain square roots, just like the entries ε_{ij} of R_4 in (16), so their values are traditionally taken in $\{\pm 1\}$. We have been unable to completely avoid this notational ambiguity, which already occurs in (16). Despite our additive definition, our proof of Rédei reciprocity in Section 8 views Rédei symbols in (46) as 'products' of local symbols $[a, b, c]_p$, which are recognised in our key Lemma 8·1 as quadratic Hilbert symbols satisfying a well-known global *product formula* that we did not rename into a sum formula. On the other hand, our quadratic characters in (8) and biquadratic characters in (38) do take values in $\mathbf{F}_2$.

5. *Computing Redei-symbols*

Definition 4·4 of the Rédei symbol $[d_1, d_2, m]$ does not immediately show how to compute it from d_1, d_2 and m, as it involves a quadratic extension F of $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ that is

dihedral over $\mathbf{Q}$. Galois theory tells us that such F come from rational points on the conic $x^2 - d_1 y^2 - d_2 z^2 = 0$, and that they are unique up to twisting by quadratic characters. This statement does not depend on the base field $\mathbf{Q}$, and we formulate it for any field Q of characteristic different from 2.

LEMMA 5·1. *Let Q be of characteristic different from 2, and $Q \subset Q(\sqrt{a})$ a quadratic extension. For $\beta \in Q(\sqrt{a})^*$ non-square of norm $N\beta = b \in Q^*$, let F be the normal closure of the quartic extension $Q(\sqrt{a}, \sqrt{\beta})$ of Q. Then*:

   (i) *for $\overline{b} \notin \{\overline{1}, \overline{a}\} \subset Q^*/Q^{*2}$, the field F is quadratic over $Q(\sqrt{a}, \sqrt{b})$, cyclic of degree 4 over $Q(\sqrt{ab})$, and dihedral of degree 8 over Q;*

  (ii) *for $\overline{b} = \overline{a} \in Q^*/Q^{*2}$, the field F is quadratic over $Q(\sqrt{a})$ and cyclic of degree 4 over Q;*

 (iii) *for $\overline{b} = \overline{1} \in Q^*/Q^{*2}$, the field F is quadratic over $Q(\sqrt{a})$ and non-cyclic abelian of degree 4 over Q.*

Conversely, every field F having the properties in (i), (ii) or (iii) is obtained in this way for some $\beta \in Q(\sqrt{a})$ of norm b.

Proof. Basic Galois theory.   □

COROLLARY 5·2. *Let $a, b \in Q^*$ and $E = Q(\sqrt{a}, \sqrt{b})$ be as in (i) of Lemma 5·1. Then a quadratic extension $E \subset F$ is cyclic over $Q(\sqrt{ab})$ and dihedral of degree 8 over Q if and only if there exists a non-zero solution $(x, y, z) \in Q^3$ to the equation*

$$x^2 - ay^2 - bz^2 = 0$$

such that for $\beta = x + y\sqrt{a} \in Q(\sqrt{a})$ and $\alpha = 2(x + z\sqrt{b}) \in Q(\sqrt{b})$ of norm $\beta\beta' \in b \cdot Q^{*2}$ and $\alpha\alpha' \in a \cdot Q^{*2}$, we have

$$F = E(\sqrt{\beta}) = E(\sqrt{\alpha}).$$

Given $F = E(\sqrt{\beta})$, any other quadratic extension of E that is dihedral over Q is of the form $F_t = E(\sqrt{t\beta})$ for some unique $t \in Q^*/\langle a, b, Q^{*2} \rangle$.

Proof. The first statement follows if we write $\beta = x + y\sqrt{a} \in Q(\sqrt{a})$ in the dihedral case (i) of Lemma 5·1, and observe that $F = Q(\sqrt{a}, \sqrt{\beta}, \sqrt{\beta'}) = E(\sqrt{\beta})$ is the normal closure over Q of $Q(\sqrt{a}, \sqrt{\beta})$, but also of $Q(\sqrt{b}, \sqrt{\alpha})$: it contains a square root of the non-square element

$$(\sqrt{\beta} + \sqrt{\beta'})^2 = \left(\sqrt{x + y\sqrt{a}} + \sqrt{x - y\sqrt{a}} \right)^2 = 2(x + z\sqrt{b}) = \alpha \in \mathbf{Q}(\sqrt{b})^*. \qquad (24)$$

The dihedral group D_4 of order 8 has center $Z(D_4) = \mathbf{F}_2$ with quotient $D_4/Z(D_4) = \mathbf{F}_2 \times \mathbf{F}_2$, and extending $Q \subset Q(\sqrt{a}, \sqrt{b})$ to a D_4-extension amounts to lifting the surjection $G_Q \to \mathbf{F}_2 \times \mathbf{F}_2 = D_4/Z(D_4)$ on the absolute Galois group of Q corresponding to $Q(\sqrt{a}, \sqrt{b})$ to a homomorphism $f : G_Q \to D_4$. Given f corresponding to $F = E(\sqrt{\beta})$, any other lift is of the form $f_t = \chi_t f$ for some quadratic character $\chi_t : G_Q \to Z(D_4) = \mathbf{F}_2$ corresponding to $Q \subset Q(\sqrt{t})$. The extension F_t corresponding to f_t is the *quadratic twist* $F_t = E(\sqrt{t\beta})$ of F, and $t \in Q^*$ yielding F_t is unique up to multiplication by elements of $E^{*2} \cap Q^* = \langle a, b, Q^{*2} \rangle$.   □

COROLLARY 5·3. *For $E = Q(\sqrt{a})$ as in Lemma* 5·1, *a quadratic extension $E \subset F$ is cyclic over Q if and only if there exists a non-zero solution $(x, y, z) \in Q^3$ to*

$$x^2 - ay^2 - az^2 = 0$$

such that we have $F = E(\sqrt{\alpha})$ for $\alpha = x + y\sqrt{a} \in Q(\sqrt{a})$ of norm $\alpha\alpha' \in a \cdot Q^{*2}$. Given one $F = E(\sqrt{\alpha})$, any other such extension is of the form $F_t = E(\sqrt{t\alpha})$ for some unique $t \in Q^*/\langle a, Q^{*2}\rangle$.

Proof. Analogous to the dihedral case. $\qquad\square$

Remark 5·4. The dihedral group D_4 of order 8 can be viewed as the Heisenberg group $U_3(\mathbf{F}_2)$ of upper triangular 3×3-matrices with coefficients in $\mathbf{F}_2$, and extending an extension $Q \subset Q(\sqrt{a}, \sqrt{b})$ to a D_4-extension amounts to an embedding problem that can be treated in terms of Massey symbols [12]. For our purposes, the basic Galois theory of Lemma 5·1 and its corollaries are already sufficient.

In order to construct an unramified extension $K \subset F$ containing $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ for $D = d_1 d_2$ satisfying the conditions of Lemma 4·2, we apply Corollary 5·2 for $Q = \mathbf{Q}$ and $(a, b) = (d_1, d_2)$. It shows that F can be explicitly generated as

$$F = F(x, y, z) = E(\sqrt{\delta_2}) = E(\sqrt{\delta_1}), \tag{25}$$

for elements $\delta_2 = x + y\sqrt{d_1} \in \mathbf{Q}(\sqrt{d_1})^*$ and $\delta_1 = 2(x + y\sqrt{d_1}) \in \mathbf{Q}(\sqrt{d_1})^*$ coming from a solution (x, y, z) to the equation

$$x^2 - d_1 y^2 - d_2 z^2 = 0. \tag{26}$$

By Corollary 5·2, scaling *any* non-zero solution (x, y, z) with an appropriate element $t \in \mathbf{Q}^*$, which amounts to replacing $F(x, y, z)$ by the *quadratic twist* $F(tx, ty, tz)$, will make $K \subset F$ unramified. As we will show in a slightly more general setting in Corollary 7·4, every *primitive* integral solution (x, y, z) to (26) yields an extension $K \subset F(x, y, z)$ that is unramified at all odd primes. Ramification over 2 can be avoided by twisting the extension with a suitable choice of $t \in \{\pm 1, \pm 2\}$.

Example 5·5. Take $K = \mathbf{Q}(\sqrt{-205})$ of discriminant $D = -4 \cdot 5 \cdot 41 = -820$, which has $t = 3$ and $r_2 = 2$. The columns of the Rédei matrix

$$R_4 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

describe the action of the Artin symbols of the three ramified primes $\mathfrak{p}_2$, $\mathfrak{p}_5$, and $\mathfrak{p}_{41}$ dividing D on the square roots of -4, 5 and 41 generating $H_2 = \mathbf{Q}(i, \sqrt{5}, \sqrt{41})$ as in (16). From the matrix R_4 we read off that r_4 equals $r_2 - \text{rank}(R_4) = 1$, that $[\mathfrak{p}_5]$ and $[\mathfrak{p}_{41}]$ span $C[2] \cap 2C$, and that $D = -20 \cdot 41$ is the unique decomposition of the second kind. The equation

$$x^2 + 20y^2 - 41z^2 = 0$$

has a primitive solution $(12,1,2)$ for which the element $\delta = 12 + 2\sqrt{-5}$ of norm $2^2 \cdot 41$ is 'primitive outside 2' and satisfies $\delta \equiv (1 + \sqrt{-5})^2 \bmod 4$. This shows that $\delta = 2(6 + \sqrt{-5})$

has an unramified square root over $E = \mathbf{Q}(\sqrt{-5}, \sqrt{41})$, whereas the primitive elements $\pm 6 + \sqrt{-5}$ yield extensions $E \subset E(\sqrt{\pm\delta/2})$ that are ramified over 2.

The solution $(17, 2, 3)$ defining the primitive element $\delta_0 = 17 + 4\sqrt{-5}$ of norm $3^2 \cdot 41$ satisfying $\delta_0 \equiv 1 \bmod 4$ also has an unramified square root over E. We have

$$\delta\delta_0 = 164 + 82\sqrt{-5} = -[\sqrt{41}(1 - \sqrt{-5})]^2 \in -1 \cdot E^{*2},$$

and $E(\sqrt{\delta_0}) = E(\sqrt{t\delta})$ for $t = -1$. Over H_2, both $\sqrt{\delta_0}$ and $\sqrt{\delta}$ generate

$$H_4 = H_2(\sqrt{\delta_0}) = H_2(\sqrt{\delta}).$$

As we know that $(\sqrt{-5 \cdot 41}) = \mathfrak{p}_5\mathfrak{p}_{41}$ is trivial in C, the class of either $\mathfrak{p}_5$ or $\mathfrak{p}_{41}$ generates $C[2] \cap 2C$. The matrix R_8 consists of a single Rédei symbol

$$[-20, 41, 5] = [-20, 41, 41]$$

describing whether the prime $\mathfrak{p}_5$ (or, equivalently, $\mathfrak{p}_{41}$) of K splits completely in H_4. It does not, as $\delta = 12 + 2\sqrt{-5}$ (like $\delta_0 = 17 + 4\sqrt{-5}$)) is congruent to the quadratic non-residue 2 modulo every prime over 5 in H_2. We conclude that we have $r_8 = 0$, and that the 2-part of C is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

In this case, the decomposition $D = d_1 d_2 = -4 \cdot 205$ is not of the second kind, but the conic

$$x^2 + 4y^2 - 205z^2 = 0$$

defined by (26) does have infinitely many rational points (x, y, z), such as $(3, 7, 1)$. None of them defines an unramified quartic extension $K \subset F(x, y, z)$.

Example 5·5 shows that non-trivial solvability of (26) over $\mathbf{Q}$ may not guarantee the existence of unramified extensions $K \subset F(x, y, z)$, whereas the slightly stronger conditions of Lemma 4·2 do. More precisely, by the classical *local-global principle* for conics, assuming solvability of (26) amounts to having quadratic Hilbert symbols $(d_1, d_2)_p = 1$ for all finite primes p, with $(d_1, d_2)_\infty = 1$ then being implied by the product formula. At $p \nmid D = d_1 d_2$, including $p = 2$, we have $(d_1, d_2)_p = 1$. For an *odd* prime p dividing $D = d_1 d_2$, say d_1, the Hilbert symbol condition at p is

$$(d_1, d_2)_p = \left(\frac{d_2}{p}\right) = 1,$$

exactly as in condition (iv) of Lemma 4·2. For $p = 2$ dividing d_1 however, we have $d_2 \equiv 1 \bmod 4$ and obtain

$$(d_1, d_2)_2 = \left(\frac{d_2}{2}\right)^{\mathrm{ord}_2(d_1)} = 1. \tag{27}$$

If D has 2-part $t_D = -4$ in (5) and we have $d_2 \equiv 5 \bmod 8$, such as for $D = -820$ and $d_2 = 205$ above, condition (27) does *not* imply condition (iv) of Lemma 4·2 for $p = 2$, as we have $(d_1, d_2)_2 = 1$ but $(d_2/2) = -1$. This discrepancy will lead us to the notion of 2-minimal ramification in Definition 7·5.

6. *Discovering Redei reciprocity*

Explicit computations of Rédei symbols exhibit a 'reciprocity law' that we can discover already by looking at the most classical example

$$K = \mathbf{Q}(\sqrt{-p}),$$

with p an odd prime. Having $r_2 = t - 1 = 1$ for K amounts to having $p \equiv 1 \bmod 4$ and $D = -4p$ by Theorem 2·1; otherwise C has odd order. Assuming this, R_4 in Theorem 3·1 has rank 0 if and only if we have $(\frac{p}{2}) = (\frac{2}{p}) = 1$, so $r_4 = 1$ happens for $p \equiv 1 \bmod 8$. We further assume $p \equiv 1 \bmod 8$.

As $(\sqrt{-p})|p$ is principal, the class of the non-principal prime $\mathfrak{p}_2|2$ generates $C[2] = C[2] \cap 2C$, and R_8 consists of a single Rédei symbol $[-4, p, 2]$. The case $r_8 = 1$ in which the symbol vanishes occurs when the prime $\mathfrak{p}_2$ of K splits completely in the 4-Hilbert class field $H_4(-p)$ of K. Solving

$$x^2 + 4y^2 - pz^2 = 0$$

with $z = 1$, we can generate $H_4(-p)$ over $E = \mathbf{Q}(i, \sqrt{p})$ by adjoining a square root of $\pi = x + 2iy$. Now $\mathfrak{p}_2$ splits into 4 primes in the extension $K \subset H_4(-p)$ if and only if the prime $(1 + i)$ over 2 in $\mathbf{Q}(i)$ splits into 4 primes in the extension

$$\mathbf{Q}(i) \subset H_4(-p) = \mathbf{Q}(\sqrt{-p}, i, \sqrt{\pi}) = \mathbf{Q}(i, \sqrt{\pi}, \sqrt{\bar{\pi}}).$$

This shows that $[-4, p, 2]$ can be viewed as a 'Kronecker symbol' $(\frac{\pi}{1+i})$ in $\mathbf{Q}(i)$. By class field theory (or quadratic reciprocity) over $\mathbf{Q}(i)$, this symbol is simply the Legendre symbol $(\frac{1+i}{p})$, which is well defined for $p \equiv 1 \bmod 8$, and we have

$$r_8 = 1 \quad \Longleftrightarrow \quad p \text{ splits completely in } \mathbf{Q}(\zeta_8, \sqrt{1+i}). \tag{28}$$

We deduce that the prime $\mathfrak{p}_2$ over 2 splits completely in the unramified extension $K \subset H_4(-p)$ if and only if p splits completely in $\mathbf{Q}(\zeta_8, \sqrt{1+i})$. By the case $(a, b) = (-1, 2)$ of Lemma 5·1, the field $\mathbf{Q}(\zeta_8, \sqrt{1+i}) = \mathbf{Q}(i, \sqrt{2}, \sqrt{1+i})$ is dihedral over $\mathbf{Q}$, just like $H_4(-p)$. In fact, both fields are abelian of exponent 2 over $\mathbf{Q}(i)$, quadratic over respectively $\mathbf{Q}(i, \sqrt{2})$ and $\mathbf{Q}(i, \sqrt{p})$, and cyclic over respectively $\mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{-p})$. We have proved a special case of *Rédei reciprocity*, and in terms of Rédei symbols it can be suggestively formulated as

$$[-4, p, 2] = [-4, 2, p]. \tag{29}$$

The symbol on the left is defined by Definition 4·4 for symbols $[d_1, d_2, m]$, but the symbol on the right is not. It is natural to take d_1 and d_2 up to squares, yielding the formulation $[-1, p, 2] = [-1, 2, p]$, but the symbol $[-1, 2, p]$ refers to the splitting of the primes over p in

$$\mathbf{Q}(\sqrt{-2}) \subset E = \mathbf{Q}(i, \sqrt{2}) \subset F = E(\sqrt{1+i}),$$

a cyclic quartic extension that is totally ramified over 2. Primes $p \equiv 1 \bmod 8$ are totally split in E, and split or inert in $E \subset F$ depending on the value of $[-1, 2, p]$.

As we can swap the arguments -1 and p in the symbol $[-1, p, 2]$ by its very definition, and 2 and p by what we just proved, one naturally wonders whether it also equals a symbol $[2, p, -1]$ that describes the splitting of "-1" in the narrow 4-Hilbert class field

$H_4(2p)$ of $\mathbf{Q}(\sqrt{2p})$. By Theorem 3·1, the field $H_4(2p)$ is quadratic over the totally real field $\mathbf{Q}(\sqrt{2}, \sqrt{p})$ for $p \equiv 1 \bmod 8$. Now Frobenius symbols at "-1", which over $\mathbf{Q}$ raise roots of unity to the power -1, arise in class field theory as complex conjugations, and act trivially on totally real fields. The dihedral field $H_4(2p)$ is abelian of exponent 2 over $\mathbf{Q}(\sqrt{2})$, and it is totally real if and only if its conductor over $\mathbf{Q}(\sqrt{2})$ is p, not $p \cdot \infty$. Looking at the ray class group

$$(\mathbf{Z}[\sqrt{2}]/p\mathbf{Z}[\sqrt{2}])^* / \langle -1, 1 + \sqrt{2} \rangle$$

modulo p of $\mathbf{Q}(\sqrt{2})$, we see that $H_4(2p)$ is real exactly when the fundamental unit $1 + \sqrt{2} \in \mathbf{Q}(\sqrt{2})$ is a square modulo p, and this happens for the primes that split completely in the dihedral field $\mathbf{Q}(\zeta_8, \sqrt{1 + \sqrt{2}})$. By equation (24) for $(a, b) = (-1, 2)$ and $(x, y, z) = (1, 1, 1)$, this is the *same* field as $\mathbf{Q}(\zeta_8, \sqrt{1 + i})$, so the Rédei symbol

$$[-1, p, 2] = [-1, 2, p] = [2, p, -1], \tag{30}$$

when properly defined, is invariant under *all permutations* of its arguments.

In Rédei's own definition, $[-1, 2, p]$ does not exist, and $[p, 2, -1]$ is trivial for all p. Our definition in the next section introduces a notion of *minimal ramification* for extensions $K \subset F$ as in (25), correcting the definition found in [5].

7. *Redei symbols*

In order to obtain Rédei reciprocity, we generalize the symbol $[d_1, d_2, m]$ in Definition 4·4 beyond the setting of dihedral fields F containing $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ that are cyclic and unramified over $K = \mathbf{Q}(\sqrt{d_1 d_2})$ and norms m of ambiguous ideals $\mathfrak{m}$ of K with trivial Artin symbol in the genus field of K. As d_1 and d_2 encode quadratic fields, and m is the norm of an ideal with ideal class in a subgroup of C of exponent 2, the general Rédei symbol $[a, b, c]$ naturally takes its arguments in the group $\mathbf{Q}^*/\mathbf{Q}^{*2}$. It will be linear in each of its arguments.

Every $\bar{a} \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ is uniquely represented by a squarefree integer a, and corresponds to a number field $\mathbf{Q}(\sqrt{a})$ that is quadratic for $a \neq 1$. Given non-trivial elements in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ represented by squarefree integers a, b, the extension

$$\mathbf{Q}(\sqrt{ab}) = K \subset E = \mathbf{Q}(\sqrt{a}, \sqrt{b}) \tag{31}$$

is quadratic, and $\mathbf{Q} \subset E$ is unramified at primes outside the discriminants $\Delta(a)$ and $\Delta(b)$ of the quadratic fields corresponding to a and b.

We now assume that a and b have relative quadratic Hilbert symbols $(a, b)_p = 1$ for all primes p. As we observed at the end of Section 5, this amounts to saying that the equation

$$x^2 - ay^2 - bz^2 = 0 \tag{32}$$

admits non-zero rational solutions. By Corollaries 5·2 and 5·3, such a solution (x, y, z) generates a cyclic quartic extension

$$\mathbf{Q}(\sqrt{ab}) = K \subset F = F(x, y, z) = E(\sqrt{\beta}) = E(\sqrt{\alpha}) \tag{33}$$

in which we take $\beta = x + y\sqrt{a}$ and $\alpha = 2(x + z\sqrt{b})$. The field F is dihedral over $\mathbf{Q}$ for $a \neq b$, and cyclic over $\mathbf{Q}(\sqrt{ab}) = \mathbf{Q}$ for $a = b$. It is uniquely determined by a and b up to twisting by rational quadratic characters χ_t, with $t \in \mathbf{Q}^*/\mathbf{Q}^{*2}$. In fact, the asymmetry in (33)

in the definition of α and β coming out of (32) can be seen as making a somewhat arbitrary choice between F and F_2. Here we use the twisting notation

$$F_t = F(tx, ty, tz) = E(\sqrt{t\beta}) = E(\sqrt{t\alpha}) \tag{34}$$

for $F = F(x, y, z)$ from Section 5.

Before defining the general symbol $[a, b, c]$, we start with the special case of a squarefree integer $a = b \neq 1$. Then $K \subset E$ in (31) is the extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt{a})$. As Hilbert symbols satisfy $(a, -a)_p = 1$ for all $a \in \mathbf{Q}^*$, our assumption on a is $(a, -1)_p = 1$ for all p. By (18), this means that the discriminant $\Delta(a) \in \{a, 4a\}$ is positive and without prime divisors 3 mod 4, i.e., in the set $\mathcal{D}$ of Conjecture 3·2. For such a, we can write the associated Dirichlet character $\chi_a : G_{\mathbf{Q}} \to \mathbf{F}_2$ in the notation of (14) as

$$\chi_a = \sum_{p|a} \chi_p,$$

with $\chi_2 = \chi_8$ the quadratic character associated to $\mathbf{Q}(\sqrt{2})$. Let ψ_p be a character of order 4 modulo $p \equiv 1$ mod 4, and ψ_2 a character of order 4 on $(\mathbf{Z}/16\mathbf{Z})^*$. Then

$$\psi_a = \sum_{p|a} \psi_p \tag{35}$$

is a quartic Dirichlet character of conductor a (or $8a$ when a is even) that satisfies $2\psi_a = \chi_a$. It corresponds to a cyclic quartic field $F_{a,a}$ containing $E = \mathbf{Q}(\sqrt{a})$. Cyclic quartic $\mathbf{Q} \subset F$ containing E are unique up to quadratic twists, as $2\psi_F = \chi_a$ only defines ψ_F up to a quadratic character. Clearly $E \subset F$ will be ramified at all primes dividing a, but not at other primes if we take $\psi_F = \psi_a$ as in (35). Such an extension $\mathbf{Q} \subset F_{a,a}$ of *minimal ramification* is not unique, as we can add χ_p to each ψ_p of odd conductor p in (35), and χ_2 and χ_{-1} to ψ_2. This makes ψ_a unique up to twisting by sums of characters χ_p with $p|a$, and in addition the character χ_{-1} in case a is even. For $a = 1$ we define ψ_a to be the trivial character.

In terms of Corollary 5·3, a minimally ramified cyclic quartic extension $\mathbf{Q} \subset F_{a,a}$ containing $E = \mathbf{Q}(\sqrt{a})$ is unique up to twisting by t in the finite *twisting subgroup*

$$T_{a,a} \subset \mathbf{Q}^*/\mathbf{Q}^{*2} \tag{36}$$

generated by the residue classes of the odd primes $p = p^*$ dividing a and, for a even, of -1 and 2. It follows that for squarefree integers a and c satisfying

$$\gcd(\Delta(a), \Delta(c)) = 1 \quad \text{and} \quad (a, a)_p = (a, c)_p = 1 \text{ for all } p, \tag{37}$$

we have $\chi_t(c) = 0$ for $t \in T_{a,a}$, and a well defined *biquadratic character*

$$\psi_a(c) = \left(\frac{c}{a}\right)_4 \in \mathbf{F}_2. \tag{38}$$

In terms of Artin symbols in the cyclotomic field $\mathbf{Q}(\zeta_a)$ (or $\mathbf{Q}(\zeta_{8a})$) containing $F_{a,a}$, we have

$$\psi_a(c) = \text{Art}(c, F_{a,a}/\mathbf{Q}) \in \text{Gal}(F_{a,a}/E) = \mathbf{F}_2. \tag{39}$$

Note that a and $\Delta(a) \in \mathcal{D}$ have the same prime factors by the hypothesis $(a, a)_p = 1$ for all p. Thus (37) implies that for a even, with $-1, 2 \in T_{a,a}$, we have $c \equiv 1$ mod 4 by the

gcd-condition, and then $c \equiv 1 \bmod 8$ by the condition $(a, c)_2 = 1$, yielding $\chi_2(c) = \chi_{-1}(c) = 0$. For odd primes p dividing a, with $p \in T_{a,a}$, the conditions $(a, c)_p = 1$ and $\chi_p(c) = 0$ coincide.

Viewing ψ_a in (38) as defined on the subgroup of $\mathbf{Q}^*/\mathbf{Q}^{*2}$ generated by the integers c satisfying (37), we obtain the following special Rédei symbol.

Definition 7·1. For $a, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ satisfying (37), we take (38) to define

$$[a, a, c] = \psi_a(c) = \left(\frac{c}{a}\right)_4 \in \mathbf{F}_2.$$

For the general case, we take $a, b \in \mathbf{Z}_{\neq 1}$ to be different squarefree integers, assuming

$$(a, b)_p = 1 \quad \text{for all primes } p \tag{40}$$

in order to have non-trivial solvability of (32). Then the quadratic extension

$$\mathbf{Q}(\sqrt{ab}) = K \subset E = \mathbf{Q}(\sqrt{a}, \sqrt{b})$$

from (31) is only ramified at primes $\mathfrak{p} \mid \gcd(\Delta(a), \Delta(b))$, and such $\mathfrak{p}$ will be totally ramified in every cyclic quartic extension $K \subset F$ in (33). Generalizing (39), we are to define the Rédei symbol in Definition 7·8 as

$$[a, b, c] = \mathrm{Art}_c(F_{a,b}/K) \in \mathrm{Gal}(F_{a,b}/E) = \mathbf{F}_2,$$

the Artin symbol of an ideal $\mathfrak{c}$ in K corresponding to c in a cyclic quartic extension $K \subset F_{a,b}$ constructed from a solution to (32) that is *minimally ramified* over E.

For *odd* primes $p \nmid \gcd(\Delta(a), \Delta(b))$, one can avoid ramification over p in $E \subset F$ by passing, if needed, to the quadratic twist F_{p^*} from (34), with $p^* = \pm p$ as in (5).

PROPOSITION 7·2. *Let* $a, b \in \mathbf{Z}_{\neq 1}$ *be distinct and squarefree, $p \nmid \Delta(b)$ an odd prime, and* $K = \mathbf{Q}(\sqrt{ab}) \subset F = E(\sqrt{\beta})$ *as in* (33).

(i) *If p divides $\Delta(a)$, then $K \subset F$ is unramified over p.*

(ii) *If p does not divide $\Delta(a)$, then exactly one of $K \subset F$ and $K \subset F_{p^*}$ is unramified over p.*

Proof. Consider F as a quartic extension of $K_a = \mathbf{Q}(\sqrt{a})$. The intermediate field $E = K(\sqrt{b}) = K_a(\sqrt{b})$ is a quadratic extension of both K and K_a that is unramified at primes dividing p, as we have $p \nmid \Delta(b)$. It follows that $K \subset F$ is unramified over p if and only if $K_a \subset F$ is.

Write $F = K_a(\sqrt{\beta}, \sqrt{\beta'})$, with $\beta \in K_a$ of norm $\beta\beta' = x^2 - ay^2 = bz^2$. As p is odd, $K_a \subset F$ is unramified over p if and only if β and β' have even valuation at the primes $\mathfrak{p} \mid p$ in K_a. For a prime $\mathfrak{p} \mid p$ of ramification index $e_{\mathfrak{p}/p}$ in K_a, we have

$$\mathrm{ord}_{\mathfrak{p}}(\beta\beta') = e_{\mathfrak{p}/p} \, \mathrm{ord}_p(bz^2) = 2e_{\mathfrak{p}/p} \, \mathrm{ord}_p(z).$$

In the ramified case $p \mid \Delta(a)$, we have $e_{\mathfrak{p}/p} = 2$ and $\mathrm{ord}_{\mathfrak{p}}(\beta\beta') = 2\,\mathrm{ord}_{\mathfrak{p}}(\beta) \equiv 0 \bmod 4$, proving (i). In the unramified case $p \nmid \Delta(a)$, we have $e_{\mathfrak{p}/p} = 1$ and $\mathrm{ord}_{\mathfrak{p}}(\beta) \equiv \mathrm{ord}_{\mathfrak{p}}(\beta') \bmod 2$. Moreover, we have $\mathrm{ord}_{\mathfrak{p}}(p^*\beta) = \mathrm{ord}_{\mathfrak{p}}(\beta) + 1$, so $\mathfrak{p}$ is unramified in exactly one of F and F_{p^*}, proving (ii). $\qquad\square$

As twisting by p^* does not change ramification outside p, Proposition 7·2 shows that $K \subset F$ in (33) can be chosen to be unramified at all odd $p \nmid \gcd(\Delta(a), \Delta(b))$. For $p = 2$ we can twist by -1 and 2, with the following outcome.

PROPOSITION 7·3. *Let* $a, b \in \mathbf{Z}_{\neq 1}$ *be distinct and squarefree,* $b = \Delta(b) \equiv 1 \bmod 4$, *and* $K = \mathbf{Q}(\sqrt{ab}) \subset F = E(\sqrt{\beta})$ *as in* (33).

  (i)   *If* $\Delta(a)$ *is odd, then* $\mathbf{Q} \subset F_t$ *is unramified at 2 for a unique* $t \in \{\pm 1, \pm 2\}$.
  (ii) *If* $\Delta(a)$ *is even and* $\Delta(b)$ *is 1 mod 8, then* $K \subset F_t$ *is unramified over 2 for exactly two values of* $t \in \{\pm 1, \pm 2\}$.
  (iii) *If* $\Delta(a)$ *is even and* $\Delta(b)$ *is 5 mod 8, then* $K \subset F_t$ *is ramified over 2 for all* $t \in \mathbf{Q}^*$, *and* $\Delta(a)$ *is 4 mod 8.*

Proof. Just as for odd p, we consider the extension $K_a \subset F = K_a(\sqrt{\beta}, \sqrt{\beta'})$. As before, up to squares, β is a 2-unit in K_a if $\Delta(a)$ is even, and exactly one of β and 2β is a 2-unit K_a if $\Delta(a)$ is odd. However, for a 2-unit to have a square root that is unramified at 2, we need the stronger condition that it is a square modulo 4.

We can assume, possibly after twisting F by $t = 2$, that β is a 2-unit in the ring of integers $\mathcal{O}$ of K_a. For $2 \nmid \Delta(a)$, the group $(\mathcal{O}/4\mathcal{O})^*$ has order 4 or 12, depending on whether 2 is split or inert in $\mathcal{O}$, and the squares form a subgroup of index 4. Together with -1, they generate the kernel of the surjective norm map

$$N : (\mathcal{O}/4\mathcal{O})^* \longrightarrow (\mathbf{Z}/4\mathbf{Z})^*.$$

By assumption, we have $\beta\beta' \equiv b \equiv 1 \bmod 4\mathcal{O}$, so the residue classes $\beta, \beta' \in \ker N$ are squares in $(\mathcal{O}/4\mathcal{O})^*$ for a unique 'sign choice' of β, and $\mathbf{Q} \subset F_t$ is unramified at 2 for a unique value $t \in \{\pm 1, \pm 2\}$. This proves (i).

For $2 | \Delta(a)$, the group $(\mathcal{O}/4\mathcal{O})^* = (\mathcal{O}/\mathfrak{p}^4\mathcal{O})^*$ has order 8, and its subgroup of squares, of index 4, is of order 2. The norm $\mathcal{O} = \mathbf{Z}[\sqrt{a}] \to \mathbf{Z}$ induces a map

$$N : (\mathcal{O}/4\mathcal{O})^* \longrightarrow (\mathbf{Z}/8\mathbf{Z})^*$$

for which the image, of order 2, is generated by $1 - a \bmod 8$ when $a \equiv \pm 2 \bmod 8$ is even, and by 5 mod 8 when $a \equiv -1 \bmod 4$ is odd.

In the case where a is even, $\ker N$ is non-cyclic of order 4, generated by -1 and the squares in $(\mathcal{O}/4\mathcal{O})^*$, and it contains $\beta \bmod 4\mathcal{O}$ as $\beta\beta' \equiv b \bmod 8$ is not 5 mod $8 \notin \operatorname{im} N$. In this case, we have $\Delta(b) = b \equiv 1 \bmod 8$, and we conclude just as before that exactly one of F and F_{-1} is unramified over K at 2. By the same argument applied to F_2, one of F_2 and F_{-2} is unramified over K at 2, so $K \subset F_t$ is unramified over 2 for exactly two values $t \in \{\pm 1, \pm 2\}$, as stated in (ii).

In the remaining case $a \equiv -1 \bmod 4$, or $\Delta(a) \equiv 4 \bmod 8$, the residue class of

$$\tau = (1 + \sqrt{a})^2/2 = (1 + a)/2 + \sqrt{a} \tag{41}$$

in $(\mathcal{O}/4\mathcal{O})^*$, which equals $\sqrt{a} \bmod 4\mathcal{O}$ for $a \equiv -1 \bmod 8$ and $2 + \sqrt{a} \bmod 4\mathcal{O}$ for $a \equiv 3 \bmod 8$, has square $-1 \bmod 4\mathcal{O}$, so it is of order 4 and generates $\ker N$.

We now have 2 cases. For $\Delta(b) = b \equiv 1 \bmod 8$ we have $\beta \bmod 4\mathcal{O} \in \ker N$, and twisting by $t = 2$, which replaces β by β/τ, may be used to move β into the subgroup $\pm 1 \bmod 4\mathcal{O}$ of squares in $(\mathcal{O}/4\mathcal{O})^*$. In this case either F and F_{-1} or F_2 and F_{-2} are unramified over K at 2, proving (ii).

The final case $a \equiv -1 \bmod 4$ and $\Delta(b) = b \equiv 5 \bmod 8$ is the case occurring in (iii). Here twisting by -1 or 2 cannot move β or β' into $\ker N$, and the extension $K_a \subset F = K_a(\sqrt{\beta}, \sqrt{\beta'})$ is ramified at the prime $\mathfrak{p}|2$ of K_a. This implies that $K \subset F_t$ is ramified over 2 for all $t \in \mathbf{Q}^*$, proving (iii).

Alternatively, one can argue for (iii) that if the ramified prime over 2 in K, which is inert in $K \subset E$, were unramified in the cyclic quartic extension $K \subset F_t$, the primes over 2 in F_t would have ramification index 2 and residue class degree 4 over $\mathbf{Q}$; but the dihedral group of order 8 has no cyclic quotient of order 4. $\square$

The *ramified case* (iii) of Proposition 7·3 does not occur when $D = \Delta(a)\Delta(b)$ is a decomposition satisfying the conditions of Lemma 4·2, as for even D, the prime 2 splits in either $\mathbf{Q}(\sqrt{a})$ or $\mathbf{Q}(\sqrt{b})$, by condition (iv) of Lemma 4·2.

COROLLARY 7·4. *Let (x, y, z) be a primitive integral solution to (26) for $D = d_1 d_2$ satisfying the conditions of Lemma 4·2. Then there exists $t \in \{\pm 1, \pm 2\}$ such that $F_t = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{tx + ty\sqrt{d_1}})$ is unramified and cyclic of degree 4 over $\mathbf{Q}(\sqrt{D})$.*

Proof. For (x, y, z) primitive and p odd, $\beta = x + y\sqrt{d_1}$ and $\alpha = 2(x + z\sqrt{d_2})$ are not divisible by p, hence units at a prime over p in $\mathbf{Q}(\beta)$ and $\mathbf{Q}(\alpha)$, making $\mathbf{Q}(\sqrt{D}) \subset F_1$ unramified outside 2. Twisting by $t \in \{\pm 1, \pm 2\}$ as in (i) and (ii) of Proposition 7·3 makes it unramified at 2 as well. $\square$

In the ramified case (iii) of Proposition 7·3, with $a \equiv -1 \bmod 4$ and $b \equiv 5 \bmod 8$, which is essential for Rédei reciprocity, the extension $K \subset F$ in (33) gives rise to a local field $F \otimes \mathbf{Q}_2$ that is dihedral of degree 8 over $\mathbf{Q}_2$, and quadratic over

$$E \otimes \mathbf{Q}_2 = \mathbf{Q}_2(\sqrt{a}, \sqrt{b}) = \mathbf{Q}_2(i, \sqrt{5}). \tag{42}$$

It is cyclic over $\mathbf{Q}_2(\sqrt{-5})$ for $a \equiv -1 \bmod 8$, and cyclic over $\mathbf{Q}_2(i)$ for $a \equiv -5 \bmod 8$. Ramification in $E \otimes \mathbf{Q}_2 \subset F \otimes \mathbf{Q}_2$ cannot be avoided, but one can obtain 2-*minimal ramification* after twisting, if necessary, by the generator $t = 2$ of

$$\mathbf{Q}_2^*/\langle a, b, \mathbf{Q}_2^{*2}\rangle = \mathbf{Q}_2^*/\langle -1, 5, \mathbf{Q}_2^{*2}\rangle \cong \mathbf{Z}/2\mathbf{Z}.$$

In view of (41), this amounts to replacing β by $\tau\beta$. In this way we can make β trivial in the group $(\mathcal{O}/2\mathcal{O})^* = \langle \overline{\tau} \rangle = \langle \sqrt{a} \bmod 2\mathcal{O}\rangle$ of order 2, and we can even change the sign of β – this does not change $F \otimes \mathbf{Q}_2$ – to achieve $\beta \equiv 1 \bmod \mathfrak{p}^3$, with $\mathfrak{p}|2$ in K_a. This is not quite the congruence $\beta \equiv 1 \bmod \mathfrak{p}^4$ that would make $K_a = \mathbf{Q}(\sqrt{a}) \subset F$ unramified over 2, but it does ensure that the local extension $\mathbf{Q}_2(\sqrt{a}) \subset F \otimes \mathbf{Q}_2$ is of conductor 2, the minimum for a ramified biquadratic extension of $\mathbf{Q}_2(\sqrt{a})$. One has $F \otimes \mathbf{Q}_2 = \mathbf{Q}_2(i, \sqrt{5}, \sqrt{x})$ with $x = 1 + 2i$ for $a \equiv -1 \bmod 8$ and $x = 3 + 2\sqrt{-5}$ for $a \equiv -5 \bmod 8$.

Definition 7·5. In the ramified case (3) of Proposition 7·3, with $a \equiv -1 \bmod 4$ and $b \equiv 5 \bmod 8$, the extension $K \subset F$ is 2-minimally ramified if the local biquadratic extension $\mathbf{Q}_2(\sqrt{a}) \subset F \otimes \mathbf{Q}_2$ is of conductor 2.

The requirement in Definition 7·5 means that we have $F = E(\sqrt{\beta})$ for an element $\beta \in 1 + 2\mathcal{O} \subset K_a^*$. Any F in case (iii) of Proposition 7·3 has a twist F_t with $t \in \{\pm 1, \pm 2\}$, unique up to sign, that is 2-minimally ramified.

For arbitrary non-trivial elements $a, b \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ for which (32) admits non-zero solutions, we are led to the following global notion of *minimal ramification*.

Definition 7·6. For $a, b \in \mathbf{Q}^*/\mathbf{Q}^{*2} \setminus \{1\}$, the extension $K \subset F$ in (33) defined by a non-zero rational solution to (32) is said to be minimally ramified over E if it is

(i) unramified over all odd primes $p \nmid \gcd(\Delta(a), \Delta(b))$;
(ii) unramified over 2 when $\Delta(a)\Delta(b)$ is odd, or one of $\Delta(a), \Delta(b)$ is 1 mod 8;
(iii) 2-minimally ramified if $(\Delta(a), \Delta(b))$ is (5, 4) or (4, 5) modulo 8.

In the special case $a = b$, we recover our earlier definition of a minimally ramified extension $\mathbf{Q} \subset F_{a,a}$, as being unramified at the primes $p \nmid a$.

Every extension $K \subset F$ in (33) can be twisted by some $t \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ to obtain a minimally ramified extension $K \subset F_{a,b}$, but $F_{a,b}$ is not uniquely determined by $a, b \in \mathbf{Q}^*/\mathbf{Q}^{*2}$. More precisely, we have a finite *twisting subgroup*

$$T_{a,b} \subset \mathbf{Q}^*/\mathbf{Q}^{*2} \tag{43}$$

just as for $a = b$ in (36). It is generated by the residue classes of the odd signed primes p^* occurring in the discriminantal factorisations (5) of $\Delta(a)$ and $\Delta(b)$, together with -1 and 2 if both $\Delta(a)$ and $\Delta(b)$ are even, and with the unique non-trivial discriminantal 2-part $t_{\Delta(a)}$ or $t_{\Delta(b)}$ in $\{-4, \pm 8\}$ if only one of them is even. For $a = b$, this definition coincides with (36). It is tailored to obtain the following.

LEMMA 7·7. *For $a, b \in \mathbf{Q}^*/\mathbf{Q}^{*2} \setminus \{1\}$ satisfying* (40)*, there exists $F = F(x, y, z)$ in* (33) *that is minimally ramified over E. For such F and $t \in \mathbf{Q}^*/\mathbf{Q}^{*2}$, we have*

$$K \subset F_t \text{ is minimally ramified} \iff t \in T_{a,b}.$$

Proof. We already showed existence. If $\Delta(a)$ and $\Delta(b)$ are not both even, it follows from (8) that the elements $t \in T_{a,b}$ are exactly the Dirichlet characters of the quadratic extensions $\mathbf{Q} \subset \mathbf{Q}(\sqrt{t})$ that become unramified over $E = \mathbf{Q}(\sqrt{a}, \sqrt{b})$, and preserve the minimal ramification of F under twisting. If both $\Delta(a)$ and $\Delta(b)$ are even, inclusion of both generators -1 and 2 'at 2' ensures that for $t_a = t_b \neq 1$, when Definition 7·6 imposes no restriction on ramification at 2 on $K \subset F$, we do allow all possible quadratic twists of 2-power conductor. $\qquad \square$

We are now ready to define the Rédei symbol $[a, b, c]$ for $a, b, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ satisfying (1) and (2) from the Introduction, i.e., with relative quadratic Hilbert symbols

$$(a, b)_p = (a, c)_p = (b, c)_p = 1$$

at all primes p, and associated discriminants satisfying the coprimality condition

$$\gcd(\Delta(a), \Delta(b), \Delta(c)) = 1.$$

Definition 7·8. For non-trivial $a, b, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ satisfying (1) and (2), let $K = \mathbf{Q}(\sqrt{ab}) \subset F_{a,b}$ be minimally ramified over $E = \mathbf{Q}(\sqrt{a}, \sqrt{b})$, as in Definition 7·6. Then the Rédei symbol

$$[a, b, c] \in \operatorname{Gal}(F_{a,b}/E) = \mathbf{F}_2$$

is defined as

$$[a, b, c] = \mathrm{Art}_c(F_{a,b}/K) = \begin{cases} \mathrm{Art}(\mathfrak{c}, F_{a,b}/K) & \text{if} \quad c > 0; \\ \mathrm{Art}(\mathfrak{c}\infty, F_{a,b}/K) & \text{if} \quad c < 0. \end{cases} \tag{44}$$

Here $\mathfrak{c}$ is an integral $\mathcal{O}_K$-ideal of norm $|c_0|$, with c_0 the squarefree integer in the class of c, and ∞ denotes an infinite prime of K.

If one of a, b, or c is trivial in $\mathbf{Q}^*/\mathbf{Q}^{*2}$, we take $[a, b, c] = 0$.

With this definition, which we show in Corollary 8·2 to be independent of the choice of the minimally ramified extension $K \subset F_{a,b}$, the Rédei symbol becomes perfectly symmetric in its 3 arguments. *Rédei's reciprocity law* is the following precise version of Theorem 1·1.

THEOREM 7·9. *For $a, b, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ satisfying* (1) *and* (2)*, the symbol* (44) *is well-defined, linear in each of its arguments, and satisfies*

$$[a, b, c] = [b, a, c] = [a, c, b] \in \mathbf{F}_2.$$

We say that the Rédei symbol $[a, b, c]$ *is defined* if its arguments $a, b, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ satisfy the conditions (1) and (2).

The inclusion of the infinite prime in the definition (44) almost by tautology leads to the following useful property.

PROPOSITION 7·10. *Let $D = d_1 d_2$ be a decomposition of the second kind as in Definition 4·4. Then the Rédei symbol $[d_1, d_2, -d_1 d_2] \in \mathbf{F}_2$ is defined and equals 0.*

Proof. Multiplying $(d_1, d_2)_p = 1$ in (44) by the trivial symbols $(d_1, -d_1)_p$ and $(-d_2, d_2)_p$, we obtain $(d_1, -d_1 d_2)_p = (-d_1 d_2, d_2) = 1$, so $[d_1, d_2, -d_1 d_2]$ satisfies (1), and obviously also (2).

Suppose $D = d_1 d_2 < 0$. Then the principal ideal $(\sqrt{D})$ in the ring of integers of $K = \mathbf{Q}(\sqrt{D})$ of norm $c = -D = -d_1 d_2 > 0$ is trivial in $C(D)$, so its Artin symbol acts trivially on any unramified abelian extension $K \subset F$. In case D is odd, c is squarefree, and definition (44) with $a = d_1$, $b = d_2$, and $\mathfrak{c} = (\sqrt{D})$ yields the desired equality $[a, b, c] = [d_1, d_2, -d_1 d_2] = 0$. For $D < 0$ even, $\mathfrak{c} = (\sqrt{D}/2)$ of squarefree norm $-d_1 d_2/4$ does the same.

In the case $D = d_1 d_2 > 0$, the class of the ideal $\mathfrak{c} = (\sqrt{D})$ of norm $D = d_1 d_2$ in $C(D)$ is the Frobenius at infinity F_∞ from (4), which acts as $\mathrm{Art}(\infty, F/K)$ on the finitely unramified abelian extension $K \subset F$. For D odd and $c = -D < 0$ squarefree, $[a, b, c] = [d_1, d_2, -d_1 d_2]$ now corresponds to the action of the *square* of $\mathrm{Art}(\infty, F/K)$ on F, which is *also* the identity, yielding $[d_1, d_2, -d_1 d_2] = 0$. For $D > 0$ even, $\mathfrak{c} = (\sqrt{D}/2)$ does the job. $\square$

8. *Proving Redei reciprocity*

We already mentioned that Rédei's original definition is different from (44). Not only does he omit a contribution of the infinite prime, putting $[a, b, -c] = [a, b, c]$, he also requires at least one of $\Delta(a)$ and $\Delta(b)$ to be odd, making a symbol like $[-1, 2, p]$ in (30) undefined. The resulting reciprocity law [16, Satz 4] has superfluous 2-adic restrictions on the entries, and for $bc < 0$ the symbols $[a, b, c]$ and $[a, c, b]$, which are only both defined for

$\Delta(a)$ without prime factors congruent to 3 mod 4, differ by a product of four quadratic and biquadratic symbols.

In his 2007 thesis, Corsman found that including an Artin symbol at infinity for $c < 0$ leads to a perfectly symmetric version of the reciprocity law. Both his definition of the symbol and his proof of the law rely heavily on an incorrect lemma [**5**, lemma 5·1·2] claiming that the assumptions (1) and (2) guarantee the existence of an extension $K \subset F$ in (44) that is unramified at *all* primes $p \nmid \gcd(\Delta(a), \Delta(b))$. Smith's paper on the average 8-rank behavior of imaginary quadratic class groups also has an incorrect version of the reciprocity law [**18**, proposition 2·1] that disregards the subtleties at both infinite and dyadic primes.

We now let a, b, and c be squarefree integers different from 1 satisfying (1) and (2). To see that $[a, b, c]$ is well-defined, and independent of the many choices that go into the definition of the symbol, we first note, using Lemma 7·7, that an extension $K \subset F_{a,b}$ in (44) that is minimally ramified over E does exist, and that it is unique up to twisting by $t \in T_{a,b}$.

Let $K \subset F$ be minimally ramified over $E = \mathbf{Q}(\sqrt{a}, \sqrt{b})$, and p a prime dividing c. Then p is split or ramified in $\mathbf{Q}(\sqrt{a})$ and in $\mathbf{Q}(\sqrt{b})$ by (1), and unramified in at least one of these fields by (2). For a prime $\mathfrak{p}_K | p$ in K, this implies that $\mathfrak{p}_K$ is of degree 1, and split in the extension $K \subset E$. Moreover, $\mathfrak{p}_K$ is *unramified* in $K \subset F$ for primes $p | c$. Indeed, for odd p we are in case (i) of Definition 7·6 by (2). For $2 | c$ at least one of $\Delta(a)$, $\Delta(b)$ is odd, say $\Delta(b)$, and then the condition $(b, c)_2 = (\Delta(b), 2)_2 = 1$ in (1) shows that we have $\Delta(b) \equiv 1 \bmod 8$, putting us in case (ii) of Definition 7·6. Thus $\mathrm{Art}(\mathfrak{p}_K, F/K) \in \mathrm{Gal}(F/E)$ is a well-defined element of $\mathrm{Gal}(F/\mathbf{Q})$. As $\mathrm{Gal}(F/E)$ is contained in the center of $\mathrm{Gal}(F/\mathbf{Q})$, and equal to it if $\mathbf{Q} \subset F$ is dihedral,

$$[a, b, c]_{F,p} = \mathrm{Art}(\mathfrak{p}_K, F/K) \in \mathrm{Gal}(F/E) \qquad (45)$$

only depends on F and p, not on $\mathfrak{p}_K | p$ in K. For $p \nmid c$ we put $[a, b, c]_{F,p} = \mathrm{id}_F$.

For $c < 0$, we have $a, b > 0$ by condition (1) for $p = \infty$, so $E = \mathbf{Q}(\sqrt{a}, \sqrt{b})$ is totally real, and the decomposition group at every infinite prime of F is generated by the Frobenius at infinity

$$[a, b, c]_{F,\infty} = \mathrm{Art}(\infty, F/K) \in \mathrm{Gal}(F/E).$$

For $c > 0$ we put $[a, b, c]_{F,\infty} = \mathrm{id}_F$.

With this notation, the Rédei symbol in (44) becomes a product

$$[a, b, c] = \prod_{p \leq \infty} [a, b, c]_{F,p} \in \mathrm{Gal}(F/E) \qquad (46)$$

of its *p-parts*. The infinite product (46) is well-defined in $\mathrm{Gal}(F/E)$, as we can only have $[a, b, c]_{F,p} \neq \mathrm{id}_F$ for primes $p | c$, with $\infty | c$ having the meaning $c < 0$.

As the prime $\mathfrak{p}_K$ in the Artin symbol $\mathrm{Art}(\mathfrak{p}_K, F/K) = [a, b, c]_{F,p}$ for $p | c$ in (45) splits in $K \subset E$, we can view it as the Artin symbol of a prime $\mathfrak{p}_E | p$ of E in the quadratic extension $E \subset F = E(\sqrt{\beta}) = E(\sqrt{\beta'})$. As $\mathfrak{p}_E$ is unramified in $E \subset F$, its norm to K_a is a prime $\mathfrak{p}$ of degree 1 over p in K_a that is unramified in at least one of the quadratic extensions $K_a(\sqrt{\beta})$ and $K_a(\sqrt{\beta'})$ of K_a. Replacing $\mathfrak{p}$ by a conjugate prime in K_a if necessary, we can take it to be unramified in $K_a \subset K_a(\sqrt{\beta})$. We can then compute the p-part of $[a, b, c]$ as

$$[a, b, c]_{F,p} = \mathrm{Art}(\mathfrak{p}, K_a(\sqrt{\beta})/K_a) \in \{\pm 1\}. \qquad (47)$$

This shows that $[a, b, c]_{F,p}$ is essentially a Legendre symbol $(\frac{\beta}{\mathfrak{p}})$ in the field K_a. The reason that we choose its value to lie in $\{\pm 1\}$ rather than in $\mathbf{F}_2$, which is of course 'only' a matter of notation, is not just a Legendre symbol tradition, or the fact that Galois groups like $\mathrm{Gal}(F/E)$ tend to be written as multiplicative groups. The point is that, for $\mathfrak{p}|p$ unramified in $K_a \subset K_a(\sqrt{\beta})$, the p-part of $[a, b, c]$ *is* the quadratic Hilbert symbol

$$[a, b, c]_{F,p} = (\beta, \pi)_{\mathfrak{p}} \in \{\pm 1\} \tag{48}$$

of β and a uniformizer π in the completion of K_a at $\mathfrak{p}$. For $c < 0$ and $p = \infty$, we have $[a, b, c]_{F,\infty} = (\beta, -1)_{\mathfrak{p}}$, as the archimedean nature of $F = E(\sqrt{\beta})$ is determined by the sign of β at a real prime $\mathfrak{p}$ of K_a. Respecting tradition, we have refrained from using Hilbert symbols with values in $\mathbf{F}_2$.

It is clear from the symmetry in a and b of the definition of the Rédei symbol $[a, b, c]$ that we have $[a, b, c] = [b, a, c]$ whenever the symbol is defined. In order to prove the nontrivial *reciprocity law* $[a, b, c] = [a, c, b]$ in Theorem 1·1, we choose a minimally ramified extension $F = E(\sqrt{\beta})$ of $K = \mathbf{Q}(\sqrt{ab})$ as in (33) in order to express $[a, b, c]$ as a product of p-parts $[a, b, c]_{F,p}$ as in (46), and similarly a minimally ramified extension $F' = E'(\sqrt{\gamma})$ of $K' = \mathbf{Q}(\sqrt{ac})$ in order to express $[a, c, b]$ as a product of $[a, c, b]_{F',p}$. Here $\beta, \gamma \in \mathbf{Q}(\sqrt{a})^*$ are elements of norm $b, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$, and the fields F and F' are the normal closures of $\mathbf{Q}(\sqrt{a}, \sqrt{\beta})$ and $\mathbf{Q}(\sqrt{a}, \sqrt{\gamma})$, respectively. In the spirit of (48), we then have the following key lemma.

LEMMA 8·1. *Let $a, b, c \in \mathbf{Q}^*/\mathbf{Q}^{*2}$ be non-trivial elements satisfying (1) and (2), and $F = E(\sqrt{\beta})$ and $F' = E'(\sqrt{\gamma})$ minimally ramified extensions of $K = \mathbf{Q}(\sqrt{ab})$ and $K' = \mathbf{Q}(\sqrt{ac})$ defined as above. For all rational primes $p \le \infty$, we then have*

$$[a, b, c]_{F,p} \cdot [a, c, b]_{F',p} = \prod_{\mathfrak{p}|p \text{ in } \mathbf{Q}(\sqrt{a})} (\beta, \gamma)_{\mathfrak{p}}. \tag{49}$$

Proof. We denote the left-and right-hand side of (49) by L_p and R_p, respectively, and note that L_p and R_p are symmetric in b and c. Moreover, we can replace β (or γ) in R_p by its conjugate without changing the value of R_p, as the expression R'_p obtained by replacing β by β' satisfies $R_p R'_p = \prod_{\mathfrak{p}|p}(b, \gamma)_{\mathfrak{p}} = (b, c)_p = 1$.

For $p = \infty$, condition (1) implies that at most one of a, b, c is negative. If they are all positive, we have $L_\infty = 1$, and both β and γ are totally positive or negative in the real quadratic field $K_a = \mathbf{Q}(\sqrt{a})$. The symbols $(\beta, \gamma)_{\mathfrak{p}}$ at the two infinite primes of K_a then have the same value, so we also have $R_\infty = 1$. If only a is negative, we have $L_\infty = 1 = R_\infty$, as the unique infinite prime of K_a is complex.

If a is positive and exactly one of b and c, say c, is negative, L_∞ is the Frobenius at infinity in $E \subset F = E(\sqrt{\beta})$, which equals 1 if $\beta \in K_a^*$ is totally positive, and -1 if β is totally negative. As γ has a positive and a negative embedding in $\mathbf{R}$, the same value is taken by the product $R_\infty = (\beta, \gamma)_{\infty_1}(\beta, \gamma)_{\infty_2}$ of the Hilbert symbols at the infinite primes of K_a. This settles the case $p = \infty$.

For p a finite prime, take a, b, c to be squarefree integers. Condition (2) implies that p divides at most two of a, b, c. If p divides b, it is split or ramified in K_a, and β is, up to squares in K_a^*, a uniformiser at a prime $\mathfrak{p}_1|p$ and, in the split case $(p) = \mathfrak{p}_1\mathfrak{p}_2$, a unit at the other prime $\mathfrak{p}_2|p$ in K_a. If p does not divide b, then the minimal ramification of $K \subset F$

implies that β is a p-unit, up to squares in K_a^*. For odd p this means that $\sqrt{\beta} \in F$ generates an extension of K_a that is unramified over p. Analogous statements apply to c and γ.

Suppose first that p is odd. If p does not divide bc, we have $L_p = 1 = R_p$, as the Hilbert symbols $(\beta, \gamma)_{\mathfrak{p}}$ at $\mathfrak{p}|p$ are equal to 1 for p-units β and γ. If p divides exactly one of b, c, say c, we can take β to be a p-unit, with square root in F that is unramified over p, and γ a uniformiser at a prime $\mathfrak{p}_1|p$. By (48), we then have

$$L_p = [a, b, c]_{F, p} = (\beta, \gamma)_{\mathfrak{p}_1}. \tag{50}$$

In the split case $(p) = \mathfrak{p}_1 \mathfrak{p}_2$, we further have $(\beta, \gamma)_{\mathfrak{p}_2} = 1$, as both β and γ are units at $\mathfrak{p}_2$. This yields $L_p = R_p$ both in the ramified and in the split case.

If p divides both b and c, it does not divide a, so we are in the split case $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ in K_a. After replacing β by its conjugate, if necessary, β is a unit at $\mathfrak{p}_1$ and a uniformizer at $\mathfrak{p}_2$, whereas γ is a uniformizer at $\mathfrak{p}_1$ and a unit at $\mathfrak{p}_2$. Again by (48),

$$L_p = [a, b, c]_{F, p} \cdot [a, c, b]_{F', p} = (\beta, \gamma)_{\mathfrak{p}_1} (\beta, \gamma)_{\mathfrak{p}_2} = R_p, \tag{51}$$

so we have proved our lemma for odd p.

For $p = 2$, we need a finer distinction as $2 \nmid b$, and even $2 \nmid \Delta(b)$, does not imply that the minimally ramified extension $K \subset F$ is unramified over 2, and that $\sqrt{\beta}$ generates a subextension of $K_a \subset F$ that is unramified over 2. For $2 \nmid \Delta(b)$, or $b \equiv 1 \bmod 4$, Definition 7·6 shows that it does in all cases except in the case $a \equiv -1(4)$ and $b \equiv 5 \bmod 8$. For $b \equiv -1 \bmod 4$, when 2 divides $\Delta(b)$ but not b, we do know that β is, up to squares in K_a^*, a 2-adic unit. Moreover, for $\Delta(b)$ even and 2 split in K_a, the extension $K_a \subset K_a(\sqrt{\beta})$ is unramified at one prime over 2, and ramified at the other. Same for c and γ.

Suppose first that bc is odd. Then we have $L_2 = 1$, and we take β and γ to be 2-units. By the condition $(b, c)_2 = 1$ at least one of b, c, say b, is 1 mod 4. For $c \equiv -1 \bmod 4$, the condition $(a, c)_2 = 1$ implies $a \not\equiv -1 \bmod 4$, so the minimally ramified extension $K \subset F$ is unramified over 2, and all Hilbert symbols $(\beta, \gamma)_{\mathfrak{p}}$ at primes $\mathfrak{p}|2$ in K_a occurring in R_2 equal 1, as γ is a unit at $\mathfrak{p}$ and $K_a \subset K_a(\sqrt{\beta})$ is unramified at $\mathfrak{p}$. For $c \equiv 1 \bmod 4$, Definition 7·6 tells us that we are in the same situation, with $R_2 = 1$ because one of β, γ is a $\mathfrak{p}$-unit and the other has a $\mathfrak{p}$-unramified square root, provided that either we have $a \not\equiv -1 \bmod 4$ or one of b, c is 1 mod 8. The remaining special case $a \equiv -1 \bmod 4$ and $b \equiv c \equiv 5 \bmod 8$ is when both $K_a \subset F$ and $K_a \subset F'$ are ramified at the prime $\mathfrak{p}|2$ of K_a. This is where the *minimal* ramification at 2 of the extensions $K \subset F$ and $K \subset F'$ from Definition 7·5 is essential: once more we have $R_2 = (\beta, \gamma)_{\mathfrak{p}} = 1$, as $\sqrt{\beta}$ generates an extension of conductor 2 of the completion $\mathbf{Q}_2(\sqrt{a})$ of K_a at $\mathfrak{p}$, and γ is 1 modulo $\mathfrak{p}^2 = (2)$ in K_a. This proves $L_2 = 1 = R_2$ for bc odd.

If exactly one of b, c is even, say c, the condition $(a, c)_2 = (b, c)_2 = 1$ implies $a, b \not\equiv 5 \bmod 8$. For $b \equiv 1 \bmod 8$, the minimally ramified extension $K \subset F$, and therefore $K_a \subset K_a(\sqrt{\beta})$, is unramified over 2. In this case, we have

$$L_2 = [a, b, c]_{F, 2} = (\beta, \gamma)_{\mathfrak{p}_1} = R_2$$

just as in the case of odd p, as we can take γ to be a uniformizer at $\mathfrak{p}_1|2$ and, in the split case, a unit at the other prime $\mathfrak{p}_2$. In the other case $b \equiv -1 \bmod 4$ both $\Delta(b)$ and $\Delta(c)$ are even, so we have $a \equiv 1 \bmod 8$ and $(2) = \mathfrak{p}_1 \mathfrak{p}_2$ in K_a. In this case, $\sqrt{\beta}$ and $\sqrt{\gamma}$ generate extensions of K_a that are ramified at one prime over 2, and unramified at the other. Replacing β or γ by their conjugate if necessary, we can assume that $K_a \subset K_a(\sqrt{\beta})$ is unramified at $\mathfrak{p}_1$ and

$K_a \subset K_a(\sqrt{\gamma})$ unramified at $\mathfrak{p}_2$. Up to squares, γ is a then a uniformiser at $\mathfrak{p}_1$ and β a unit at $\mathfrak{p}_2$, so we have

$$L_2 = [a, b, c]_{F,2} = (\beta, \gamma)_{\mathfrak{p}_1} = (\beta, \gamma)_{\mathfrak{p}_1}(\beta, \gamma)_{\mathfrak{p}_2} = R_2.$$

Finally, for b and c both even, we are also in the split case, as $\Delta(a)$ is odd and $(a, b)_2 = (a, 2)_2 = 1$ implies $a \equiv 1 \bmod 8$. As above, we can choose $K_a \subset K_a(\sqrt{\beta})$ unramified at $\mathfrak{p}_1$ and $K_a \subset K_a(\sqrt{\gamma})$ unramified at $\mathfrak{p}_2$. Up to squares, this makes β a uniformizer at $\mathfrak{p}_2$ and γ a uniformizer at $\mathfrak{p}_1$. We obtain

$$L_2 = [a, b, c]_{F,2}[a, c, b]_{F',2} = (\beta, \gamma)_{\mathfrak{p}_1}(\beta, \gamma)_{\mathfrak{p}_2} = R_2,$$

and we have finished the proof of Lemma 8·1. $\qquad\square$

Proof of Theorem 1·1. By Lemma 8·1, the sum in $\mathbf{F}_2$ of the Rédei symbols $[a, b, c]$ and $[a, c, b]$, when defined as in (44) with the help of $F = E(\sqrt{\beta})$ and $F' = E'(\sqrt{\gamma})$, respectively, is the additive analogue of $\prod_{\mathfrak{p} \le \infty}(\beta, \gamma)_{\mathfrak{p}} \in \{\pm 1\}$, where the product ranges over all primes $\mathfrak{p} \le \infty$ of $\mathbf{Q}(\sqrt{a})$. By the product formula for Hilbert symbols, this product is equal to 1, so we have $[a, b, c] = [a, c, b]$, as desired. As we can trivially swap a and b in $[a, b, c]$, this shows that the Rédei symbol is perfectly symmetric in its 3 arguments.

The linearity of $[a, b, c]$ in c is clear from its description as a product of Artin symbols $[a, b, c]_p$ of order 2 at the primes $p|c$. It must therefore be linear in all arguments. $\qquad\square$

COROLLARY 8·2. *The value of the symbol $[a, b, c]$ in (44) is the same for all $K \subset F_{a,b}$ that are minimally ramified over $\mathbf{Q}(\sqrt{a}, \sqrt{b})$.*

Proof. By Theorem 1·1, the symbol is equal to $[a, c, b]$, which is defined independently of a choice $K \subset F_{a,b}$.

One can of course also prove this directly: by Lemma 7·7, two F's that are minimally ramified over $\mathbf{Q}(\sqrt{a}, \sqrt{b})$ differ by a twist $t \in T_{a,b}$, and twisting $F = F_{a,b}$ in (44) changes the value of $[a, b, c]$ by $\chi_t(c)$, which equals 0 for $t \in T_{a,b}$ by the conditions (1) and (2). $\qquad\square$

Even though the symbol $[a, b, c]$ itself is independent of the choice of F in (7·8), its p-parts $[a, b, c]_{F,p}$ in (46) *do* depend on the minimally ramified extension $K \subset F$.

It is also possible to define $[a, b, c]$ as an Artin symbol in an abelian extension $K \subset \mathcal{F}_{a,b}$ that is uniquely defined in terms of a and b. For any minimally ramified extension $K \subset F$ as in (33), we can take the compositum

$$\mathcal{F}_{a,b} = F G_{a,b},$$

of F with the multiquadratic extension $G_{a,b}$ obtained by adjoining the square roots $\sqrt{t}$ of the elements $t \in T_{a,b}$ from (43). By Lemma 7·7, the number field $\mathcal{F}_{a,b}$ is the compositum of *all* minimally ramified extensions $K \subset F$, so it is uniquely defined in terms of a and b. We now replace $F_{a,b}$ by $\mathcal{F}_{a,b}$ in (44) and define the Rédei symbol $[a, b, c] \in \mathrm{Gal}(\mathcal{F}_{a,b}/G_{a,b}) = \mathbf{F}_2$ as

$$[a, b, c] = \mathrm{Art}_c(\mathcal{F}_{a,b}/K) = \begin{cases} \mathrm{Art}(\mathfrak{c}, \mathcal{F}_{a,b}/K) & \text{if} \quad c > 0; \\ \mathrm{Art}(\mathfrak{c}\infty, \mathcal{F}_{a,b}/K) & \text{if} \quad c < 0. \end{cases} \tag{52}$$

Although Definition (52) is in many ways the 'correct' definition of $[a, b, c]$, it has the psychological disadvantage of being defined using a field $\mathcal{F}_{a,b}$ that is potentially very large.

For the proof of the reciprocity of the symbol, and for actual computations of Rédei symbols, the p-parts of $[a, b, c]$, which are simply Legendre symbols in quadratic fields such as $K_a = \mathbf{Q}(\sqrt{a})$ by (47), are handled more easily.

9. *Governing fields*

An immediate application of Rédei's reciprocity law in the form we have stated it is the existence of *governing fields* for the 8-rank of the narrow class group $C(dp)$ of the quadratic field $\mathbf{Q}(\sqrt{dp})$, with d a fixed squarefree integer and p a variable prime. By this, we mean that there exists a normal number field $\Omega_{8,d}$ with the property that for primes p, $p' \nmid d$ that are coprime to its discriminant and have the same Frobenius conjugacy class in $\text{Gal}(\Omega_{8,d}/\mathbf{Q})$, the groups $C(dp)/C(dp)^8$ and $C(dp')/C(dp')^8$ are isomorphic.

Theorem 2·1 trivially implies that $\Omega_{2,d} = \mathbf{Q}(i)$ is a governing field for the 2-rank of $C(dp)$. By the explicit form (16) of Theorem 3·1, we can take the multi-quadratic field

$$\Omega_{4,d} = \mathbf{Q}(i, \{\sqrt{p} : p|d \text{ prime}\})$$

as a governing field for the 4-rank of $C(dp)$.

Now suppose p and p' are primes that are unramified in $\Omega_{4,d}$ and have the same Artin symbol in $\text{Gal}(\Omega_{4,d}/\mathbf{Q})$. Then the Rédei matrices R_4 and R_4' for $C(dp)$ and $C(dp')$ as given in (16) *coincide* if the primes in dp and dp' are numbered in the obvious compatible way. This implies that the 8-rank maps in (22) can be described by matrices R_8 and R_8' for $C(dp)$ and $C(dp')$ with entries given by (23) that may be compared 'entry-wise'. In other words, every entry $[d_1, d_2, m]$ from Definition 4·4 in the matrix R_8 for $D = d_1 d_2 \in \{dp, 4dp\}$ corresponds to a Rédei symbol $[d_1', d_2', m']$ for R_8' in which the arguments are obtained by replacing every prime factor p in the entries of $[d_1, d_2, m]$ by the factor p'.

Possibly switching the role of d_1 and d_2, we may assume that all symbols $[d_1, d_2, m]$ in R_8 have $p \nmid d_1$. Moreover, if we have $p|m$ in a symbol $[d_1, d_2, m]$, we can add the trivial symbol $[d_1, d_2, -d_1 d_2]$ from Proposition 7·10 to it to rewrite it as a symbol

$$[d_1, d_2, m] = [d_1, d_2, -d_1 d_2/m] = [d_1, d_2, dp/m] \tag{1}$$

with $p \nmid (dp/m)$. Thus, we may write the entries of R_8 as $[d_1, d_2, m]$ with $p \nmid d_1 m$. Then the entries of R_8' become $[d_1', d_2', m'] = [d_1, d_2', m]$.

In order to show that the value of $[d_1, d_2, m]$ for $p \nmid d_1 m$ is governed by the splitting behavior of p in some finite extension of $\Omega_{4,d}$, it suffices to rewrite it using Theorem 1·1 as

$$[d_1, d_2, m] = [d_1, m, d_2],$$

and observe that we now have $[d_1, m, d_2] = [d_1, m, d_2']$ for $d_2' = p'd_2/p$ whenever p and p' have the same splitting behaviour in $\Omega_{4,d}(\sqrt{\mu})$, with $\mu \in \mathbf{Q}(\sqrt{d_1})$ an element with norm in $m \cdot \mathbf{Q}^{*2}$ that generates a minimally ramified extension of $K = \mathbf{Q}(\sqrt{md_1})$ as in (33) for $(a, b) = (d_1, m)$. Note that $\Omega_{4,d} \subset \Omega_{4,d}(\sqrt{\mu})$ is unramified outside $2d$.

Taking $\Omega_{8,d}$ to be the compositum of the fields $\Omega_{4,d}(\sqrt{\mu})$ arising for each of the entries $[d_1, d_2, m]$ of R_8, we see that R_8 and R_8' coincide for primes p, p' having the same Frobenius conjugacy class in $\text{Gal}(\Omega_{8,d}/\mathbf{Q})$. We arrive at the following theorem, which was proved in a more involved way in 1988 in [20]. The short proof we gave above already occurs in [5].

THEOREM 9·1. *A governing field $\Omega_{8,d}$ for the 8-rank of $C(dp)$ exists, and one can take for it the maximal exponent 2 extension of $\Omega_{4,d}$ unramified outside $2d$.* □

The existence of $\Omega_{8,d}$ implies, by the Chebotarev density theorem, that we can compute the density of the set of primes p for which $C(dp)$ has prescribed 2-, 4- and 8-rank. Cohn and Lagarias [4] conjectured in 1983 that such governing fields Ω_{2^k} should exist for the 2^k-rank of $C(dp)$ for all $k \geq 1$. Recent work of Milovic and Koymans [10, 11] establishes density results for 16-ranks of class groups $C(dp)$ with cyclic 2-part, such as $C(-2p)$, with error terms that are "too good" to come from a governing field, making it unlikely that the conjecture holds for 2^k-ranks with $k \geq 4$. Smith [19] nevertheless arrives at proving *average* distributions for higher 2^k-ranks by 'governing less', focusing not on individual quadratic fields K but on their related behavior in well-chosen families.

10. *The negative Pell equation*

By (20), proving Conjecture 3·2 entails controlling the archimedean character of the full narrow Hilbert class field H of $K = \mathbf{Q}(\sqrt{D})$ for the discriminants D in the thin set $\mathcal{D}$ of discriminants for which the genus field H_2 is totally real. The 4-Hilbert class field H_4 of K can be given explicitly, in the sense of Corollary 7·4, as a compositum of cyclic quartic extensions $K \subset F_{d_1,d_2}$ that are unramified over the fields $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$, with $D = d_1 d_2$ ranging over (a basis of) the decompositions of D of the second kind, as characterized in Lemma 4·2. By Definition 7·8, the archimedean character of the dihedral field F_{d_1,d_2} is given by the Rédei symbol $[d_1, d_2, -1] = \mathrm{Art}(\infty, F_{d_1,d_2}/K)$, which is defined since $d_1, d_2 \in \mathcal{D}$ satisfy $(d_1, -1)_p = (d_2, -1)_p = 1$ for all p.

THEOREM 10·1. *Let $D = d_1 d_2$ be a decomposition of the second kind for $D \in \mathcal{D}$, and $K \subset F_{d_1,d_2}$ a corresponding unramified extension as in (1) of Lemma 4·2. Then F_{d_1,d_2} is totally real if and only if we have*

$$[d_1, d_2, -1] = \left(\frac{d_1}{d_2}\right)_4 + \left(\frac{d_2}{d_1}\right)_4 = 0 \in \mathbf{F}_2.$$

Proof. Add to $[d_1, d_2, -1]$ the symbol $[d_1, d_2, -d_1 d_2] = 0$ from Proposition 7·10, and use the linearity and reciprocity properties of the Rédei symbol together with the special case in Definition 7·1 to obtain the desired equality

$$[d_1, d_2, -1] = [d_1, d_2, d_1 d_2] = [d_1, d_2, d_1] + [d_1, d_2, d_2]$$
$$= [d_1, d_1, d_2] + [d_2, d_2, d_1] = \left(\frac{d_2}{d_1}\right)_4 + \left(\frac{d_1}{d_2}\right)_4. \qquad \square$$

Theorem 10·1 was already known to Rédei, but his symbol 'without infinite primes' cannot be used to give the short proof above. A long proof can be found in [6, pp. 2061–2064].

Theorem 10·1 implies that H_4 is totally real if and only if all Rédei symbols $[d_1, d_2, -1]$ corresponding to r_4 decompositions $D = d_1 d_2$ of the second kind spanning $\widehat{C}[2] \cap 2\widehat{C}$ vanish. The explicit form of the symbol as a sum of two biquadratic symbols was used by Fouvry and Klüners [6] to show that these r_4 different Rédei symbols vanish for the expected fraction 2^{-e} of all discriminants in the subset $\mathcal{D}(e) \subset \mathcal{D}$ of D having $r_4 = e$. As $\mathcal{D}(e)$ has density $P(e)$ in $\mathcal{D}$, a short calculation [21, corollary 4·4] involving the explicit values following equation (21) shows that the density of $D \in \mathcal{D}$ with H_4 totally real equals

$$\sum_{e=0}^{\infty} 2^{-e} P(e) = \sum_{e=0}^{\infty} 2^{-e} \cdot \alpha \cdot \prod_{j=1}^{e} (2^j - 1)^{-1} = \frac{2}{3}.$$

In the direction of Conjecture 3·2, this yields an upper density $\overline{P} \le \frac{2}{3} \approx .667$ for the subset $\mathcal{D}^-$ of $\mathcal{D}$.

For discriminants $D \in \mathcal{D}$ having $r_8 = 0$, the necessary condition for $D \in \mathcal{D}^-$ that H_4 be totally real is also sufficient, and this gives rise to lower bounds. Discriminants in $\mathcal{D}(0)$ trivially have $r_8 = r_4 = 0$, and the inclusion $\mathcal{D}(0) \subset \mathcal{D}^-$ yields the lower bound $P(0) = \alpha \approx .419$ from (21) for the lower density $\underline{P}$ of $\mathcal{D}^-$ in $\mathcal{D}$ that we already mentioned at the end of Section 3.

Discriminants $D \in \mathcal{D}(1)$ have a unique non-trivial decomposition $D = d_1 d_2$ of the second kind, and the kernel of the symmetric matrix R_4 is spanned by the discriminantal divisors d_1 and d_2. In this case Rédei reciprocity for the special symbols in Definition 7·1 shows that R_8 has a matrix representation

$$R_8 = \left([d_1, d_2, d_1] \, [d_1, d_2, d_2] \right) = \left(\left(\frac{d_2}{d_1} \right)_4 \quad \left(\frac{d_1}{d_2} \right)_4 \right)$$

in terms of biquadratic symbols. In view of Theorems 4·1 and 10·1, having $r_8 = 0$ and H_4 totally real now amounts to

$$\left(\frac{d_2}{d_1} \right)_4 = \left(\frac{d_1}{d_2} \right)_4 = 1 \in \mathbf{F}_2, \tag{1}$$

and, again, for the expected fraction $1/4$ of discriminants in $\mathcal{D}(1)$, both biquadratic symbols are non-trivial [7]. This yields $P(0) + (P(1))/4 = 5/4\alpha \approx .524$ as a lower bound for the lower density $\underline{P}$.

For discriminants $D \in \mathcal{D}(e)$ with $e \ge 2$, the Rédei symbols in the matrix R_8 are not restricted to biquadratic symbols, but Chan, Koymans, Milovic and Pagano [3] show that they can still be 'governed' by an adaptation of the methods in Smith's recent work [18, 19]. They prove that the density of discriminants $D \in \mathcal{D}$ of 4-rank $r_4 = e$ for which $r_8 = 0$ and H_4 is totally real equals $2^{-e(e+3)/2} \cdot \alpha$, extending the trivial case $e = 0$ and the special case $e = 1$ above. This improves the lower bound $\alpha + \alpha/4$ above to $\sum_{e=0}^{\infty} 2^{-e(e+3)/2} \cdot \alpha$. Thus, the published state of affairs towards Conjecture 3·2, which claims $\underline{P} = \overline{P} = 1 - \alpha = .581$, becomes

$$.538 \approx \sum_{e=0}^{\infty} 2^{-e(e+3)/2} \cdot \alpha \ \le \ \underline{P} \ \le \ \overline{P} \ \le \ 2/3 \approx .667.$$

Improving these bounds involves dealing with the remaining 12.8% of discriminants $D \in \mathcal{D}$ having $r_8 > 0$. As this article goes to press (March 2021), Koymans and Pagano have announced that they have been able to extend Smith's techniques [19] to also control these discriminants, and to prove my full Conjecture 3·2 after almost 30 years.

REFERENCES

[1] D. Boneh and A. Silverberg. *Applications of multilinear forms to cryptography*. Topics in algebraic and noncommutative geometry (Luminy/Annapolis, MD, 2001). *Contemp. Math.* vol. 324 (Amer. Math. Soc., Providence, RI, 2003), pp. 71–90.

[2] W. Bosma and P. Stevenhagen. Density computations for real quadratic units. *Math. Comp.* **65** (1996), no. 215, 1327–1337.

[3] S. Chan, P. Koymans, D. Milovic and C. Pagano. On the negative Pell equation, arXiv:1908.01752v1 (2019).

[4] H. Cohn and J. C. Lagarias. On the existence of fields governing the 2-invariants of the classgroup of $\mathbf{Q}(\sqrt{dp})$ as p varies, *Math. Comp.* **41** (1983), no. 164, 711–730.

[5] J. Corsman. Rédei symbols and governing fields. ProQuest LLC, Ann Arbor, MI, 2007. PhD thesis McMaster University (Canada).

[6] É. FOUVRY and J. KLÜNERS. On the negative Pell equation. *Ann. of Math.* (2) **172** (2010). no. 3, 2035–2104.

[7] É. FOUVRY and J. KLÜNERS. The parity of the period of the continued fraction of $\sqrt{d}$, *Proc. Lond. Math. Soc.* (3) **101** (2010), no. 2, 337–391.

[8] J. GÄRTNER. Rédei symbols and arithmetical mild pro-2-groups. *Ann. Math. Qué.* **38** (2014), no. 1, 13–36 (English, with English and French summaries).

[9] H. W. LENSTRA JR. Solving the Pell equation. Algorithmic number theory: lattices, number fields, curves and cryptography. *Math. Sci. Res. Inst. Publ.*, vol. 44 (Cambridge Univerity Press, Cambridge, 2008) pp. 1–23.

[10] D. MILOVIC. On the 16-rank of class groups of $\mathbf{Q}(\sqrt{-8p})$ for $p \equiv -1 \bmod 4$, *Geom. Funct. Anal.* **27** (2017), no. 4, 973–1016.

[11] P. KOYMANS and D. Z. MILOVIC. Spins of prime ideals and the negative Pell equation $x^2 - 2py^2 = -1$. *Composition Math.* **155** (2019), no. 1, 100–125.

[12] J. MINÁČ and N. DUY TÂN. Construction of unipotent Galois extensions and Massey products. *Adv. Math.* **304** (2017), 1021–1054.

[13] M. MORISHITA. *Knots and Primes* (Universitext, Springer, London, 2012). An introduction to arithmetic topology.

[14] L. RÉDEI and H. REICHARDT. Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers *J. Reine Angew. Math.* **170** (1934), 69–74.

[15] L. RÉDEI. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.* **171** (1934), 55–60.

[16] L. RÉDEI. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I. *J. Reine Angew. Math.* **180** (1939), 1–43.

[17] G. J. RIEGER. Über die Anzahl der als Summe von zwei Quadraten darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke. *J. Reine Angew. Math.* **217** (1965), 200–216.

[18] A. SMITH. Governing fields and statistics for 4-Selmer groups and 8-class groups, ArXiv:1607.07860 (2016), 1–29.

[19] A. SMITH. 2∞-Selmer groups, 2∞-class groups, and Goldfeld's conjecture, ArXiv:1702.02325 (2017), 1–72.

[20] P. STEVENHAGEN. Ray class groups and governing fields, Théorie des nombres, Année 1988/89, Fasc. 1, *Publ. Math. Fac. Sci.* (Besançon, Univ. Franche-Comté, Besançon, 1989), pp. 1–93.

[21] P. STEVENHAGEN. The number of real quadratic fields having units of negative norm. *Experiment. Math.* **2** (1993), no. 2, 121–136. MR1259426

[22] P. STEVENHAGEN. On a problem of Eisenstein. *Acta Arith.* **74** (1996), no. 3, 259–268.