Norms of Units and 4-rank of Class Groups

Tommy Bülow

Ph.D. thesis

Defence:
December 10, 2004

Thesis advisor:
Christian U. Jensen, University of Copenhagen, Denmark

Evaluating committee:
Franz Halter-Koch, University of Graz, Austria
Ian Kiming (chairman), University of Copenhagen, Denmark
Noriko Yui, Queen's University, Canada

Institute for Mathematical Sciences · University of Copenhagen · 2004

Tommy Bülow
Department of Mathematics
University of Copenhagen
Universitetsparken 5
2100 Copenhagen Ø
Denmark
tommy@math.ku.dk

ISBN 87-7834-619-3

Preface

This is my Ph.D. thesis in mathematics at the University of Copenhagen. The thesis is based on the following three papers:

[2] T. Bülow: Power Residue Criteria for Quadratic Units and the Negative Pell Equation, Canad. Math. Bull Vol. 46 (1), 2003, 39-53;

[3] T. Bülow: Relative Norms of Units and 4-rank of Class Groups (submitted);

[4] T. Bülow: 4-rank of the Class Group of Certain Biquadratic Number Fields of Dirichlet Type (preprint).

The structure of the thesis is as follows:

The first introductory chapter deals with the classical negative Pell equation and indicates two possible ways to continue the classical theory. These matters are investigated in parts I and II.

In part I, which consists of the chapters 2 and 3, power residue criteria for units of real quadratic fields are proved by means of class field theory. Part I is based on [2].

Part II, which consists of the chapters 4 and 5, deals with the surjectivity of the relative norm map $N_{L/K}$ restricted to unit groups (for certain extensions L/K of number fields). It turns out that this question is related to concepts which also influence the structure of the (2–)class group of L, especially the 4–rank of the class group of L. For certain fields, the 4–rank of the class group is also studied for its own sake. Part II is based on [3] and [4].

The class field theory that will be used is summarized in an appendix.

I would like to thank my thesis advisor professor Christian U. Jensen, who was also my master's thesis advisor, warmly for being an excellent advisor over the years. He has been a great inspiration and I am glad that he introduced me to the interesting theory of the classical negative Pell equation.

Tommy Bülow

Contents

Notation

We list some of the notation that will be used.

$\mathbb{Z}$ is the set of rational integers;
$\mathbb{N}$ is the set of positive integers;
$\mathbb{N}_0$ is the set of non-negative integers;
$\mathbb{Q}$ is the field of rational numbers;
$\mathbb{R}$ is the field of real numbers;
$\mathbb{C}$ is the field of complex numbers;
$\mathbb{F}_q$ is the finite field with q elements where q is a prime power.
$N_{L/K}$ is the relative norm map for an extension L/K of number fields;
$N(\cdot)$ is the absolute norm map;
Let K be a number field; then:
  $\mathcal{O}_K$ is the ring of integers of K;
  $\mathcal{O}_K^*$ is the group of units in $\mathcal{O}_K$;
  $Cl(K)$ is the class group;
  $h(K)$ is the class number;
  $[\mathfrak{a}]_K$ is the ideal class in $Cl(K)$ containing the fractional ideal $\mathfrak{a}$ of K;
$\vee$ is the logical 'or';
$\wedge$ is the logical 'and';
$||$ means 'divides exactly' (for prime powers);
$\left(\frac{D}{p}\right)$ is the Legendre symbol (or the Kronecker symbol).

Chapter 1

Introduction

1.1 The Classical Negative Pell Equation

Let D be a non-square positive integer. The problem of deciding whether the negative Pell equation

$$x^2 - Dy^2 = -1, \tag{1.1}$$

has integral solutions is a classical problem in number theory which is not solved in general. Obvious necessary conditions for the solvability of (1.1) are that $4 \nmid D$ and that every odd prime factor of D is congruent to 1 modulo 4; they are *not* sufficient.

Consider two indefinite integral binary quadratic forms of positive discriminant: $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$. Then f and g are called equivalent if there is a matrix $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in GL_2(\mathbb{Z})$ such that $f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y)$; if this holds and $A \in SL_2(\mathbb{Z})$, then f and g are called *properly* equivalent (these matters where studied by Gauss). The discriminant of f is $b^2 - 4ac$. If we consider forms of fixed positive non-square discriminant D, then it is known that

$$\text{proper equivalence} = \text{equivalence} \quad \Leftrightarrow \quad x^2 - Dy^2 = -4 \text{ is solvable.}$$

If $4 \nmid D$, then these two statements are true if and only if $x^2 - Dy^2 = -1$ is solvable.

Many mathematicians have made sporadic contributions to the problem about the solvability of (1.1). Fermat, Euler and Galois were some of the first to study the equation systematically.

First, suppose that D is square-free.

Dirichlet [5] proved the following result by elementary means (quadratic reciprocity and simple considerations about biquadratic residues).

Theorem 1.1. *Let p_1, p_2, p_3 be distinct primes $\equiv 1 \pmod 4$. If D is equal to one of the following, the equation $x^2 - Dy^2 = -1$ is solvable:*

1. *D=p_1;*
2. *D=$2p_1$, where $p_1 \equiv 5 \pmod 8$;*
3. *D=$2p_1$, where $p_1 \equiv 9 \pmod{16}$ and $\left(\frac{2}{p_1}\right)_4 = -1$;*[1]
4. *D=p_1p_2, where $\left(\frac{p_1}{p_2}\right) = -1$;*
5. *D=p_1p_2, where $\left(\frac{p_1}{p_2}\right) = 1$ and $\left(\frac{p_1}{p_2}\right)_4 = \left(\frac{p_2}{p_1}\right)_4 = -1$;*
6. *D=$p_1p_2p_3$, where at least two of $\left(\frac{p_1}{p_2}\right), \left(\frac{p_2}{p_3}\right), \left(\frac{p_3}{p_1}\right)$ are =-1;*
7. *D=$p_1p_2p_3$, where $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_3}{p_1}\right) = 1$ and $\left(\frac{p_2}{p_3}\right) = \left(\frac{p_2p_3}{p_1}\right)_4 = \left(\frac{p_1}{p_2}\right)_4 = \left(\frac{p_1}{p_3}\right)_4 = -1$;*
8. *D=$p_1p_2p_3$, where $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_3}\right) = \left(\frac{p_3}{p_1}\right) = 1$ and $\left(\frac{p_2p_3}{p_1}\right)_4 = \left(\frac{p_1p_3}{p_2}\right)_4 = \left(\frac{p_1p_2}{p_3}\right)_4 = \left(\frac{p_1}{p_2}\right)_4\left(\frac{p_1}{p_3}\right)_4 = \left(\frac{p_2}{p_1}\right)_4\left(\frac{p_2}{p_3}\right)_4 = \left(\frac{p_3}{p_1}\right)_4\left(\frac{p_3}{p_2}\right)_4 = -1$.*

More recent results about the negative Pell equation can be found in [6], [23], [24], [25].

We now turn to the connection between the solvability of the negative Pell equation and class field theory.

From now on, we use the class field theory and the notation in appendix A.

Let K be a number field.

Consider the ideal group $S_{(1)}$ in K; let L_1 be the corresponding abelian extension of K (cf. theorem A.9). Then $\mathfrak{f}_{L_1/K} = (1)$, so that (cf. theorem A.6) $S_{(1)}$ is an ideal group corresponding to L_1. We have

$$Gal(L_1/K) \simeq A_{(1)}/S_{(1)}.$$

Since any unramified (including at infinity) abelian extension of K has conductor (1), so that its corresponding ideal group contains $S_{(1)}$, A.11 implies that

$$L_1 = \text{the maximal unramified (including at infinity) abelian extension of } K.$$

[1] Let $a \in \mathbb{Z}$ and let p be an odd prime number; in this paper we use $\left(\frac{a}{p}\right)_4$ only in the following sense: if $\left(\frac{a}{p}\right) = 1$, then $\left(\frac{a}{p}\right)_4 = \begin{cases} 1, & \textit{if a is a 4th power residue mod p} \\ -1, & \textit{if a is not a 4th power residue mod p} \end{cases}$.

L_1 is the *Hilbert class field of* K.
Let ∞ be the divisor of K which is the product of the real embeddings of K. Let L_2 be the abelian extension of K corresponding to S_∞. Then $\mathfrak{f}_{L_2/K} \mid \infty$, so that S_∞ is an ideal group corresponding to L_1. We have

$$Gal(L_2/K) \simeq A_{(1)}/S_\infty.$$

$A_{(1)}/S_\infty$ is the *strict class group of* K. Since any finitely unramified abelian extension of K has a conductor dividing ∞, so that its corresponding ideal group contains S_∞, we have that

$$L_2 = \text{the maximal finitely unramified abelian extension of } K.$$

L_2 is the *strict Hilbert class field of* K.
Clearly, $L_1 \subseteq L_2$ and $L_1 = L_2 \Leftrightarrow S_{(1)} = S_\infty$.

Let p be a prime number. For a finite abelian group G, let $Syl_p(G)$ denote the p–Sylow group of G.

Let $L_1^{(p)}$ be the abelian extension of K corresponding to H_1 where

$$A_{(1)}/S_{(1)} = Syl_p(A_{(1)}/S_{(1)})H_1/S_{(1)}.$$

Let $L_2^{(p)}$ be the abelian extension of K corresponding to H_2 where

$$A_{(1)}/S_\infty = Syl_p(A_{(1)}/S_\infty)H_2/S_\infty.$$

($H_1/S_{(1)}$ (resp. H_2/S_∞) is the product of the other Sylow groups in $A_{(1)}/S_{(1)}$ (resp. $A_{(1)}/S_\infty$).) We have

$$Gal(L_1^{(p)}/K) \simeq A_{(1)}/H_1 \simeq A_1/S_{(1)}\Big/H_1/S_{(1)} \simeq Syl_p(A_{(1)}/S_{(1)}),$$

$$L_1^{(p)} = \text{maximal unramified (including at infinity) abelian } p-\text{extension of } K$$

$$Gal(L_2^{(p)}/K) \simeq A_{(1)}/H_2 \simeq A_1/S_\infty\Big/H_1/S_\infty \simeq Syl_p(A_{(1)}/S_\infty)$$

and

$$L_2^{(p)} = \text{the maximal finitely unramified abelian } p-\text{extension of } K.$$

$L_1^{(p)}$ is called the *p–class field of* K; $L_2^{(p)}$ is the *strict p–class field of* K. It is clear that $L_1^{(p)} \subseteq L_2^{(p)}$.
$Syl_p(A_{(1)}/S_{(1)})$ is called the *p–class group of* K; $Syl_p(A_{(1)}/S_\infty)$ is the *strict p–class group of* K.

Suppose that $K \subseteq \mathbb{R}$. Then $L_1 \subseteq \mathbb{R}$ (since L_1/K is unramified at infinity) and $L_1^{(p)} \subseteq \mathbb{R}$ (since $L_1^{(p)}/K$ is unramified at infinity). Moreover, it is clear that

$$L_2 \subseteq \mathbb{R} \;\Leftrightarrow\; L_2/K \text{ is unramified at infinity } \;\Leftrightarrow\; L_1 = L_2 \;\Leftrightarrow\; S_{(1)} = S_\infty.$$

Suppose further that $K = \mathbb{Q}(\sqrt{D})$ where $D > 1$ is a square-free integer, and let ε_D be the fundamental unit (> 1) of K. Then it is easily seen that $S_{(1)} = S_\infty \Leftrightarrow N(\varepsilon_D) = -1$ (N is the norm). If, in addition, $p = 2$, then

$$\begin{aligned} L_2^{(2)} \subseteq \mathbb{R} &\Leftrightarrow L_2^{(2)} \text{ is unramified at infinity} \\ &\Leftrightarrow L_1^{(2)} = L_2^{(2)} \\ &\Leftrightarrow Syl_2(A_{(1)}/S_{(1)}) \simeq Syl_2(A_{(1)}/S_\infty) \\ &\Leftrightarrow |A_{(1)}/S_{(1)}| = |A_{(1)}/S_\infty| \\ &\Leftrightarrow S_{(1)} = S_\infty \end{aligned}$$

(we used that $|A_{(1)}/S_{(1)}|$ and $|A_{(1)}/S_\infty|$ differ by a factor 1 or 2).

These observations are summarized in the following

Proposition 1.2. *Let $D > 1$ be a square-free integer. The following statements are equivalent:*

1. *$x^2 - Dy^2 = -1$ is solvable;*
2. *$x^2 - Dy^2 = -4$ is solvable;*
3. *$N(\varepsilon_D) = -1$;*
4. *$S_{(1)} = S_\infty$;*
5. *the strict Hilbert class field of $\mathbb{Q}(\sqrt{D})$ is real;*
6. *the strict Hilbert class field of $\mathbb{Q}(\sqrt{D})$ = the Hilbert class field of $\mathbb{Q}(\sqrt{D})$;*
7. *the strict 2–class field of $\mathbb{Q}(\sqrt{D})$ is real;*
8. *the strict 2–class field of $\mathbb{Q}(\sqrt{D})$ = the 2–class field of $\mathbb{Q}(\sqrt{D})$.*

In [27], class field theory in connection with the criteria in Proposition 1.2 (especially those involving 2–class fields) was used to prove the next result about the case where D has two prime factors (supplementing Dirichlet).

Theorem 1.3. *1) If $D = p_1p_2$ where p_1, p_2 are distinct primes $\equiv 1 \pmod 4$ with $\left(\frac{p_1}{p_2}\right) = 1$ and $\left(\frac{p_1}{p_2}\right)_4 = -\left(\frac{p_2}{p_1}\right)_4$, then $x^2 - Dy^2 = -1$ is not solvable.*

2) If D=2p where p is a prime $\equiv 1 \pmod{16}$ with $\left(\frac{2}{p}\right)_4 = -1$, then $x^2 - Dy^2 = -1$ is not solvable.

1.2 D Not Square-free and Power Residues of Units

In this section, we consider the negative Pell equation $x^2 - Dy^2 = -1$ with D *not* square-free, and we discuss its relation to certain power residues of units of quadratic fields which will be the main topic of part I of this thesis.

We write (uniquely) $D = dk^2$ with $d > 1$ square-free and $k > 1$.

First we give a formulation of the problem in terms of class field theory: Consider the two ideal groups in $K := \mathbb{Q}(\sqrt{d})$:

$$H' := \{(\alpha) \in A_{(k)}(K) \mid \exists r \in \mathbb{Q} : \alpha \equiv r \pmod{(k)}\} \quad \textit{and}$$

$$H'' := \{(\alpha) \in A_{(k)}(K) \mid \exists r \in \mathbb{Q} : \alpha \equiv r \pmod{(k)\infty}\};$$

(k) (resp. $(k)\infty$) is clearly a congruence module for H' (resp. H''); ∞ is, as before, the divisor of K which is the product of the real embeddings of K. Let L' (resp. L'') be the abelian extension of K corresponding to H' (resp. H''). By definition of infinite ramification, $L' \subseteq \mathbb{R}$. It is also clear that $H' \supseteq H''$. Then we have the following analogue of proposition 1.2:

Proposition 1.4. *The following three conditions are equivalent.*

1. $x^2 - dk^2y^2 = -4$ *is solvable.*

2. $H' = H''$.

3. $L'' \subseteq \mathbb{R}$

If $2 \nmid k$, *these conditions are equivalent to*

4. $x^2 - dk^2y^2 = -1$ *is solvable.*

Proof. For $\beta \in K$ let β' denote the conjugate.

'1. $\Rightarrow$ 2.': Let $a^2 - dk^2b^2 = -4$, $a, b \in \mathbb{N}$, and consider the units

$$\varepsilon = \frac{a + kb\sqrt{d}}{2}, \ \varepsilon' = \frac{a - kb\sqrt{d}}{2} \in \mathcal{O}_K$$

which have opposite signs. If $(\alpha) \in H'$, $r \in \mathbb{Q}$, and $\alpha \equiv r \pmod{k}$, then (by adding a suitable integral multiple of k to r, if necessary) we can assume that r and α have the same sign, and so

$$\alpha \equiv r \pmod{k\infty} \quad \text{or} \quad \varepsilon\alpha \equiv \frac{a}{2}r \pmod{k\infty}.$$

Hence $(\alpha) \in H''$. It follows that $H' = H''$.

‘2. $\Rightarrow$ 1.’: Assume that $H' = H''$. Put $\alpha := 1 + k\sqrt{d}$; then $(\alpha) \in H' = H''$. Then there is a unit $\varepsilon \in \mathcal{O}_K$ and (a rational number and (after multiplication by a suitable power of its denominator) also) an integer g such that $\varepsilon\alpha \equiv g \pmod{k\infty}$. As, in particular, $\varepsilon\alpha/g, \varepsilon'\alpha'/g > 0$, we have

$$N(\varepsilon) = \frac{\varepsilon\alpha}{g}\frac{\varepsilon'\alpha'}{g}\frac{g^2}{N(\alpha)} < 0,$$

and so $N(\varepsilon) = -1$.
We can write $\varepsilon = \frac{a+b\sqrt{d}}{2}, a, b \in \mathbb{Z}$; then

$$2g \equiv 2\varepsilon\alpha = a + b\sqrt{d} + 2k\sqrt{d}\varepsilon \equiv a + b\sqrt{d} \pmod{2k}.$$

Hence $k \mid b$, and so we get $\quad -4 = 4N(\varepsilon) = a^2 - dk^2\left(\frac{b}{k}\right)^2$.

‘2. $\Rightarrow$ 3.’: $H' = H'' \;\Rightarrow L'' = L' \subseteq \mathbb{R}$.

‘3. $\Rightarrow$ 1.’: Suppose that $L'' \subseteq \mathbb{R}$, i.e. $\mathfrak{f}_{L''/K}$ is an integral ideal. Therefore, we can choose $n \in \mathbb{N}$ with $\mathfrak{f}_{L''/K} \mid (n)$. Hence $S_{(nk)} \subseteq H''$. Put $\alpha := 1 + nk\sqrt{d}$. Since $(\alpha) \in S_{(nk)} \subseteq H''$, there is a unit $\varepsilon \in \mathcal{O}_K$ and an integer $g \in \mathbb{Z}$ with

$$\varepsilon\alpha \equiv g \pmod{k\infty}.$$

As $\frac{\varepsilon\alpha}{g}, \frac{\varepsilon'\alpha'}{g} > 0$, we have

$$N(\varepsilon)\frac{N(\alpha)}{g^2} = \frac{\varepsilon\alpha}{g} \cdot \frac{\varepsilon'\alpha'}{g} > 0,$$

and so $N(\varepsilon) = -1$. From $\varepsilon \equiv \varepsilon\alpha \equiv g \pmod{k}$ we find that

$$\varepsilon - g = k\frac{x + y\sqrt{d}}{2}, x, y \in \mathbb{Z};$$

hence $\quad -4 = N(2\varepsilon) = (kx + 2g)^2 - dk^2y^2$.

To finish the proof we note that $2 \nmid k$ implies that $4 \nmid dk^2$; so if $2 \nmid k$, then $x^2 - dk^2y^2 = -1$ is solvable if and only if $x^2 - dk^2y^2 = -4$ is solvable. □

A necessary condition for the solvability of $x^2 - dk^2y^2 = -1$ is, of course, that $x^2 - dy^2 = -1$ has a solution. Hence it is also necessary that k is odd and that every odd prime dividing dk is $\equiv 1 \pmod 4$. By the next proposition (from [15]) one can assume that k is a prime $\equiv 1 \pmod 4$.

Proposition 1.5. [2] *Let $d > 1$ be square-free and let the odd number k have the prime decomposition $k = \prod_i p_i^{\nu_i}$. Then*

$$x^2 - dk^2y^2 = -1 \text{ is solvable } \Leftrightarrow \forall i: \; x^2 - dp_i^2y^2 = -1 \text{ is solvable.}$$

So it is enough to deal with the equation $x^2 - dp^2y^2 = -1$ where $d > 1$ is square-free and p is a prime $\equiv 1 \pmod 4$. We shall assume that $p \nmid d$.

First we settle the case $\left(\frac{d}{p}\right) = -1$ completely.

We shall need the following result from genus theory.

Lemma 1.6. *Let K be a quadratic number field where $p_1, \ldots, p_w$ are the (distinct) prime factors of the discriminant of K. Let $\mathfrak{p}_i$ be the prime ideal in K above p_i. The square of each $\mathfrak{p}_i$ is (of course) a principal ideal with a generator of positive norm. Moreover,*

1. *exactly 2 of the 2^w ideals*

$$\mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_1^{\mu_w}, \mu_i \in \{0, 1\},$$

are principal with a generator of positive norm;

2. *every fractional ideal B in K whose ideal class has order 1 or 2 (in K's class group) is strictly equivalent to one of the ideals*

$$\mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_1^{\mu_w}, \mu_i \in \{0, 1\}$$

(i.e. B differs from one of these by a principal ideal with a generator of positive norm).

Lemma 1.7. *Let $d > 1$ be square-free. Assume that $x^2 - dy^2 = -1$ has a solution. Let d_1 be a divisor of d. Then*

$$x^2 - dy^2 = d_1 \text{ is solvable } \Leftrightarrow d_1 \in \{\pm 1, \pm d\}.$$

Proof. '$\Leftarrow$': Obvious.
'$\Rightarrow$': It is enough to show that (at most) 4 divisors d_1 result in a solvable equation. Consider $\mathbb{Q}(\sqrt{d})$ whose discriminant has the same prime factors as d. Let $d = p_1 \cdots p_w$ be the prime decomposition of d and consider a divisor $d_1 = \pm \prod_{i \in B} p_i$, $B \subseteq \{1, \ldots, w\}$, of d. Let $\mathfrak{p}_i$ be the prime ideal in $\mathbb{Q}(\sqrt{d})$ above p_i. Since

$$x^2 - dy^2 = d_1 \text{ is solvable } \Leftrightarrow \prod_{i \in B} \mathfrak{p}_i \text{ is a principal ideal}$$

and since (by lemma 1.6) exactly 2 of the ideals $\mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_1^{\mu_w}, \mu_i \in \{0, 1\}$, are principal, we are done. □

[2] In [15] only an odd d is considered; however, the proof given there does not use this.

Theorem 1.8. *Let $d > 1$ be square-free. Assume that $x^2 - dy^2 = -1$ has a solution. Let $p \equiv 1 \pmod 4$ be a prime with $\left(\frac{d}{p}\right) = -1$. Then $x^2 - dp^2y^2 = -1$ is solvable.*

Proof. Assume that $x^2 - dp^2y^2 = -1$ is not solvable, and let $x, y \in \mathbb{N}$ be minimal with $x^2 - dp^2y^2 = 1$. As $dp^2 \equiv 1, 2, 5 \pmod 8$, x must be odd and y even. The integers $\frac{x+1}{2}$ and $\frac{x-1}{2}$ are coprime. From

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

we therefore get

$$\frac{x+1}{2} = d_1a_1^2 \quad \textit{and} \quad \frac{x-1}{2} = d_2a_2^2$$

where $d = d_1d_2$ and $p\frac{y}{2} = a_1a_2$. Since

$$(d_1a_1)^2 - da_2^2 = d_1(d_1a_1^2 - d_2a_2^2) = d_1,$$

lemma 1.7 implies that $d_1 \in \{\pm 1, \pm d\}$, and so $(d_1, d_2) \in \{(1, d), (d, 1)\}$. This gives 4 cases, each one being impossible:

i) $d_1 = d \wedge a_1 = pb$: $\quad a_2^2 - dp^2b^2 = -1$.

ii) $d_2 = d \wedge a_2 = pb$: $\quad a_1^2 - dp^2b^2 = 1$ and $|a_1| = \sqrt{\frac{x+1}{2}} < x$.

iii) $d_1 = d \wedge a_2 = pb$: $\quad da_1^2 - p^2b^2 = 1$; hence $\left(\frac{d}{p}\right) = 1$.

iv) $d_2 = d \wedge a_1 = pb$: $\quad da_2^2 - p^2b^2 = -1$; hence $\left(\frac{d}{p}\right) = 1$. □

This settles the case $\left(\frac{d}{p}\right) = -1$. From now on, we concentrate on the case $\left(\frac{d}{p}\right) = 1$. In this case, the following result (proved in [15] by elementary means) transforms the question of solvability of the negative Pell equation into a problem about a congruence in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Lemma 1.9. *Let $d > 1$ be square-free, let the fundamental unit $\varepsilon = \varepsilon_d$ of $\mathbb{Q}(\sqrt{d})$ have norm –1 and let $p \equiv 1 \pmod 4$ be a prime with $\left(\frac{d}{p}\right) = 1$. Suppose that $2^\lambda || p-1$. Then*

$$x^2 - dp^2y^2 = -1 \textit{ is solvable} \Leftrightarrow \varepsilon^{\frac{p-1}{2^{\lambda-1}}} \equiv -1 \pmod p \quad (\textit{in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})}).$$

If c is an integer not divisible by the odd prime p and the Legendre symbol $\left(\frac{c}{p}\right)$ has the value 1, then we define the symbol $\left(\frac{c}{p}\right)_4$ to be be 1 or -1 according as c is or is not a fourth power modulo p. If $\left(\frac{d}{p}\right) = 1$, then we can interpret ε_d as an integer modulo p and if the norm $N(\varepsilon_d)$ of ε_d is 1 or if $N(\varepsilon_d) = -1$ and $p \equiv 1 \pmod 4$, the symbol $\left(\frac{\varepsilon_d}{p}\right)$ is well-defined. When there is no risk of ambiguity we define, recursively, the symbol $\left(\frac{\varepsilon_d}{p}\right)_{2^{t+1}}$ as follows: $\left(\frac{\varepsilon_d}{p}\right)_{2^{t+1}} = 1$ (resp. $= -1$) means that $\left(\frac{\varepsilon_d}{p}\right)_{2^t} = 1$ and ε_d is (resp. is not) a 2^{t+1}th power modulo p. For our purposes it will be sufficient to know that if $N(\varepsilon_d) = 1$ or if $N(\varepsilon_d) = -1$ and $p \equiv 1 \pmod 8$, the symbol $\left(\frac{\varepsilon_d}{p}\right)_4$ is well defined.

Remark 1.10. Let $p \equiv 1 \pmod{2^\lambda}$ $(\lambda = 2, 3)$ be a prime number with $\left(\frac{d}{p}\right) = 1$ and let $\mathfrak{p}$ be one of the two prime ideals in $\mathbb{Q}(\sqrt{-d})$ above p. Then for $\lambda = 2, 3$:

$$\begin{aligned}\left(\frac{\varepsilon_d}{p}\right)_{2^{\lambda-1}} = 1 \quad &\Leftrightarrow \quad (\varepsilon_d)^{\frac{p-1}{2^{\lambda-1}}} \equiv 1 \pmod p \\ &\Leftrightarrow \quad \mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt[2^{\lambda-1}]{\varepsilon_d}, i),\end{aligned}$$

by theorem 119 in [12]. In particular, we immediately have (cf. lemma 1.9):
A) $p \equiv 5 \pmod 8$:

$$x^2 - dp^2y^2 = -1 \quad \textit{is solvable} \ \Leftrightarrow \left(\frac{\varepsilon_d}{p}\right) = -1;$$

B) $p \equiv 9 \pmod{16}$:

$$x^2 - dp^2y^2 = -1 \quad \textit{is solvable} \ \Leftrightarrow \left(\frac{\varepsilon_d}{p}\right)_4 = -1;$$

C) $p \equiv 1 \pmod{16}$:

$$x^2 - dp^2y^2 = -1 \quad \textit{is solvable} \ \Rightarrow \left(\frac{\varepsilon_d}{p}\right)_4 = 1.$$

In part I of this thesis, we concentrate on the problem of finding $\left(\frac{\varepsilon_d}{p}\right)$ and $\left(\frac{\varepsilon_d}{p}\right)_4$ for certain classes of d. As indicated by remark 1.10, power residue criteria can be interpreted in terms of the solvability of $x^2 - dp^2y^2 = -1$.

We now describe some of the known results dealing with the power residue criteria for ε_d or the solvability of $x^2 - dp^2y^2 = -1$ with p being a prime. They are almost all expressed in terms of one or two representations of powers of p by binary quadratic forms.

[8] contains several power residue criteria for ε_d being a 2^tth power residue $(t = 1, 2, 3)$ for special classes of d. A typical example is Potenzrestkriterium 1 in [8]:

Theorem 1.11. *Let $d \equiv 7 \pmod 8$, let the prime divisors q of m be $\equiv \pm 1 \pmod 8$, let the class group of $\mathbb{Q}(\sqrt{-d})$ have no invariant divisible by 4, let m be the odd part of the class number of $\mathbb{Q}(\sqrt{-d})$, let $p \equiv 1 \pmod 8$ be a prime number such that $\left(\frac{q}{p}\right) = 1$ for every prime factor q of d. Then $p^m = s^2 + 16dv^2, s, v \in \mathbb{Z}$,*
$\left(\frac{\varepsilon_d}{p}\right) = 1$ *and* $\left(\frac{\varepsilon_d}{p}\right)_4 = (-1)^v$.
If $p \equiv 1 \pmod{16}$ and $\left(\frac{\varepsilon_d}{p}\right)_4 = 1.$, i.e. $p^m = s^2 + 64d(v_1)^2, s, v_1 \in \mathbb{Z}$, then
$\left(\frac{\varepsilon_d}{p}\right)_8 = (-1)^{v_1}$.

We refer to [8] for references to older power residue criteria in the literature.

Let us now turn to the case which interests us in part I of this paper, namely $N(\varepsilon_d) = -1$ (i.e. $x^2 - dy^2 = -1$ is solvable), $p \equiv 1 \pmod 4$ and $\left(\frac{d}{p}\right) = 1$. This is assumed in the rest of this section.

The old paper [22] contains the following criterion:

Theorem 1.12. *Let $p \equiv 1 \pmod 8$ be a prime represented by $p = s^2 + 2v^2$; a necessary condition for the solvability of $x^2 - 2p^2y^2 = -1$ is that $8|v$; for $p \equiv 9 \pmod{16}$ this condition is also sufficient.*

Remark 1.13. Let $p \equiv 1 \pmod 8$ be a prime. Then (by Gauss) 2 is a biquadratic residue modulo p if and only if $p = x^2 + 64y^2$. If $p \equiv 1 \pmod{16}$, then this is equivalent to $p = s^2 + 128v^2$. (See for example [10].)

In [16], theorem 1.12 was extended to a similar criterion when $p \equiv 17 \pmod{32}$:

Theorem 1.14. *Let $p \equiv 1 \pmod{16}$ be a prime satisfying the necessary condition of theorem 1.12, i.e. representable by the form $p = s^2 + 128v_1^2$ and hence also by $p = x^2 + 64y^2$. Then a necessary condition for the solvability of $x^2 - 2p^2y^2 = -1$ is that $y + v_1 \equiv \frac{p-1}{16} \pmod 2$; for $p \equiv 17 \pmod{32}$ this condition is also sufficient.*

In [15], a necessary and sufficient condition was given in the case $d = q \equiv 1 \pmod 4$ a prime and $p \equiv 5 \pmod 8$. For example, for $q \equiv 5 \pmod 8$:

Theorem 1.15. *Let $q \equiv 5 \pmod 8$ be a prime. Let p be a prime $\equiv 1 \pmod 4$ with $\left(\frac{d}{p}\right) = 1$. Then $p^{h/2} = u^2 + qv^2$, h being the class number of $\mathbb{Q}(\sqrt{-q})$.*
A necessary condition for the solvability of $x^2 - qp^2y^2 = -1$ is that $\frac{p-1}{4} + v$ is even; for $p \equiv 5 \pmod 8$ this condition is also sufficient.

1.3 Norms of Units and 4-rank of Class Groups

The problem of the solvability of the negative Pell equation, $x^2 - dy^2 = -1$ with $d > 1$ square-free can, as we know, be formulated as a question of whether the fundamental unit ε_d of $\mathbb{Q}(\sqrt{d})$ has norm -1. In other words, we ask whether the relative norm map between unit groups,

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} : \ \mathcal{O}^*_{\mathbb{Q}(\sqrt{d})} \to \ \mathcal{O}^*_{\mathbb{Q}} = \{\pm 1\},$$

is surjective.

In general, we could ask the following natural question:

Let L/K be an extension of number fields. What can be said about the relative norm map

$$N_{L/K} : \ \mathcal{O}^*_L \to \ \mathcal{O}^*_K$$

between unit groups? (Clearly, units of L are mapped to units of K.)
In particular, can we decide whether this is a surjective map?

In part II of this thesis, we investigate this problem for certain cyclic extensions of prime degree, mostly quadratic.

Apart from the classical case, the only thing which seems to be known about the general question is a *reformulation* (in terms of the ramified primes of L/K) of the problem given by Hilbert (see [13]) only in the special case of $K = \mathbb{Q}(i)$ the Gaussian field and $L = K(\sqrt{d})$, d an integer. We shall have more to say about this case later and we use it to illustrate some of the results.

We mention two classical results.

Definition 1.16. Let D be the discriminant of the quadratic number field K. Consider factorizations $D = D_1 D_2$ of D where each of D_1 and D_2 is a product of prime discriminants or equal to 1. The factorizations $D = D_1 D_2$ and $D = D_2 D_1$ are considered the same.
The factorization $D = D_1 D_2$ is of type 2 (German: Von zweiter Art) if

$$\forall \text{ prime } p | D_1 : \left(\frac{D_2}{p}\right) = 1 \qquad \text{and} \qquad \forall \text{ prime } p | D_2 : \left(\frac{D_1}{p}\right) = 1.$$

Here $\left(\frac{D_i}{\cdot}\right)$ is the Kronecker symbol.

Definition 1.17. For a finite abelian group G, the number of cyclic factors of the 2–Sylow subgroup of G whose order is divisible by 4 is called the 4–rank of G.

In 1934, Redei and Reichardt (see [25] and [26])) proved the following theorem:

Theorem 1.18. *Let the quadratic number field K have discriminant D. If the number of factorizations $D = D_1D_2$ of D of type 2 is 2^u, then u is the 4–rank of the strict class group of K.*

They also proved the following

Theorem 1.19. *Let $d > 1$ be a square-free integer. Assume that d is not divisible by a prime congruent to 3 modulo 4. If only the trivial factorization of the discriminant of $\mathbb{Q}(\sqrt{d})$ is of type 2 (which, by theorem 1.18, means that the strict 2–class group of $\mathbb{Q}(\sqrt{d})$ is elementary abelian), then $N(\varepsilon_d) = -1$.*

Theorems 1.18 and 1.19 are, along with the above-mentioned paper, [13], of Hilberts, the starting point for the investigations in part II. More precisely, we ask for possible analogues of these theorems to certain quadratic extensions L/K. In the case of an analogue of theorem 1.19, we shall also look at certain cyclic extensions of prime degree.

When studying the 4-rank of class groups, we shall use, among other things, genus theory of quadratic fields as it can be found in for example [30]. Hilberts similar theory of 'Geschlechter' for quadratic extensions L of $\mathbb{Q}(i)$ (see [13]) will also play a part at a certain point. The concepts 'Geschlecht', 'Hauptgeschlecht' and 'Geschlechter der Hauptart' were defined by Hilbert in terms of certain character symbols.

In general, an ideal class C of $Cl(L)$ was proved (by Hilbert) to be a square if and only if C is in the 'Hauptgeschlecht'.

Consider quadratic extensions of $\mathbb{Q}(i)$ of the special form $L = \mathbb{Q}(i, \sqrt{d})$ where d is an integer. Hilbert proved that the composite of (the natural images of) $Cl(\mathbb{Q}(\sqrt{d}))$ and $Cl(\mathbb{Q}(\sqrt{-d}))$ in $Cl(\mathbb{Q}(i, \sqrt{d}))$ is equal to the 'Geschlechter der Hauptart'.

See also [7] where these concepts are studied in a more general context.

Part I

Power Residue Criteria for Quadratic Units

Chapter 2

Preparations

2.1 Galois Groups

Let $d > 1$ be a square-free integer and assume that $N(\varepsilon_d) = -1$ for the fundamental unit $\varepsilon = \varepsilon_d$ of $\mathbb{Q}(\sqrt{d})$. Let $p \equiv 1 \pmod 4$ be a prime number with with $\left(\frac{d}{p}\right) = 1$, i.e. p splits totally in $\mathbb{Q}(\sqrt{-d})$ and in $\mathbb{Q}(\sqrt{d})$. In part I of this thesis, criteria for $\left(\frac{\varepsilon_d}{p}\right) = 1$ and $\left(\frac{\varepsilon_d}{p}\right)_4 = 1$ are proved for certain (infinite) classes of not necessarily prime d. For example, these criteria will cover all d for which the 2-class group of $\mathbb{Q}(\sqrt{-d})$ is elementary abelian

We are going to use the following

Lemma 2.1. *Let L/K be a quadratic extension of number fields; so we can assume that $L = K(\sqrt{\alpha})$, $\alpha \in \mathcal{O}_K$. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal not dividing (2α). Then*

$$\begin{aligned} \mathfrak{p} \textit{ splits totally in } L \quad &\Leftrightarrow \quad x^2 \equiv \alpha \pmod{\mathfrak{p}} \quad \textit{is solvable in } \mathcal{O}_K \\ &\Leftrightarrow \quad \alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv 1 \pmod{\mathfrak{p}}. \end{aligned}$$

Proof. The first equivalence is contained in [12], theorem 118; the second is well known from the theory of quadratic residues. □

Remark 1.10 hints at the possibility of applying class field theory (cf. theorem A.12). In fact, $\mathbb{Q}(\sqrt{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ turns out to be abelian. Unfortunately, $\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ is not even a Galois extension for $d \neq 2$; this will be remedied by bringing the extension $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ into the discussion.

Proposition 2.2. *1)* $\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}$ *is Galois, and* $Gal(\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})) \simeq \mathbb{Z}/4$*.*

2) $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}$ *is Galois, and* $Gal(\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})) \simeq \mathbb{Z}/8$*.*

3) $\mathbb{Q}(\sqrt{\varepsilon}, i)/\mathbb{Q}$ *is Galois, and* $Gal(\mathbb{Q}(\sqrt{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})) \simeq \mathbb{Z}/4$*.*

4) $\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ *is not Galois for* $d \neq 2$*.*

5) $\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}$ *is Galois for* $d = 2$*, and in this case* $Gal(\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})) \simeq \mathbb{Z}/8$*.*

Proof. We first prove 1) and 2). Put $2\varepsilon = u + t\sqrt{d},\ u, t \in \mathbb{Z}$.

The polynomial $f(x) := x^4 - 2ux^2 - 4$ has the roots $\pm\sqrt{u \pm t\sqrt{d}}$. As

$$\sqrt{u + t\sqrt{d}}\sqrt{u - t\sqrt{d}} = \sqrt{-4} = 2i,$$

$\mathbb{Q}(\sqrt{2\varepsilon}, i)$ is the splitting field of $f(x)$ over $\mathbb{Q}$.

The polynomial $g(x) := f(x^2)$ has the roots $\{\pm 1, \pm i\}\sqrt[4]{u \pm t\sqrt{d}}$. As

$$\sqrt[4]{u + t\sqrt{d}}\sqrt[4]{u - t\sqrt{d}} = \sqrt[4]{-4} = \sqrt{2i} = 1 + i,$$

$\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)$ is the splitting field of $g(x)$ over $\mathbb{Q}$. We claim that

a) $\sqrt{u + t\sqrt{d}} \notin \mathbb{Q}(\sqrt{d}))$, and b) $\sqrt[4]{u + t\sqrt{d}} \notin \mathbb{Q}(\sqrt{u + t\sqrt{d}})$.

Proof of a):

$$\begin{aligned} \sqrt{u + t\sqrt{d}} \in \mathbb{Q}(\sqrt{d})) \quad &\Rightarrow \quad f(x) \textit{ reducible over } \mathbb{Q} \\ &\Rightarrow \quad 2i = \sqrt{u + t\sqrt{d}}\sqrt{u - t\sqrt{d}} \in \mathbb{Q} \ \vee \\ & \quad u + t\sqrt{d} = \left(\sqrt{u + t\sqrt{d}}\right)^2 \in \mathbb{Q}. \end{aligned}$$

Proof of b): Since $u + t\sqrt{d} > 0$, we have (using a)):

$$\begin{aligned}
\sqrt[4]{u+t\sqrt{d}} \in (\mathbb{Q}(\sqrt{d}))\left(\sqrt{u+t\sqrt{d}}\,\right) \quad &\Rightarrow \quad \sqrt[4]{u+t\sqrt{d}} = \alpha + \beta\sqrt{u+t\sqrt{d}};\ \ \alpha,\beta \in \mathbb{Q}(\sqrt{d}) \\
&\Rightarrow \quad \sqrt{u+t\sqrt{d}} = (\alpha^2 + \beta^2(u+t\sqrt{d})) + \\
& \quad 2\alpha\beta\sqrt{u+t\sqrt{d}} \\
&\Rightarrow \quad 0 = \alpha^2 + \beta^2(u+t\sqrt{d}). \\
&\Rightarrow \quad \alpha = \beta = 0.
\end{aligned}$$

a) implies that $[\mathbb{Q}(\sqrt{2\varepsilon}, i) : \mathbb{Q}(\sqrt{-d})] = 4$; this and b) implies that $[\mathbb{Q}(\sqrt[4]{2\varepsilon}, i) \ : \ \mathbb{Q}(\sqrt{-d})] = 8$.

Let $Gal(\mathbb{Q}(\sqrt{d}, i)/\mathbb{Q}(\sqrt{-d})) = \langle\tau\rangle$, i.e. $\tau(\sqrt{d}) = -\sqrt{d}$ (and $\tau(i) = -i$). Let $\tau', \tau'' \in Gal(\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d}))$ be the two automorphisms restricting to τ. As

$$\left(\tau'\left(\sqrt{u+t\sqrt{d}}\,\right)\right)^2 = \left(\tau''\left(\sqrt{u+t\sqrt{d}}\,\right)\right)^2 = \tau(u+t\sqrt{d}) = u - t\sqrt{d},$$

we can assume that

$$\tau'\left(\sqrt{u+t\sqrt{d}}\,\right) = \sqrt{u-t\sqrt{d}} \quad \left(\mathit{and} \quad \tau''\left(\sqrt{u+t\sqrt{d}}\,\right) = -\sqrt{u-t\sqrt{d}}\,\right).$$

Since

$$\begin{aligned}
(\tau')^2\left(\sqrt{u+t\sqrt{d}}\,\right) &= \tau'\left(\sqrt{u-t\sqrt{d}}\,\right) \\
&= \tau'\left(\frac{2i}{\sqrt{u+t\sqrt{d}}}\right) \\
&= \frac{-2i}{\sqrt{u-t\sqrt{d}}} \\
&= -\sqrt{u+t\sqrt{d}},
\end{aligned}$$

we must have

$$Gal(\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})) = \langle\tau'\rangle \simeq \mathbb{Z}/4.$$

Let $\sigma, \sigma' \in Gal(\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d}))$ be the two automorphisms restricting to τ'. As

$$\left(\sigma\left(\sqrt[4]{u+t\sqrt{d}}\,\right)\right)^2 = \left(\sigma'\left(\sqrt[4]{u+t\sqrt{d}}\,\right)\right)^2 = \tau'\left(\sqrt{u+t\sqrt{d}}\,\right) = \sqrt{u-t\sqrt{d}},$$

we can assume that

$$\sigma\left(\sqrt[4]{u+t\sqrt{d}}\right)=\sqrt[4]{u-t\sqrt{d}}\quad\left(and\quad\sigma'\left(\sqrt[4]{u+t\sqrt{d}}\right)=-\sqrt[4]{u-t\sqrt{d}}\right).$$

Note that

$$\sigma\left(\sqrt[4]{u-t\sqrt{d}}\right)=\sigma\left(\frac{1+i}{\sqrt[4]{u+t\sqrt{d}}}\right)=\frac{1-i}{\sqrt[4]{u-t\sqrt{d}}}.$$

Since

$$\begin{aligned}\sigma^4\left(\sqrt[4]{u+t\sqrt{d}}\right) &= \sigma^3\left(\sqrt[4]{u-t\sqrt{d}}\right)\\ &= \sigma^2\left(\frac{1-i}{\sqrt[4]{u-t\sqrt{d}}}\right)\\ &= \sigma\left(\frac{1+i}{1-i}\sqrt[4]{u-t\sqrt{d}}\right)\\ &= \frac{(1-i)^2}{(1+i)\sqrt[4]{u-t\sqrt{d}}}\\ &= -\frac{1+i}{\sqrt[4]{u-t\sqrt{d}}}\\ &= -\sqrt[4]{u+t\sqrt{d}},\end{aligned}$$

we conclude that $\quad Gal(\mathbb{Q}(\sqrt[4]{2\varepsilon},i)/\mathbb{Q}(\sqrt{-d}))=\langle\sigma\rangle\simeq\mathbb{Z}/8.$

3) The proof of 3) is analogous to that of 1).

4) Suppose that $d\neq 2$ and that $\mathbb{Q}(\sqrt[4]{\varepsilon},i)/\mathbb{Q}(\sqrt{-d})$ is Galois; then arguments completely similar to those in 2) would give that

$$Gal(\mathbb{Q}(\sqrt[4]{\varepsilon},i)/\mathbb{Q}(\sqrt{-d}))\simeq\mathbb{Z}/8$$

and that $\delta\in\mathbb{Q}(\sqrt[4]{\varepsilon},i)$ where δ is a primitive eighth root of unity. Then

$$\sqrt{2}\in\mathbb{Q}(\sqrt{2},i)=\mathbb{Q}(\delta)\subseteq\mathbb{Q}(\sqrt[4]{\varepsilon},i),$$

and hence $\mathbb{Q}(\sqrt{2},\sqrt{-d})=\mathbb{Q}(\sqrt{-d},i)$, and so $d=2$ which is a contradiction.

5) If $d=2$, $\mathbb{Q}(\sqrt{-d},i)$ is the eighth cyclotomic field. Therefore, the proof of the fact that $\mathbb{Q}(\sqrt[4]{\varepsilon},i)/\mathbb{Q}$ is Galois is analogous to what was done in 2); the computation of the mentioned Galois group is also similar. □

Now we show that the question of the splitting of prime ideals in $\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ can be reformulated as a question of the splitting of prime ideals in *abelian* extensions. First an easy lemma.

Lemma 2.3. *Let L/K be a V_4-extension of number fields. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ which is unramified in L. Let L_1, L_2, L_3 be the non-trivial intermediate fields in L/K. Then $\mathfrak{p}$ splits totally in exactly one or three of the fields L_1, L_2, L_3.*

Proof. Note that $\mathfrak{p}$ cannot be inert in L_1, L_2, L_3 (for otherwise $\mathfrak{p}$ would be inert L, and hence $Gal(L/K)$ would be cyclic). So we can assume that $\mathfrak{p}$ splits totally in L_1. If $\mathfrak{p}$ splits totally in L/L_1, then $\mathfrak{p}$ splits totally in L_2 and L_3. If $\mathfrak{p}$ does not split totally in L/L_1, $\mathfrak{p}$ does not split totally in L_2 and not in L_3. □

Proposition 2.4. *Assume that $p \equiv 1 \pmod 8$. For a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ above p we have:*

$$\mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt[4]{\varepsilon}, i) \Leftrightarrow$$

$$\mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt{\varepsilon}, i) \wedge$$

$$\left(\left(\left(\frac{2}{p}\right)_4 = 1 \wedge \mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i) \right) \vee \right.$$

$$\left. \left(\left(\frac{2}{p}\right)_4 = -1 \wedge \mathfrak{p} \textit{ does not split totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i) \right) \right).$$

Proof. Suppose first that $d \neq 2$. We begin by proving
a) The extensions $\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)$ and $\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{\varepsilon}, i)$ are Galois with

$$Gal(\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)) \simeq \mathbb{Z}/4,$$

$$Gal(\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{\varepsilon}, i)) \simeq \mathbb{Z}/2 \quad \textit{and} \quad \mathbb{Q}(\sqrt[4]{\varepsilon}, i) \not\subseteq \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2}).$$

Proof of a): As

$$Gal(\mathbb{Q}(\sqrt{\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})) \simeq \mathbb{Z}/4,$$

we have $\sqrt{2} \in \mathbb{Q}(\sqrt{\varepsilon}, i) \Rightarrow \mathbb{Q}(\sqrt{-d}, \sqrt{2}) = \mathbb{Q}(\sqrt{-d}, i) \Rightarrow d = 2$; hence

$$Gal(\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)) \simeq \mathbb{Z}/2.$$

The extension $\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)$ is clearly Galois, but it is not yet obvious whether $\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})$. Let

$$\tau \in Gal(\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})/\mathbb{Q}(\sqrt{\varepsilon}, i))$$

with $\tau(\sqrt{2}) = -\sqrt{2}$. Consider an automorphism

$$\sigma \in Gal(\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i))$$

restricting to τ (perhaps $\sigma = \tau$). Since $\sigma(\sqrt[4]{2}) = (-1)^k i\sqrt[4]{2}, k \in \{0, 1\}$, we see that

$$\sigma^2(\sqrt[4]{2}) = \sigma((-1)^k i\sqrt[4]{2}) = i^2(-1)^k(-1)^k\sqrt[4]{2} = -\sqrt[4]{2};$$

hence ($\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})$ and) $Gal(\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)) \simeq \mathbb{Z}/4$.

Just as in the proof of $\sqrt[4]{2\varepsilon} \notin \mathbb{Q}(\sqrt{2\varepsilon}, i)$ (see the proof of proposition 2.2) we get $\sqrt[4]{\varepsilon} \notin \mathbb{Q}(\sqrt{\varepsilon}, i)$. This gives

$$Gal(\mathbb{Q}(\sqrt[4]{\varepsilon}, i)/\mathbb{Q}(\sqrt{\varepsilon}, i)) \simeq \mathbb{Z}/2.$$

Assume that $\mathbb{Q}(\sqrt[4]{\varepsilon}, i) \subseteq \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})$. As $\sqrt[4]{\varepsilon} \notin \mathbb{Q}(\sqrt{\varepsilon}, i)$ and

$$Gal(\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)) \simeq \mathbb{Z}/4,$$

it follows that $\mathbb{Q}(\sqrt[4]{\varepsilon}, i) = \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})$ which is a Galois extension of $\mathbb{Q}(\sqrt{-d})$, by proposition 2.2 3). This contradiction (to proposition 2.2, 4)) finishes the proof of a).

From a) it immediately follows that $\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)$ is Galois of degree 8. As $\sqrt{2} \notin \mathbb{Q}(\sqrt{\varepsilon}, i)$, clearly $[\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})]$=4, and then we must have

$$Gal(\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})) \simeq V_4.$$

The three (non-trivial) fields between $\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})$ and $\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})$ are

$$L_1 = \mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt{2}), \quad L_2 = \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2}), \quad L_3 = \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2\varepsilon}).$$

Let $\mathfrak{p}''$ be a prime ideal in $\mathbb{Q}(\sqrt{\varepsilon}, i)$ above $\mathfrak{p}$; $\mathfrak{p}''$ is obviously unramified in $\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})$ (the discriminant of $\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})$ clearly divides a power of 2), and $\mathfrak{p}''$ splits totally in $\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})$ ($p \equiv 1 \pmod 8$). Let $\mathfrak{p}'$ be a prime ideal in $\mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt{2})$ above $\mathfrak{p}''$.

Suppose now that $d = 2$. We have:

i) $\sqrt[4]{\varepsilon} \notin \mathbb{Q}(\sqrt{\varepsilon}, i)$ (as above);

ii) $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{\varepsilon}, i)$ (since

$$\begin{aligned} & \sqrt[4]{2} \in \mathbb{Q}(\sqrt{\varepsilon}, i) \\ \Rightarrow \quad & \sqrt[4]{2} \in \mathbb{Q}(\sqrt{\varepsilon}, i) \cup \mathbb{R} = \mathbb{Q}(\sqrt{\varepsilon}) \\ \Rightarrow \quad & \mathbb{Q}(\sqrt{2})(\sqrt{\varepsilon})) = \mathbb{Q}(\sqrt{\varepsilon}) = \mathbb{Q}(\sqrt[4]{2})) = \mathbb{Q}(\sqrt{2})\left(\sqrt{\sqrt{2}}\right) \\ \Rightarrow \quad & 1+\sqrt{2} = \varepsilon = (a+b\sqrt{2})^2\sqrt{2} = 4ab + (a^2+2b^2)\sqrt{2}, a, b \in \mathbb{Q} \\ \Rightarrow \quad & 4ab = 1 \wedge a^2 + 2b^2 = 1 \\ \Rightarrow \quad & a^4 - a^2 + 1/8 = 0 \quad \text{(which is impossible));} \end{aligned}$$

iii) $\sqrt[4]{2\varepsilon} \notin \mathbb{Q}(\sqrt{\varepsilon}, i)$ (since $[\mathbb{Q}(\sqrt[4]{2\varepsilon}) : \mathbb{Q}] = 8 > 4 = [\mathbb{Q}(\sqrt{\varepsilon}) : \mathbb{Q}]$);

iv) $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{\varepsilon}, i)$ (since

$$\begin{aligned} \sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{\varepsilon}, i) \quad \Rightarrow \quad & \sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{\varepsilon}) \\ \Rightarrow \quad & \mathbb{Q}(\sqrt{\varepsilon})\left(\sqrt{\sqrt{2\varepsilon}}\right) = \mathbb{Q}(\sqrt{\varepsilon})\left(\sqrt{\sqrt{2}}\right) \\ \Rightarrow \quad & \sqrt{2\varepsilon} = \gamma^2\sqrt{2}, \gamma \in \mathbb{Q}(\sqrt{\varepsilon}) \\ \Rightarrow \quad & \sqrt[4]{\varepsilon} = \pm\gamma \in \mathbb{Q}(\sqrt{\varepsilon})). \end{aligned}$$

From i), ii), iii) and iv) we deduce that

$$Gal(\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})/\mathbb{Q}(\sqrt{\varepsilon}, i)) \simeq V_4.$$

The three (non-trivial) fields between $\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})$ and $\mathbb{Q}(\sqrt{\varepsilon}, i)$ are

$$L_1 = \mathbb{Q}(\sqrt[4]{\varepsilon}, i), \quad L_2 = \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2}), \quad L_3 = \mathbb{Q}(\sqrt{\varepsilon}, i, \sqrt[4]{2\varepsilon}).$$

Let $\mathfrak{p}'$ be a prime ideal in $\mathbb{Q}(\sqrt{\varepsilon}, i)$ above $\mathfrak{p}$; $\mathfrak{p}'$ is obviously unramified in $\mathbb{Q}(\sqrt[4]{\varepsilon}, i, \sqrt[4]{2})$.

In the rest of the proof we deal with both cases ($d \neq 2$ and $d = 2$) at the same time. By lemma 2.3 $\mathfrak{p}'$ splits totally in 1 or 3 of the fields L_1, L_2, L_3.

If $\left(\frac{2}{p}\right)_4 = 1$, then $\mathfrak{p}'$ splits totally in L_2 and hence (when 'split(s)' means 'split(s) totally'):

$$\begin{aligned} \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt[4]{\varepsilon}, i) \quad \Leftrightarrow \quad & \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt{\varepsilon}, i) \ \wedge \ \mathfrak{p}' \textit{ splits in } L_1 \\ \Leftrightarrow \quad & \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt{\varepsilon}, i) \ \wedge \ \mathfrak{p}' \textit{ splits in } L_3 \\ \Leftrightarrow \quad & \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt{\varepsilon}, i) \ \wedge \ \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i). \end{aligned}$$

If $\left(\frac{2}{p}\right)_4 = -1$, then $\mathfrak{p}'$ does not split totally in L_2 and so:

$$\begin{aligned} \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt[4]{\varepsilon}, i) &\Leftrightarrow \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt{\varepsilon}, i) \ \wedge\ \mathfrak{p}' \textit{ splits in } L_1 \\ &\Leftrightarrow \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt{\varepsilon}, i) \ \wedge\ \mathfrak{p}' \textit{ does not split in } L_3 \\ &\Leftrightarrow \mathfrak{p} \textit{ splits in } \mathbb{Q}(\sqrt{\varepsilon}, i) \ \wedge\ \mathfrak{p} \textit{ does not split in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i). \end{aligned}$$

This proves the proposition. □

By this proposition and remark 1.10, the problem of finding $\left(\frac{\varepsilon_d}{p}\right)$ and $\left(\frac{\varepsilon_d}{p}\right)_4$ for $d > 1$ square-free, $N(\varepsilon_d) = -1$ and $\left(\frac{d}{p}\right) = 1$ is thus reduced to the question of the splitting of prime ideals above p in certain cyclic extensions of $\mathbb{Q}(\sqrt{-d})$. By theorem A.12 this is equivalent to the problem of deciding whether prime ideals in $\mathbb{Q}(\sqrt{-d})$ above p are in the ideal groups in $\mathbb{Q}(\sqrt{-d})$ corresponding to these cyclic extensions. The investigation of these ideal groups will be the main topic of the rest of this chapter.

2.2 Two Types of Prime Factors of d

The notation and the assumptions introduced here will be maintained throughout this chapter and the next.

Let $d > 1$ be square-free and suppose that $N(\varepsilon_d) = -1$ for the fundamental unit ε_d of $\mathbb{Q}(\sqrt{d})$. Let $p \equiv 1 \pmod 4$ be a prime number with $\left(\frac{d}{p}\right) = 1$.

Lemma 2.5. *Let $n \equiv 1 \pmod 4$ be a prime number. Then*

$$\left(\frac{-4}{n}\right)_4 = 1.$$

If $n \equiv 1 \pmod 8$, then $4|h$ where h is the class number of $\mathbb{Q}(\sqrt{-n})$; and

$$\left(\frac{-4}{n}\right)_8 = (-1)^{\frac{h}{4}}.[1]$$

Proof. If $n \equiv 5 \pmod 8$, then

$$\left(\frac{-4}{n}\right)_4 = \left(\frac{-1}{n}\right)_4 \left(\frac{2^2}{n}\right)_4 = (-1)^{\frac{n-1}{4}} \left(\frac{2}{n}\right) = (-1)(-1) = 1.$$

[1] if $\left(\frac{a}{n}\right)_4 = 1$, we define $\left(\frac{a}{n}\right)_8 = 1$ or -1 according as a is a 8th power residue mod n or not.

Now let $n \equiv 1 \pmod 8$. First we find

$$\left(\frac{-4}{n}\right)_4 = \left(\frac{-1}{n}\right)_4 \left(\frac{2^2}{n}\right)_4 = (-1)^{\frac{n-1}{4}} \left(\frac{2}{n}\right) = 1 \cdot 1 = 1.$$

By the help of genus theory it can be proved (see for example [11]) that $4|h$ and that

$$\left(\frac{2}{n}\right)_4 = (-1)^{\frac{n-1}{8}+\frac{h}{4}};$$

hence

$$\left(\frac{-4}{n}\right)_8 = (-1)^{\frac{n-1}{8}} \left(\frac{2^2}{n}\right)_8 = (-1)^{\frac{n-1}{8}} \left(\frac{2}{n}\right)_4 = (-1)^{\frac{h}{4}}.$$

□

Write

$$2\varepsilon = u + t\sqrt{d}, \; u, t \in \mathbb{Z}.$$

It turns out that odd prime factors (necessarily $\equiv 1 \pmod 4$) of d must be divided into 2 classes, each class having its own significance for the value of biquadratic residue symbol $\left(\frac{\varepsilon_d}{p}\right)_4$. Let d_0 be the odd part of d (so $d_0 = d$ if d is odd). Write

$$d_0 = q_1 \cdots q_\alpha p_1 \cdots p_\beta$$

where q_i and p_j are prime numbers such that:

i) $\left(\frac{u}{q_1}\right)_4 = \cdots = \left(\frac{u}{q_\alpha}\right)_4 = 1$ (primes of type I);

ii) $\left(\frac{u}{p_1}\right)_4 = \cdots = \left(\frac{u}{p_\beta}\right)_4 = -1$ (primes of type II).

Remark 2.6. For an odd prime n dividing d we have

$$\left(\frac{u}{n}\right) = \left(\frac{u^2}{n}\right)_4 = \left(\frac{u^2 - dt^2}{n}\right)_4 = \left(\frac{-4}{n}\right)_4 = 1,$$

by lemma 2.5. It follows that n satisfies (exactly) one of the conditions i), ii).
For $n \equiv 1 \pmod 8$ it can be checked whether n satisfies i) or ii) without knowing the fundamental unit $\varepsilon = \frac{u+t\sqrt{d}}{2}$; actually it can be checked without leaving $\mathbb{Z}$. This follows from

$$\left(\frac{u}{n}\right)_4 = \left(\frac{u^2}{n}\right)_8 = \left(\frac{u^2 - dt^2}{n}\right)_8 = \left(\frac{-4}{n}\right)_8,$$

where $\left(\frac{-1}{n}\right)_4 = 1$ was used. By lemma 2.5 a knowledge of the class number $h(\mathbb{Q}(\sqrt{-n}))$ is also sufficient.

2.3 The Ideal Groups

In this section we begin the important investigation of the ideal groups in $\mathbb{Q}(\sqrt{-d})$ corresponding to the cyclic extensions

$$\mathbb{Q}(\sqrt{d},i)/\mathbb{Q}(\sqrt{-d}),\ \mathbb{Q}(\sqrt{\varepsilon},i)/\mathbb{Q}(\sqrt{-d}),\ \mathbb{Q}(\sqrt{2\varepsilon},i)/\mathbb{Q}(\sqrt{-d}),\ \mathbb{Q}(\sqrt[4]{2\varepsilon},i)/\mathbb{Q}(\sqrt{-d}).$$

Since each of these extensions is built up from $\mathbb{Q}(\sqrt{-d})$ by successively adjoining square roots of integral elements (such as 2ε) which generate principal ideals all of whose prime factors lie above 2, it is clear that these extensions have relative discriminants dividing some power of (the principal ideal generated by) 2. Therefore these extensions have conductors dividing (2^g) for some fixed $g \in \mathbb{N}$. In other words: We can use (2^g) as a common congruence module for the corresponding ideal groups in the sense of theorem A.6 (i.e. we can, in ii) of theorem A.6, take (2^g) as a common divisor $\mathscr{M}$ for all four ideal groups). Let these ideal groups be $H_{-1}, H_{\varepsilon}, H_{2\varepsilon}, H$ where

a) H_{-1} corresponds to $\mathbb{Q}(\sqrt{d},i)$;

b) H_{ε} corresponds to $\mathbb{Q}(\sqrt{\varepsilon},i)$;

c) $H_{2\varepsilon}$ corresponds to $\mathbb{Q}(\sqrt{2\varepsilon},i)$;

d) H corresponds to $\mathbb{Q}(\sqrt[4]{2\varepsilon},i)$.

By theorem A.11 we have (where, of course, $A_{(2)}$ denotes the group of fractional ideals in $\mathbb{Q}(\sqrt{-d})$ prime to (2))

$$H_{\varepsilon} \subseteq H_{-1} \subseteq A_{(2)} \supseteq H_{-1} \supseteq H_{2\varepsilon} \supseteq H$$

where each inclusion indicates that the subgroup has index 2. We also have (where the exact value of g is yet unknown):

$$\begin{aligned}
A_{(2)} \supseteq H_{-1} \supseteq S_{\mathfrak{f}_{\mathbb{Q}(\sqrt{d},i)/\mathbb{Q}(\sqrt{-d})}} \supseteq S_{(2^g)};\\
A_{(2)} \supseteq H_{\varepsilon} \supseteq S_{\mathfrak{f}_{\mathbb{Q}(\sqrt{\varepsilon},i)/\mathbb{Q}(\sqrt{-d})}} \supseteq S_{(2^g)};\\
A_{(2)} \supseteq H_{2\varepsilon} \supseteq S_{\mathfrak{f}_{\mathbb{Q}(\sqrt{2\varepsilon},i)/\mathbb{Q}(\sqrt{-d})}} \supseteq S_{(2^g)};\\
A_{(2)} \supseteq H \supseteq S_{\mathfrak{f}_{\mathbb{Q}(\sqrt[4]{2\varepsilon},i)/\mathbb{Q}(\sqrt{-d})}} \supseteq S_{(2^g)}.
\end{aligned}$$

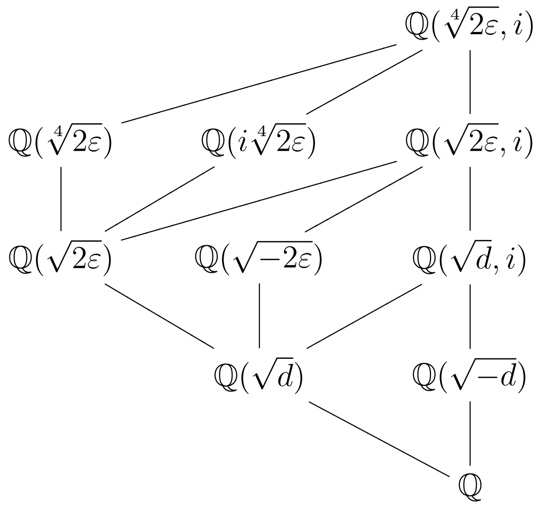
$\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)$
$\mathbb{Q}(\sqrt[4]{2\varepsilon})$
$\mathbb{Q}(i\sqrt[4]{2\varepsilon})$
$\mathbb{Q}(\sqrt{2\varepsilon}, i)$
$\mathbb{Q}(\sqrt{2\varepsilon})$
$\mathbb{Q}(\sqrt{-2\varepsilon})$
$\mathbb{Q}(\sqrt{d}, i)$
$\mathbb{Q}(\sqrt{d})$
$\mathbb{Q}(\sqrt{-d})$
$\mathbb{Q}$

Figure 1: Some subfields of $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)$

Propositions, 2.7, 2.8 and 2.9 (see below) are true no matter how we choose g.

Proposition 2.7. *Assume that $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\sqrt{-d})$ above one of the odd prime factors of d. Then*

1. $\mathfrak{p} \in H_{2\varepsilon}$.

2. $(\sqrt{-d}) \in H_{2\varepsilon}$ *if d is odd.*

Proof. 1. Let n be the odd prime factor of d below $\mathfrak{p}$, and let $\mathfrak{p}_1$ be the prime ideal in $\mathbb{Q}(\sqrt{d})$ above n. Using theorem A.12 and lemma 2.1 (and $2\varepsilon = u + t\sqrt{d}$) we have:

$$\begin{aligned}
\mathfrak{p} \in H_{2\varepsilon} \quad &\Leftrightarrow \quad \mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt{2\varepsilon}, i) \\
&\Leftrightarrow \quad \mathfrak{p}_1 \textit{ splits totally in } \mathbb{Q}(\sqrt{2\varepsilon}) \\
&\Leftrightarrow \quad x^2 \equiv u + t\sqrt{d} \pmod{\mathfrak{p}_1} \textit{ is solvable in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \\
&\Leftrightarrow \quad x^2 \equiv u \pmod{\mathfrak{p}_1} \textit{ is solvable in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \\
&\Leftrightarrow \quad u^{\frac{N(\mathfrak{p}_1)-1}{2}} \equiv 1 \pmod{\mathfrak{p}_1} \\
&\Leftrightarrow \quad u^{\frac{n-1}{2}} \equiv 1 \pmod{n} \\
&\Leftrightarrow \quad \left(\frac{u}{n}\right) = 1.
\end{aligned}$$

And this last statement is true, by remark 2.6.

2. Follows from 1. and the fact that $(\sqrt{-d})$ is the product of the prime ideals in $\mathbb{Q}(\sqrt{-d})$ above the prime factors of d. □

Proposition 2.8. *Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Q}(\sqrt{-d})$ above the odd prime factor n of d. Let $d_0 = q_1 \cdots q_\alpha p_1 \cdots p_\beta$ be as in section 2.2. Then*

1. *$\mathfrak{p} \in H \;\Leftrightarrow\; n$ is of type I (i.e. $n \in \{q_1, \ldots, q_\alpha\}$).*

2. *For d odd: $(\sqrt{-d}) \in H \;\Leftrightarrow\; 2|\beta$.*

Proof. 1. Let (cf. proposition 2.7) $\mathfrak{p}_2$ be one of the two prime ideals in $\mathbb{Q}(\sqrt{2\varepsilon})$ above n. Using theorem A.12 and lemma 2.1 we have:

$$\begin{aligned}
\mathfrak{p} \in H \;&\Leftrightarrow\; \mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i)\\
&\Leftrightarrow\; \mathfrak{p}_2 \textit{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon})\\
&\Leftrightarrow\; x^2 \equiv \sqrt{u + t\sqrt{d}} \pmod{\mathfrak{p}_2} \textit{ is solvable in } \mathcal{O}_{\mathbb{Q}(\sqrt{2\varepsilon})}\\
&\Leftrightarrow\; \left(\sqrt{u + t\sqrt{d}}\right)^{\frac{N(\mathfrak{p}_2)-1}{2}} \equiv 1 \pmod{\mathfrak{p}_2}\\
&\Leftrightarrow\; (u + t\sqrt{d})^{\frac{n-1}{4}} \equiv 1 \pmod{\mathfrak{p}_2}\\
&\Leftrightarrow\; u^{\frac{n-1}{4}} \equiv 1 \pmod{\mathfrak{p}_2}\\
&\Leftrightarrow\; u^{\frac{n-1}{4}} \equiv 1 \pmod{n}\\
&\Leftrightarrow\; \left(\frac{u}{n}\right)_4 = 1.\\
&\Leftrightarrow\; n \textit{ is of type } I.
\end{aligned}$$

2. As $\mathfrak{p} \in H_{2\varepsilon}$ (by proposition 2.7), this follows immediately from 1. and the fact that $|H_{2\varepsilon}/H| = 2$. □

Proposition 2.9. *Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Q}(\sqrt{-d})$ above the odd prime factor n of d. Then*

1. *$\mathfrak{p} \in H_\varepsilon \;\Leftrightarrow\; n \equiv 1 \pmod 8$.*

2. *$(\sqrt{-d}) \in H_\varepsilon \;\Leftrightarrow\; d \equiv 1 \pmod 8$.*

Proof. 1. Let $\mathfrak{p}_1$ be the prime ideal in $\mathbb{Q}(\sqrt{d})$ above n. Using theorem A.12, lemma 2.1 and remark 2.6 we have:

$$\begin{aligned}
\mathfrak{p} \in H_\varepsilon \quad &\Leftrightarrow \quad \mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt{\varepsilon}, i) \\
&\Leftrightarrow \quad \mathfrak{p}_1 \textit{ splits totally in } \mathbb{Q}(\sqrt{\varepsilon}) \\
&\Leftrightarrow \quad x^2 \equiv \frac{u + t\sqrt{d}}{2} \pmod{\mathfrak{p}_1} \textit{ is solvable in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \\
&\Leftrightarrow \quad x^2 \equiv 2^2 \frac{u}{2} \pmod{\mathfrak{p}_1} \textit{ is solvable in } \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \\
&\Leftrightarrow \quad (2u)^{\frac{N(\mathfrak{p}_1)-1}{2}} \equiv 1 \pmod{\mathfrak{p}_1} \\
&\Leftrightarrow \quad (2u)^{\frac{n-1}{2}} \equiv 1 \pmod{n} \\
&\Leftrightarrow \quad \left(\frac{2u}{n}\right) = 1 \\
&\Leftrightarrow \quad \left(\frac{2}{n}\right) = 1 \\
&\Leftrightarrow \quad n \equiv 1 \pmod{8}.
\end{aligned}$$

2. As $\mathfrak{p} \in H_{-1}$ (by proposition 2.7), this follows immediately from 1. and the fact that $|H_{-1}/H_\varepsilon| = 2$. □

The following observation, which we shall use, belongs to class field theory.

Proposition 2.10. *Let L/K be a Galois extension of number fields without infinite ramification; let M be a number field such that M/L is abelian. Let H be the ideal group in L corresponding to M modulo some integral divisor $\mathscr{M}$. Assume that $\forall \sigma \in Gal(L/K): \ \sigma(\mathscr{M}) = \mathscr{M}$. Then*

$$M/K \textit{ is Galois } \Leftrightarrow \forall \sigma \in Gal(L/K): \ \sigma(H) = H.$$

Proof. '⇒': Assume that M/K is Galois. Let $\sigma \in Gal(L/K)$; let $\tau \in Gal(M/K)$ restrict to σ. As $\sigma(\mathscr{M}) = \mathscr{M}$, we easily get $\tau(A_{\mathscr{M}}) = A_{\mathscr{M}}$ and $\tau(S_{\mathscr{M}}) = S_{\mathscr{M}}$. The ideal group in L corresponding to $\tau(M)$ is $\tau(H)$ (cf. theorem A.12 - an extension is uniquely determined by its set of primes splitting totally). As $\tau(M) = M$, we have $\sigma(H) = \tau(H) = H$.

'⇐': Assume that $\forall \sigma \in Gal(L/K): \ \sigma(H) = H$. Let τ be a K-embedding of M in $\mathbb{C}$. As $\tau\big|_L \in Gal(L/K)$, it follows that $\tau(H) = \tau\big|_L(H) = H$. Since the extension $\tau(M)/L$ is abelian, $\tau(H) = H$ is the ideal group modulo $\mathscr{M}$ in L corresponding to $\tau(M)$. Hence $\tau(M) = M$, and so M/K is Galois. □

2.4 The Principal Ideals

We now turn to the determination of all principal ideals in the four ideal groups.

Proposition 2.11. *Let $p \equiv 1 \pmod 4$ be a prime number. Let $2\varepsilon = u + t\sqrt{d}$ where $\varepsilon = \varepsilon_d$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$ which has norm -1. Then*

1. *For $p|d$:*
$$(p) \in H.$$
2. *For $\left(\frac{d}{p}\right) = 1$:*
$$(p) \in H.$$
3. *For $\left(\frac{d}{p}\right) = -1$:*
$$(u + t\sqrt{d})^{\frac{p^2-1}{4}} \equiv 1 \pmod p \quad in\ \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \ \Rightarrow\ (p) \in H.$$

Proof. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Q}(\sqrt{-d})$ above p, let $\mathfrak{p}'$ be the conjugate ideal; let $\mathfrak{p}_1$ be a prime ideal in $\mathbb{Q}(\sqrt{d})$ above p.

1. $p|d$: By proposition 2.7 we have $\mathfrak{p} \in H_{2\varepsilon}$; hence (since $|H_{2\varepsilon}/H| = 2$) $(p) = \mathfrak{p}^2 \in H$.

2. $\left(\frac{d}{p}\right) = 1$: As $\mathfrak{p}$ and $\mathfrak{p}'$ split totally in $\mathbb{Q}(\sqrt{d}, i)$, the inertial degrees of $\mathfrak{p}$ and $\mathfrak{p}'$ in $L := \mathbb{Q}(\sqrt[4]{2\varepsilon}, i)$ divide 4. So if we put $K := \mathbb{Q}(\sqrt{-d})$, then theorem A.12 gives that
$$ord\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right) = ord(\mathfrak{p}H) = ord(\mathfrak{p}'H) = \ ord\left(\left(\frac{L/K}{\mathfrak{p}'}\right)\right) \mid 4$$

($ord(\mathfrak{p}H) = ord(\mathfrak{p}'H)$ follows from proposition 2.10:
$$\mathfrak{p}^k \in H \Leftrightarrow (\mathfrak{p}')^k \in H' \Leftrightarrow (\mathfrak{p}')^k \in H).$$

If $ord(\mathfrak{p}H) = ord(\mathfrak{p}'H) = 1$, then $(p) = \mathfrak{p}\mathfrak{p}' \in H$.

If $ord(\mathfrak{p}H) = ord(\mathfrak{p}'H) = 2$, then (since $A_{(2)}/H \simeq \mathbb{Z}/8$)
$$(p) \in (p)H = (\mathfrak{p}H)(\mathfrak{p}'H) = H.$$

Consider the remaining case: $ord(\mathfrak{p}H) = ord(\mathfrak{p}'H) = 4$; then
$$\left(\frac{L/K}{\mathfrak{p}}\right), \left(\frac{L/K}{\mathfrak{p}'}\right) \in Gal(L/\mathbb{Q}(\sqrt{d}, i)).$$

So $\left(\frac{L/K}{\mathfrak{p}}\right)$ and $\left(\frac{L/K}{\mathfrak{p}'}\right)$ are determined by their values on $\sqrt[4]{2\varepsilon}$. It is clear that

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[4]{2\varepsilon}) = (-1)^a i\sqrt[4]{2\varepsilon}, \quad \left(\frac{L/K}{\mathfrak{p}'}\right)(\sqrt[4]{2\varepsilon}) = (-1)^b i\sqrt[4]{2\varepsilon}$$

for suitable $a, b \in \{0, 1\}$. By conjugating we get

$$\begin{aligned}
& \left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[4]{2\varepsilon}) = (-1)^a i\sqrt[4]{2\varepsilon} \\
\Rightarrow\quad & (-1)^a i\sqrt[4]{2\varepsilon} \equiv (\sqrt[4]{2\varepsilon})^p \pmod{\mathfrak{p}\mathcal{O}_L} \\
\Rightarrow\quad & -(-1)^a i\sqrt[4]{2\varepsilon} \equiv (\sqrt[4]{2\varepsilon})^p \equiv \left(\frac{L/K}{\mathfrak{p}'}\right)(\sqrt[4]{2\varepsilon}) \pmod{\mathfrak{p}'\mathcal{O}_L} \\
\Rightarrow\quad & \left(\frac{L/K}{\mathfrak{p}'}\right)(\sqrt[4]{2\varepsilon}) = -(-1)^a i\sqrt[4]{2\varepsilon} \\
\Rightarrow\quad & \left(\frac{L/K}{\mathfrak{p}}\right)\circ\left(\frac{L/K}{\mathfrak{p}'}\right)(\sqrt[4]{2\varepsilon}) = \sqrt[4]{2\varepsilon} \\
\Rightarrow\quad & \left(\frac{L/K}{\mathfrak{p}}\right)\circ\left(\frac{L/K}{\mathfrak{p}'}\right) = id_L.
\end{aligned}$$

Hence, by the isomorphism in theorem A.6 (induced by the Artin map),

$$(p) \in (p)H = (\mathfrak{p}H)(\mathfrak{p}'H) = H.$$

3. $\left(\frac{d}{p}\right) = -1$: Since p is inert in $\mathbb{Q}(\sqrt{-d})$ and in $\mathbb{Q}(\sqrt{d})$, we have, using theorem A.12 and lemma 2.1:

$$\begin{aligned}
\mathfrak{p} \in H_{2\varepsilon} \quad & \Leftrightarrow \quad \mathfrak{p} \textit{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}, i) \\
& \Leftrightarrow \quad \mathfrak{p}_1 \textit{ splits totally in } \mathbb{Q}(\sqrt[4]{2\varepsilon}) \\
& \Leftarrow \quad (u + t\sqrt{d})^{\frac{N(\mathfrak{p}_1)-1}{4}} \equiv 1 \pmod{p} \\
& \Leftrightarrow \quad (u + t\sqrt{d})^{\frac{p^2-1}{4}} \equiv 1 \pmod{p}.
\end{aligned}$$

□

We can now determine the principal ideals in the ideal groups.

Recall that $d_0 = q_1 \cdots q_\alpha p_1 \cdots p_\beta$ is the odd part of d.

Theorem 2.12. *The four ideal groups $H_{-1}, H_\varepsilon, H_{2\varepsilon}, H$ have (8) as a common congruence module, i.e. we can use g=3. The subgroups of principal ideals are as follows:*

1. $d \equiv 1 \pmod 4$:

$$H_{-1} \cap S_{(1)} = A_{(2)} \cap S_{(1)};$$

$$H_\varepsilon \cap S_{(1)} = \begin{cases} A_{(2)} \cap S_{(1)}, & if\ d \equiv 1 \pmod 8 \\ S_{(2)}, & if\ d \equiv 5 \pmod 8 \end{cases};$$

$$H_{2\varepsilon} \cap S_{(1)} = \{(1), (\sqrt{-d})\} S_{(4)};$$

$$H \cap S_{(1)} = \begin{cases} \{(1), (5), (\sqrt{-d}), (5\sqrt{-d})\} S_{(8)}, & 2|\beta \\ \{(1), (5), (4+\sqrt{-d}), (4+5\sqrt{-d})\} S_{(8)}, & 2 \nmid \beta \end{cases}.$$

2. $2|d$:

$$H_{-1} \cap S_{(1)} = S_{(2)};$$

$$H_\varepsilon \cap S_{(1)} = H_{2\varepsilon} \cap S_{(1)} = S_{(4)};$$

$$H \cap S_{(1)} = \{(1), (5)\} S_{(8)}.$$

Proof. We prove the case $d \equiv 1 \pmod 4$ for the ideal groups corresponding to $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ and its sub-extensions; the other assertions are proved in a similar way.

Since $\mathbb{Q}(\sqrt{d}, i)/\mathbb{Q}(\sqrt{-d})$ is unramified, we have

$$H_{-1} \cap S_{(1)} = A_{(2)} \cap S_{(1)}.$$

It is not hard to show (for instance by the conductor-discriminant formula, theorem A.15) that the conductor of the abelian extension $\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ divides (4); hence $S_{(4)} \subseteq H_{2\varepsilon}$. As $\mathbb{Q}(\sqrt{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ is ramified, we have $H_{2\varepsilon} \cap S_{(1)} \neq A_{(2)} \cap S_{(1)}$. We infer that

$$[A_{(2)} \cap S_{(1)} : H_{2\varepsilon} \cap S_{(1)}] = [H_{-1} \cap S_{(1)} : H_{2\varepsilon} \cap S_{(1)}] = 2.$$

Since $(\sqrt{-d}) \in H_{2\varepsilon} \cap S_{(1)}$ (by proposition 2.7), we conclude that

$$H_{2\varepsilon} \cap S_{(1)} = \{(1), (\sqrt{-d})\} S_{(4)}.$$

It is not difficult to show (for instance by the conductor-discriminant formula) that the conductor of the extension $\mathbb{Q}(\sqrt[4]{2\varepsilon}, i)/\mathbb{Q}(\sqrt{-d})$ divides (8); hence $S_{(8)} \subseteq H$.

We prove the following

Claim: $(5) \in H$.

Proof of the claim: We consider the possibilities for d modulo 5:

$d \equiv 0, 1, 4 \pmod 5$: This is in proposition 2.11.

$d \equiv 2 \pmod 5$: From $u^2 + 3t^2 \equiv 1 \pmod 5$ we get $(u^2, t^2) \equiv (1, 0), (4, 4) \pmod 5$. If $(u^2, t^2) \equiv (1, 0) \pmod 5$, then

$$(u + t\sqrt{d})^{\frac{5^2-1}{4}} \equiv u^6 \equiv 1 \pmod 5.$$

If $(u^2, t^2) \equiv (4, 4) \pmod 5$, then

$$\begin{aligned}(u + t\sqrt{d})^3 &= u^3 + 3dut^2 + (3u^2t + dt^3)\sqrt{d} \\ &\equiv 4u + 4u + (2t + 3t)\sqrt{d} \\ &\equiv 3u \\ &\equiv \pm 1 \pmod 5,\end{aligned}$$

and so

$$(u + t\sqrt{d})^{\frac{5^2-1}{4}} \equiv 1 \pmod 5.$$

Hence this case follows from proposition 2.11.

$d \equiv 3 \pmod 5$: From $u^2 + 2t^2 \equiv 1 \pmod 5$ we get $(u^2, t^2) \equiv (1, 0), (4, 1) \pmod 5$. If $(u^2, t^2) \equiv (1, 0) \pmod 5$, then

$$(u + t\sqrt{d})^{\frac{5^2-1}{4}} \equiv u^6 \equiv 1 \pmod 5.$$

If $(u^2, t^2) \equiv (4, 1) \pmod 5$, then

$$\begin{aligned}(u + t\sqrt{d})^3 &= u^3 + 3dut^2 + (3u^2t + dt^3)\sqrt{d} \\ &\equiv 4u + 4u + (2t + 3t)\sqrt{d} \\ &\equiv 3u \\ &\equiv \pm 1 \pmod 5,\end{aligned}$$

and so

$$(u + t\sqrt{d})^{\frac{5^2-1}{4}} \equiv 1 \pmod 5.$$

Hence this case also follows from proposition 2.11. This proves the claim.

Since $H(A_{(2)} \cap S_{(1)})/H$ is cyclic and $H_{2\varepsilon} \neq H(A_{(2)} \cap S_{(1)})$, we have

$$\begin{aligned} & [\{(1), (\sqrt{-d})\}S_{(4)} : H \cap S_{(1)}] = 1 \\ \Rightarrow\ & [H_{2\varepsilon} \cap S_{(1)} : H \cap S_{(1)}] = 1 \\ \Rightarrow\ & [A_{(2)} \cap S_{(1)} : H \cap S_{(1)}] = [A_{(2)} \cap S_{(1)} : H_{2\varepsilon} \cap S_{(1)}] = 2 \\ \Rightarrow\ & \forall \mathfrak{a} = \mathfrak{h}(\alpha) \in H(A_{(2)} \cap S_{(1)}) :\ \mathfrak{a}^2 = \mathfrak{h}^2(\alpha)^2 \in H(H \cap S_{(1)}) \subseteq H \\ \Rightarrow\ & [H(A_{(2)} \cap S_{(1)}) : H] = 2 \\ \Rightarrow\ & H_{-1}/H \text{ is not cyclic.} \end{aligned}$$

Hence $[\{(1),(\sqrt{-d})\}S_{(4)} : H \cap S_{(1)}] = 2$. As

$$A_{(2)} \cap S_{(1)} = \{(1),(1+2\sqrt{-d}),(2+\sqrt{-d}),(\sqrt{-d})\}S_{(4)}$$

and

$$(\sqrt{-d})^2 \equiv -1, \quad (1+2\sqrt{-d})^2 \equiv 1 \pmod 4,$$

it follows that $A_{(2)} \cap S_{(1)} / S_{(4)} \simeq V_4$. Hence $H \cap S_{(1)} \neq S_{(4)}$. From $(5) \in H$ and

$$\begin{aligned}&\{(1),(5),(1+4\sqrt{-d}),(5+4\sqrt{-d}),(\sqrt{-d}),(5\sqrt{-d}),(4+\sqrt{-d}),(4+5\sqrt{-d})\}S_{(8)}\\ &= \{(1),(\sqrt{-d})\}S_{(4)} \supseteq H \cap S_{(1)} \supseteq S_{(8)}\end{aligned}$$

it follows that

$$H \cap S_{(1)} = \{(1),(5),(\sqrt{-d}),(5\sqrt{-d})\}S_{(8)}$$

or

$$H \cap S_{(1)} = \{(1),(5),(4+\sqrt{-d}),(4+5\sqrt{-d})\}S_{(8)}.$$

Since

$$H \cap S_{(1)} = \{(1),(5),(\sqrt{-d}),(5\sqrt{-d})\}S_{(8)} \;\Leftrightarrow\; (\sqrt{-d}) \in H \cap S_{(1)} \;\Leftrightarrow\; 2|\beta$$

(cf. proposition 2.8), we have proved what was asserted about $H \cap S_{(1)}$. □

2.5 Indices of the Subgroups of Principal Ideals

Let d_0 be the odd part of d. Write, as before,

$$d_0 = q_1 \cdots q_\alpha p_1 \cdots p_\beta$$

where the q_i are prime numbers of type I and the p_j are prime numbers of type II.

Let $r := \alpha + \beta$ (the number of odd prime factors of d).

Let the class number of $\mathbb{Q}(\sqrt{-d})$ be $h = h(\mathbb{Q}(\sqrt{-d})) = 2^z m, 2 \nmid m$ (by genus theory $r \leq z$, cf. lemma 1.6).

In order to make the statements of the next chapter (and the rest of this) easier to read we use an additional numbering of the odd prime factors of d: Let

$$\bar{p}_1, \ldots, \bar{p}_r$$

be the odd prime factors of d in some arbitrary, but fixed, order.

Let P_0 be the prime ideal in $\mathbb{Q}(\sqrt{-d})$ above 2. Let P_i be the prime ideal in $\mathbb{Q}(\sqrt{-d})$ above $\bar{p}_i$, $1 \le i \le r$.

We shall write $P_i \equiv a \pmod{b}$ (resp. say that P_i is of type I/II) if $\bar{p}_i \equiv a \pmod{b}$ (resp. if $\bar{p}_i$ is of type I/II), $1 \le i \le r$.

Lemma 2.13. *The indices of the subgroups of principal ideals in the ideal groups are given by:*

1. $d \equiv 1 \pmod{4}$:

$$[H_{-1} : H_{-1} \cap S_{(1)}] = [H : H \cap S_{(1)}] = h/2;$$

$$[H_\varepsilon : H_\varepsilon \cap S_{(1)}] = \begin{cases} h/4, & d \equiv 1 \pmod{8} \\ h/2, & d \equiv 5 \pmod{8} \end{cases}.$$

2. $2|d$:

$$[H_{-1} : H_{-1} \cap S_{(1)}] = [H_\varepsilon : H_\varepsilon \cap S_{(1)}] = [H : H \cap S_{(1)}] = h.$$

Proof. As $[A_{(2)} : A_{(2)} \cap S_{(1)}] = [A_{(1)} : S_{(1)}] = h$ (by proposition A.4), we calculate, using theorem 2.12:

$$\begin{aligned} 8[H : H \cap S_{(1)}] &= [A_{(2)} : H][H : H \cap S_{(1)}] \\ &= [A_{(2)} : A_{(2)} \cap S_{(1)}][A_{(2)} \cap S_{(1)} : H \cap S_{(1)}] \\ &= h \begin{cases} 4, & d \equiv 1 \pmod{4} \\ 8, & 2|d \end{cases}; \end{aligned}$$

$$\begin{aligned} 4[H_\varepsilon : H_\varepsilon \cap S_{(1)}] &= [A_{(2)} : H_\varepsilon][H_\varepsilon : H_\varepsilon \cap S_{(1)}] \\ &= [A_{(2)} : A_{(2)} \cap S_{(1)}][A_{(2)} \cap S_{(1)} : H_\varepsilon \cap S_{(1)}] \\ &= h \begin{cases} 1, & d \equiv 1 \pmod{8} \\ 2, & d \equiv 5 \pmod{8} \\ 4, & 2|d \end{cases}; \end{aligned}$$

$$\begin{aligned} 2[H_{-1} : H_{-1} \cap S_{(1)}] &= [A_{(2)} : H_{-1}][H_{-1} : H_{-1} \cap S_{(1)}] \\ &= [A_{(2)} : A_{(2)} \cap S_{(1)}][A_{(2)} \cap S_{(1)} : H_{-1} \cap S_{(1)}] \\ &= h \begin{cases} 1, & d \equiv 1 \pmod{4} \\ 2, & 2|d \end{cases}. \end{aligned}$$

□

Definition 2.14. Let G be a finite abelian group. Put

$$G_2 := \left\{ g \in G | g^2 = e \right\}.$$

G_2 is clearly an elementary abelian 2-group; a basis for G_2 will be called a 2-basis for G (or for G_2). The 2-rank of G (i.e. the number of elements in a 2-basis) will be denoted by $rank_2(G)$.

Proposition 2.15. *With notation as above we have:*

1. $d \equiv 1 \pmod 4 :$

$$rank_2(A_{(2)}/(A_{(2)} \cap S_{(1)})) = r,$$

and

$$\left\{ P_0 \left(\frac{1+\sqrt{-d}}{2} \right), P_1, \ldots, P_{r-1} \right\} (A_{(2)} \cap S_{(1)})$$

is 2-basis for $A_{(2)}/(A_{(2)} \cap S_{(1)})$.

2. $2|d :$

$$rank_2(A_{(2)}/A_{(2)} \cap S_{(1)}) = r,$$

and

$$\{P_1, \ldots, P_r\} (A_{(2)} \cap S_{(1)})$$

is a 2*–basis for* $A_{(2)}/(A_{(2)} \cap S_{(1)})$.

3. $d \equiv 5 \pmod 8 :$

$$rank_2(H/(H \cap S_{(1)})) = r - 1,$$

and

$$\{P_i | P_i \text{ is of type } I,\ 1 \leq i \leq r-1\} (H \cap S_{(1)}) \cup$$
$$\left\{ P_i(1+4\sqrt{-d}) | P_i \text{ is of type } II,\ 1 \leq i \leq r-1 \right\} (H \cap S_{(1)})$$

is a 2*–basis for* $H/(H \cap S_{(1)})$.

4. $2|d :$

$$rank_2(H/(H \cap S_{(1)})) = r,$$

and

$$\{P_i | P_i \text{ is of type } I,\ 1 \leq i \leq r\} (H \cap S_{(1)}) \cup$$
$$\left\{ P_i(1+4\sqrt{-d}) | P_i \text{ is of type } II,\ 1 \leq i \leq r \right\} (H \cap S_{(1)})$$

is a 2*–basis for* $H/(H \cap S_{(1)})$.

5. $d \equiv 1 \pmod 8$:

$$rank_2(H/H \cap S_{(1)}) = r.$$

6. $d \equiv 5 \pmod 8$:

$$rank_2(H_\varepsilon/(H_\varepsilon \cap S_{(1)})) = r - 1,$$

and

$$\left\{P_i(\sqrt{-d})|P_i \equiv 5 \pmod 8,\ 1 \leq i \leq r-1\right\}(H_\varepsilon \cap S_{(1)}) \cup$$
$$\{P_i|P_i \equiv 1 \pmod 8,\ 1 \leq i \leq r-1\}(H_\varepsilon \cap S_{(1)})$$

is a 2*–basis for* $H_\varepsilon/(H_\varepsilon \cap S_{(1)})$.

7. $2|d$:

$$rank_2(H_\varepsilon/(H_\varepsilon \cap S_{(1)})) = r,$$

and

$$\left\{P_i(1+2\sqrt{-d})|P_i \equiv 5 \pmod 8,\ 1 \leq i \leq r\right\}(H_\varepsilon \cap S_{(1)}) \cup$$
$$\{P_i|P_i \equiv 1 \pmod 8,\ 1 \leq i \leq r\}(H_\varepsilon \cap S_{(1)})$$

is a 2*–basis for* $H_\varepsilon/(H_\varepsilon \cap S_{(1)})$.

Proof. First we make two important observations:

i) Let d be odd. Then $P_1 \cdots P_r = (\sqrt{-d})$ is a principal ideal with a generator of positive norm (which, of course, is the case for every principal ideal). As $2, \bar{p}_1, \ldots, \bar{p}_r$ are the prime numbers dividing the discriminant of $\mathbb{Q}(\sqrt{-d})$, it follows from lemma 1.6 that P_0 and any $r-1$ of $P_1, \ldots, P_r$ constitute a 2–basis for $A_{(1)}/S_{(1)}$.

ii) Let d be even. Then $P_0 P_1 \cdots P_r = (\sqrt{-d})$ is a principal ideal. As $2, \bar{p}_1, \ldots, \bar{p}_r$ are the prime numbers dividing the discriminant of $\mathbb{Q}(\sqrt{-d})$, it follows from lemma 1.6 that any r of $P_0, P_1, \ldots, P_r$ constitute a 2–basis for $A_{(1)}/S_{(1)}$.

1. $d \equiv 1 \pmod 4$:

Since

$$A_{(2)}/(A_{(2)} \cap S_{(1)}) \simeq A_{(1)}/S_{(1)},$$

via the map $\mathcal{A}(A_{(2)} \cap S_{(1)}) \mapsto \mathcal{A}S_{(1)}$ (by proposition A.4), the assertion follows from i) and the fact that

$$P_0\left(\frac{1+\sqrt{-d}}{2}\right), P_1, \ldots, P_{r-1} \in A_{(2)}$$

$\left(2 \nmid \frac{1+d}{2} = N\left(P_0\left(\frac{1+\sqrt{-d}}{2}\right)\right) \Rightarrow P_0\left(\frac{1+\sqrt{-d}}{2}\right) \in A_{(2)}\right).$

2. $2|d$:

Since

$$A_{(2)}/(A_{(2)} \cap S_{(1)}) \simeq A_{(1)}/S_{(1)},$$

via the map $\mathcal{A}(A_{(2)} \cap S_{(1)}) \mapsto \mathcal{A}S_{(1)}$ (by proposition A.4), the assertion follows from ii) and the fact that

$$P_1, \ldots, P_r \in A_{(2)}.$$

4. $2|d$:

We have the isomorphism

$$H/(H \cap S_{(1)}) \simeq A_{(2)}/(A_{(2)} \cap S_{(1)}),\ \mathcal{A}(H \cap S_{(1)}) \mapsto \mathcal{A}S_{(1)},$$

since the embedding $H/(H \cap S_{(1)}) \hookrightarrow A_{(2)}/(A_{(2)} \cap S_{(1)}),\ \mathcal{A}(H \cap S_{(1)}) \mapsto \mathcal{A}S_{(1)}$, must be surjective by lemma 2.13.

By theorem 2.12 and propositions 2.8, 2.9, we have, for $i \geq 1$,

a) $P_i \in H$ for P_i of type I, and

b) $P_i(1+4\sqrt{-d}) \in H$ for P_i of type II
(since, for P_i of type II, we have $P_i, (1+4\sqrt{-d}) \in H_{2\varepsilon} \backslash H)$. Hence 4. follows from 2.

3. and 5. $d \equiv 1 \pmod 4$:

By lemma 2.13 we get, as above,

$$H/(H \cap S_{(1)}) \simeq H_{-1}/(H_{-1} \cap S_{(1)}) = H_{-1}/(A_{(2)} \cap S_{(1)})$$

where the equality is from theorem 2.12. From theorem 2.12 we have

$$\left(P_0\left(\frac{1+\sqrt{-d}}{2}\right)\right)^2 = \left(\frac{1-d}{2} + \sqrt{-d}\right) \begin{cases} \notin H_{2\varepsilon}, & d \equiv 5 \pmod 8 \\ \in H_{2\varepsilon}, & d \equiv 1 \pmod 8 \end{cases} .$$

Hence, as $A_{(2)}/H_{2\varepsilon} \simeq \mathbb{Z}/4$, we get

$$P_0\left(\frac{1+\sqrt{-d}}{2}\right) \begin{cases} \notin H_{-1}, & d \equiv 5 \pmod 8 \\ \in H_{-1}, & d \equiv 1 \pmod 8 \end{cases} .$$

Since also $P_1, \ldots, P_{r-1} \in H_{-1}$ (cf. proposition 2.7), $\big(H_{-1}/(A_{(2)} \cap S_{(1)})\big)_2$ must, for $d \equiv 5 \pmod 8$, be a $(r-1)$-dimensional $\mathbb{Z}/2$-subspace of $\big(A_{(2)}/(A_{(2)} \cap S_{(1)})\big)_2$ because exactly one of the r basis vectors

$$P_0\left(\frac{1+\sqrt{-d}}{2}\right)(A_{(2)}\cap S_{(1)}), P_1(A_{(2)}\cap S_{(1)}), \ldots, P_{r-1}(A_{(2)}\cap S_{(1)})$$

is not in the subspace. Hence for $d \equiv 5 \pmod 8$ the 2-rank must be $r-1$. For $d \equiv 1 \pmod 8$ the 2-rank is clearly r.

From theorem 2.12 we have $(1+4\sqrt{-d}) \in H_{2\varepsilon}\backslash H$; hence 3. follows from propositions 2.7 and 2.8.

6. $d \equiv 5 \pmod 8:$

By lemma 2.13 we get, as above,

$$H/(H \cap S_{(1)}) \simeq H_\varepsilon/(H_\varepsilon \cap S_{(1)});$$

hence, by 3., $rank_2(H_\varepsilon/(H_\varepsilon \cap S_{(1)})) = r-1$. As $(\sqrt{-d}) \in H_{-1}\backslash H_\varepsilon$ (by theorem 2.12), the claim about the 2–basis follows from propositions 2.7 ($H_{2\varepsilon} \subseteq H_{-1}$) and 2.9.

7. $2|d:$

By lemma 2.13 we get, as above,

$$H_\varepsilon/(H_\varepsilon \cap S_{(1)}) \simeq A_{(2)}/(A_{(2)} \cap S_{(1)});$$

hence, by 2., $rank_2(H_\varepsilon/(H_\varepsilon \cap S_{(1)})) = r$. As $(1+2\sqrt{-d}) \in H_{-1}\backslash H_\varepsilon$ (by theorem 2.12), the rest follows from propositions 2.7 and 2.9. □

Remark 2.16. In the next chapter we shall, from proposition 2.15, only use 1., 2. and the fact that the basis ideals in H and H_ε are contained in the given ideal group.

Chapter 3

Power Residue Criteria

We recall the relevant notation and assumptions.
Let $d > 1$ be a square-free integer. Let $\bar{p}_1, \ldots, \bar{p}_r$ be the odd prime factors of d. Let $\varepsilon_d = \frac{u+t\sqrt{d}}{2} > 1$ $(u, t \in \mathbb{Z})$ be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Assume that $N(\varepsilon_d) = -1$. We know that $\left(\frac{u}{\bar{p}_i}\right) = 1$, by remark 2.6. If u is a biquadratic residue modulo $\bar{p}_i$, we say that $\bar{p}_i$ is of type I; otherwise, $\bar{p}_i$ is of type II. Let β be the number of $\bar{p}_i$ of type II.
The symbol $\wedge$ will denote the logical 'and'; the symbol $\vee$ is the logical 'or'. Recall the discussion of the residue symbols just before remark 1.10.

3.1 The Criteria

Proofs of the results in this section can be found in the subsequent section.

Lemma 3.1. *Let $d > 1$ be a square-free integer and assume that $N(\varepsilon_d) = -1$. Let $p \equiv 1 \pmod 4$ be a prime number such that $\left(\frac{d}{p}\right) = 1$; let $\mathfrak{p}$ be one of the two prime ideals in $\mathbb{Q}(\sqrt{-d})$ above p. Let the class number of $\mathbb{Q}(\sqrt{-d})$ be $h(\mathbb{Q}(\sqrt{-d})) = 2^z m$, $2 \nmid m$.*
For $d \equiv 5 \pmod 8$ or $2 \mid d$: Assume that $\mathfrak{p}^{2m}$ is a principal ideal;
For $d \equiv 1 \pmod 8$: Assume that $\mathfrak{p}^m$ is a principal ideal
Then the following assertions hold:

1) $d \equiv 5 \pmod 8$: There is a relation

$$p^{m_0} = d_1 s^2 + d_2 v^2, \;\; s, v \in \mathbb{Z}\backslash\{0\}, \;\; d_1, d_2 \in \mathbb{N}, \;\; d_1 d_2 = d, \;\; \bar{p}_r \nmid d_1, \tag{3.1}$$

with m_0 minimal (this implies $m_0 \mid m$). With this m_0 the absolute values $|s|$, $|v|$ in *a relation as in (3.1) are uniquely determined. Put*

$$\Sigma_1 := \textit{the number of prime factors of } d_1 \textit{ of type II (with respect to } d).$$

2) $2 \mid d:$ *There is a relation*

$$p^{m_0} = d_1 s^2 + d_2 v^2, \ \ s, v \in \mathbb{Z}\backslash\{0\}, \ \ d_1, d_2 \in \mathbb{N}, \ \ d_1 d_2 = d, \ \ 2 \nmid d_1, \tag{3.2}$$

with m_0 *minimal (this implies* $m_0 \mid m$*). With this* m_0 *the absolute values* $|s|$*,* $|v|$ *in a relation as in (3.2) are uniquely determined. Put*

$$\Sigma_2 := \textit{the number of prime factors of } d_1 \textit{ of type II (with respect to } d).$$

3) $d \equiv 1 \pmod 8 : \quad \exists\ s, v \in \mathbb{Z}\backslash\{0\}, \ \textit{minimal odd } n_0 \in \mathbb{N}: \quad p^{n_0} = s^2 + dv^2.$

And this is equivalent to $\mathfrak{p}^m$ *being a principal ideal*

Theorem 3.2. *Let the assumptions and the notation be as in lemma 3.1. Then*

$$\left(\frac{\varepsilon_d}{p}\right) = (-1)^{\frac{p-1}{4} + \frac{sv}{2}}.$$

Remark 3.3. Clearly, if $2 \mid d$, then this can be written as $\left(\frac{\varepsilon_d}{p}\right) = (-1)^{\frac{p-1}{4} + \frac{v}{2}}$; and if $d \equiv 1 \pmod 8$, then we have $\left(\frac{\varepsilon_d}{p}\right) = 1$.

Theorem 3.4. *Let the assumptions and the notation be as in lemma 3.1. Let* $d \equiv 5 \pmod 8$*. Let* $p \equiv 1 \pmod 8$ *and write* $p = a^2 + 16b^2$*,* $a, b \in \mathbb{Z}$*. Then for*

i) $2 \mid \beta:$

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \quad \Leftrightarrow$$

$$(2 \mid b \ \wedge \ ((2 \mid \Sigma_1 \ \wedge \ 8 \mid sv) \ \vee \ (2 \nmid \Sigma_1 \ \wedge \ 4 || sv))) \ \vee$$

$$(2 \nmid b \ \wedge \ ((2 \mid \Sigma_1 \ \wedge \ 4 || sv) \ \vee \ (2 \nmid \Sigma_1 \ \wedge \ 8 \mid sv)));$$

ii) $2 \nmid \beta:$

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \quad \Leftrightarrow$$

$$(2 \mid b \ \wedge \ ((2 \mid \Sigma_1 \ \wedge \ (4 || s \ \vee \ 8 \mid v)) \ \vee \ (2 \nmid \Sigma_1 \ \wedge \ (8 \mid s \ \vee \ 4 || v)))) \ \vee$$

$$(2 \nmid b \ \wedge \ ((2 \mid \Sigma_1 \ \wedge \ (8 \mid s \ \vee \ 4 || v)) \ \vee \ (2 \nmid \Sigma_1 \ \wedge \ (4 || s \ \vee \ 8 \mid v)))).$$

Theorem 3.5. *Let the assumptions and the notation be as in lemma 3.1. Let* $2|d$. *Let* $p \equiv 1 \pmod 8$ *and write* $p = a^2 + 16b^2,\ a, b \in \mathbb{Z}$. *Then*

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \quad \Leftrightarrow$$
$$(2 \mid b \ \wedge \ ((2 \mid \Sigma_2 \ \wedge \ 8 \mid v) \ \vee \ (2 \nmid \Sigma_2 \ \wedge \ 4||v))) \vee$$
$$(2 \nmid b \ \wedge \ ((2 \mid \Sigma_2 \ \wedge \ 4||v) \ \vee \ (2 \nmid \Sigma_2 \ \wedge \ 8 \mid v))).$$

Theorem 3.6. *Let the assumptions and the notation be as in lemma 3.1. Let* $d \equiv 1 \pmod 8$. *Let* $p \equiv 1 \pmod 8$ *and write* $p = a^2 + 16b^2,\ a, b \in \mathbb{Z}$. *Then for*

i) $2 \mid \beta$:
$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \quad \Leftrightarrow \quad (2 \mid b \ \wedge \ 8 \mid sv) \ \vee \ (2 \nmid b \ \wedge \ 8 \nmid sv);$$

ii) $2 \nmid \beta$:
$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \quad \Leftrightarrow \quad (2 \mid b \ \wedge \ (4||s \ \vee \ 8 \mid v)) \ \vee \ (2 \nmid b \ \wedge \ 4 \not\| s \ \wedge \ 8 \nmid v).$$

Remark 3.7. If $N(\varepsilon_d) = -1$ and the 2-class group of $\mathbb{Q}(\sqrt{-d})$ is elementary abelian, then the condition about $\mathfrak{p}^{2m}$ being principal is clearly fulfilled for all p and it is not hard to show that $d \equiv 5 \pmod 8$ or $2 \mid d$. So the theorems 3.4 and 3.4 cover this case.

3.2 Proofs of the Criteria

We now turn to the proofs of the results of the previous section. We concentrate on $d \equiv 5 \pmod 8$; the other cases are similar.

In $\mathbb{Q}(\sqrt{-d})$, conjugation is denoted by α' etc.

We work in the group $G := A_{(2)}/(A_{(2)} \cap S_{(1)})$. The assumption about $\mathfrak{p}^{2m}$ means that $\mathfrak{p}^m(A_{(2)} \cap S_{(1)})$ has order 1 or 2 in G. Hence, by proposition 2.15, we have

$$\mathfrak{p}^m \left(P_0 \left(\frac{1+\sqrt{-d}}{2}\right)\right)^{a_0} P_1^{a_1} \cdots P_{r-1}^{a_{r-1}} = (s + v\sqrt{-d}) \in A_{(2)} \cap S_{(1)} \tag{3.3}$$

for suitable $a_0, \ldots, a_{r-1} \in \{0, 1\}$ and $s, v \in \mathbb{Z}$. (Recall that, by the notation of section 2.5, $d = \bar{p}_1 \cdots \bar{p}_r$, and if we put $p_0 = 2$, then P_i is the prime ideal in $\mathbb{Q}(\sqrt{-d})$ above $p_i,\ i = 0, 1, \ldots, r$.) By taking norms, we get

$$p^m \left(\frac{1+d}{2}\right)^{a_0} \bar{p}_1^{a_1} \cdots \bar{p}_{r-1}^{a_{r-1}} = s^2 + dv^2. \tag{3.4}$$

Since $\frac{1+d}{2} \equiv 3 \pmod 4$ and $s^2+dv^2, \bar{p}_i, p \equiv 1 \pmod 4$, we must have $a_0 = 0$ (this is where we use that $d \equiv 5 \pmod 8$ and not just $d \equiv 1 \pmod 4$). We can not have $v = 0$; for then, as $P_i' = P_i$, (3.3) would imply that $\mathfrak{p}' = \mathfrak{p}$. If $s = 0$, (3.4) would imply that $p = \bar{p}_r$. This proves the existence of a minimal m_0 as claimed.

Now we prove the asserted uniqueness. Let an equation as (3.1) be given. By considering the norm map, it follows that

$$\mathfrak{p}^{x_0}(\mathfrak{p}')^{y_0} P_1^{a_1} \cdots P_1^{a_{r-1}} = (s + v\sqrt{-d}) \tag{3.5}$$

for some $x_0, y_0 \in \mathbb{N}_0$ with $x_0 + y_0 = m_0$ and $a_0, \ldots, a_{r-1} \in \{0,1\}$. Since

$$x_0 = y_0 \;\Rightarrow\; (s + v\sqrt{-d}) = (s + v\sqrt{-d})' \;\Rightarrow\; sv = 0,$$

we have $x_0 \neq y_0$. Since a change of sign of v conjugates the ideal $(s + v\sqrt{-d})$, it follows from (3.5) that we can assume that $y_0 < x_0$. We can write (3.5) as

$$\mathfrak{p}^{x_0 - y_0} P_1^{a_1} \cdots P_1^{a_{r-1}} = \left(\frac{s}{p^{y_0}} + \frac{v}{p^{y_0}}\sqrt{-d}\right)$$

where necessarily $\frac{s}{p^{y_0}}, \frac{v}{p^{y_0}} \in \mathbb{Z}\backslash\{0\}$ since the ideal on the left is an integral ideal and since $-d \equiv 3 \pmod 4$. From the minimality of m_0 we conclude that $x_0 - y_0 = m_0$, i.e. $x_0 = m_0$ and $y_0 = 0$. Hence

$$\mathfrak{p}^{m_0} P_1^{a_1} \cdots P_{r-1}^{a_{r-1}} = (s + v\sqrt{-d}). \tag{3.6}$$

Since, because of this equation, $\mathfrak{p}^{m_0}(A_{(2)} \cap S_{(1)})$ has order 1 or 2 in G, the uniqueness of the a_i follows from proposition 2.15; the uniqueness of the absolute values $|s|$, $|v|$ now follows from (3.6).

We need to show that $m_0 | m$. We first show that m_0 is odd. Assume that $2 | m_0$. As $4 \nmid ord(\mathfrak{p}(A_{(2)} \cap S_{(1)}))$, it follows from (3.6) that $a_1 = \cdots = a_{r-1} = 0$; hence $\mathfrak{p}^{m_0} = (s + v\sqrt{-d})$. Since $\mathfrak{p}^m(A_{(2)} \cap S_{(1)})$ has order 1 or 2, there are $b_1, \ldots, b_{r-1} \in \{0,1\}$ and $s', v' \in \mathbb{Z}\backslash\{0\}$ with

$$\mathfrak{p}^m P_1^{b_1} \cdots P_{r-1}^{b_{r-1}} = (s' + v'\sqrt{-d}). \tag{3.7}$$

(We remove a factor $\left(P_0\left(\frac{1+\sqrt{-d}}{2}\right)\right)^{b_0}$ as before.) Since $m_0 \nmid m$, we can write

$$m = km_0 + g, \quad 0 < g < m_0.$$

Combining the equations (3.6) and (3.7), we find

$$\mathfrak{p}^g P_1^{b_1} \cdots P_{r-1}^{b_{r-1}} = (s' + v'\sqrt{-d})/(s + v\sqrt{-d})^k =: (e + f\sqrt{-d})$$

where necessarily $e, f \in \mathbb{Z}$ since the ideal on the left is an integral ideal and since $-d \equiv 3 \pmod 4$. Taking norms, we get

$$p^g \bar{p}_1^{b_1} \cdots \bar{p}_{r-1}^{b_{r-1}} = e^2 + df^2.$$

We have $f \neq 0$ since the left-hand side is not a square (as $2 \nmid g$); and $e \neq 0$ since otherwise the last equation would imply that $p = \bar{p}_r$. As $g < m_0$, we have obtained a contradiction to the minimality of m_0. Hence m_0 is odd.

Put A:=ord($\mathfrak{p}(A_{(2)} \cap S_{(1)})$). Put

$$A' := \begin{cases} A, & 2 \nmid A \\ A/2, & 2|A \end{cases}.$$

As before we choose $c_1, \dots, c_{r-1} \in \{0, 1\}$ and $e, f \in \mathbb{Z}$ with

$$\mathfrak{p}^{A'} P_1^{c_1} \cdots P_{r-1}^{c_{r-1}} = (e + f\sqrt{-d}).$$

From

$$p^{A'} \bar{p}_1^{c_1} \cdots \bar{p}_{r-1}^{c_{r-1}} = e^2 + df^2$$

we easily get $e, f \neq 0$ (A' is odd); and hence, by minimality of m_0, the inequality $A' \geq m_0$ holds. If $2 \nmid A$, then

$$m_0 \leq A' = A \leq m_0,$$

hence $A = m_0$ (and all $a_i = 0$); if $2|A$, then

$$2m_0 \leq 2A' = A \leq 2m_0,$$

hence $A = 2m_0$ (and there is an i with $a_i = 1$) (we used (3.6) to get the last inequality in both cases). From $m_0|A|2m$ and the fact that m_0 is odd it follows that $m_0|m$.

We now put $d_1 := \bar{p}_1^{a_1} \cdots \bar{p}_{r-1}^{a_{r-1}}$ (and $d_2 = d/d_1$). Let $a_r := 0$. Note that

$$\Sigma_1 = \sum_{p_i \textit{ of type II}} a_i.$$

Put

$$\Sigma_a := \sum_{p_i \equiv 5 \pmod 8} a_i.$$

First we claim that

$$v \equiv \Sigma_a \pmod 2 \Leftrightarrow (4|sv \ \wedge \ p \equiv 1 \pmod 8) \vee (4 \nmid sv \ \wedge \ p \equiv 5 \pmod 8)).$$

Since $s \not\equiv v \pmod 2$ and m_0 is odd, we have (from (3.1)) the following 4 observations which prove the claim:

$$\begin{aligned}
v \equiv \Sigma_a \equiv 0 \pmod 2 \quad &\Rightarrow \quad 2|v \;\wedge\; s^2 + dv^2 \equiv p \pmod 8 \\
&\Rightarrow \quad \left\{ \begin{array}{ll} 2||v, & p \equiv 5 \pmod 8 \\ 4|v, & p \equiv 1 \pmod 8 \end{array} \right. ;
\end{aligned}$$

$$\begin{aligned}
v \equiv \Sigma_a \equiv 1 \pmod 2 \quad &\Rightarrow \quad 2|s \;\wedge\; s^2 + dv^2 \equiv 5p \pmod 8 \\
&\Rightarrow \quad \left\{ \begin{array}{ll} 2||s, & p \equiv 5 \pmod 8 \\ 4|s, & p \equiv 1 \pmod 8 \end{array} \right. ;
\end{aligned}$$

$$\begin{aligned}
v \not\equiv \Sigma_a \equiv 0 \pmod 2 \quad &\Rightarrow \quad 2|s \;\wedge\; s^2 + dv^2 \equiv p \pmod 8 \\
&\Rightarrow \quad \left\{ \begin{array}{ll} 4|s, & p \equiv 5 \pmod 8 \\ 2||s, & p \equiv 1 \pmod 8 \end{array} \right. ;
\end{aligned}$$

$$\begin{aligned}
v \not\equiv \Sigma_a \equiv 1 \pmod 2 \quad &\Rightarrow \quad 2|v \;\wedge\; s^2 + dv^2 \equiv 5p \pmod 8 \\
&\Rightarrow \quad \left\{ \begin{array}{ll} 4|v, & p \equiv 5 \pmod 8 \\ 2||v, & p \equiv 1 \pmod 8 \end{array} \right. .
\end{aligned}$$

Since m_0 is odd, we get, using proposition 2.15 and theorem 2.12,

$$\begin{aligned}
\mathfrak{p} \in H_\varepsilon \quad &\Leftrightarrow \quad \mathfrak{p}^{m_0} \in H_\varepsilon \\
&\Leftrightarrow \quad \mathfrak{p}^{m_0} \cdot \prod_{p_i \equiv 5 \pmod 8} (P_i(\sqrt{-d}))^{a_i} \cdot \prod_{p_i \equiv 1 \pmod 8} P_i^{a_i} \in H_\varepsilon \\
&\Leftrightarrow \quad (2 \mid \Sigma_a \;\wedge\; (s + v\sqrt{-d}) \in H_\varepsilon) \;\vee \\
&\qquad\quad (2 \nmid \Sigma_a \;\wedge\; (s + v\sqrt{-d})(\sqrt{-d}) \in H_\varepsilon) \\
&\Leftrightarrow \quad (2 \mid \Sigma_a \;\wedge\; 2 \mid v) \;\vee\; (2 \nmid \Sigma_a \;\wedge\; 2 \nmid v) \\
&\Leftrightarrow \quad v \equiv \Sigma_a \pmod 2 \\
&\Leftrightarrow \quad (4 \mid sv \;\wedge\; p \equiv 1 \pmod 8) \;\vee\; (4 \nmid sv \;\wedge\; p \equiv 5 \pmod 8)
\end{aligned}$$

and

$$\begin{aligned}
\mathfrak{p} \in H \quad &\Leftrightarrow \quad \mathfrak{p}^{m_0} \in H \\
&\Leftrightarrow \quad \mathfrak{p}^{m_0} \cdot \prod_{p_i \textit{ of type I}} P_i^{a_i} \cdot \prod_{p_i \textit{ of type II}} (P_i(1 + 4\sqrt{-d}))^{a_i} \in H \\
&\Leftrightarrow \quad (2 \mid \Sigma_1 \;\wedge\; (s + v\sqrt{-d}) \in H) \;\vee \\
&\qquad\quad (2 \nmid \Sigma_1 \;\wedge\; (s + v\sqrt{-d})(1 + 4\sqrt{-d}) \in H) \\
&\Leftrightarrow \quad \left\{ \begin{array}{ll} (2 \mid \Sigma_1 \;\wedge\; 8 \mid sv) \;\vee\; (2 \nmid \Sigma_1 \;\wedge\; 4||sv), & 2 \mid \beta \\ (2 \mid \Sigma_1 \;\wedge\; (4||s \;\vee\; 8 \mid v)) \;\vee\; (2 \nmid \Sigma_1 \;\wedge\; (8 \mid s \;\vee\; 4||v)), & 2 \nmid \beta \end{array} \right. .
\end{aligned}$$

Note that $\left(\frac{\varepsilon_d}{p}\right) = 1$ if and only if $\mathfrak{p} \in H_\varepsilon$ and that $\left(\frac{\varepsilon_d}{p}\right)_4 = 1$ if and only if $\mathfrak{p} \in H_\varepsilon \wedge\ ((2 \mid b\ \wedge\ \mathfrak{p} \in H)\ \vee\ (2 \nmid b\ \wedge\ \mathfrak{p} \notin H))$, cf. observation 1.10 and proposition 2.4. From this it is routine to deduce the criteria in the previous section. Note that $\left(\frac{2}{p}\right)_4 = 1$ is equivalent to $2 \mid b$ (if $p = a^2 + 16b^2$), cf. remark 1.13.

3.3 A Similar Result

We give a general result for d even.

Theorem 3.8. *Let $d > 1$ be square-free and even, and assume that $N(\varepsilon_d) = -1$. Let $p \equiv 1 \pmod 4$ be a prime number with $\left(\frac{d}{p}\right) = 1$. Let the class number of $\mathbb{Q}(\sqrt{-d})$ be $h = h(\mathbb{Q}(\sqrt{-d})) = 2^z m,\ 2 \nmid m$. For $p \equiv 1 \pmod 8$ we write $p = a^2 + 16b^2$, $a, b \in \mathbb{Z}$.*

1) There are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in H$ such that

$$\mathfrak{p}_1(A_{(2)} \cap S_{(1)}), \ldots, \mathfrak{p}_r(A_{(2)} \cap S_{(1)})$$

is a basis for the finite abelian group

$$Syl_2(A_{(2)}/(A_{(2)} \cap S_{(1)})).$$

In fact, each of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ can be chosen in infinitely many ways. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be fixed in what follows. Put $g_i := ord(\mathfrak{p}_i(A_{(2)} \cap S_{(1)})) - 1$.
2) There are prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in H_\varepsilon$ such that

$$\mathfrak{q}_1(A_{(2)} \cap S_{(1)}), \ldots, \mathfrak{q}_r(A_{(2)} \cap S_{(1)})$$

is a basis for the finite abelian group

$$Syl_2(A_{(2)}/(A_{(2)} \cap S_{(1)}));$$

In fact, each of $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ can be chosen in infinitely many ways. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be fixed. Put $g_i' := ord(\mathfrak{q}_i(A_{(2)} \cap S_{(1)})) - 1$.
3) The norms of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are prime numbers; put $\hat{p}_i := N(\mathfrak{p}_i)$ and $\hat{q}_i := N(\mathfrak{q}_i)$.
4) Let $p \notin \{\hat{p_1}, \ldots, \hat{p_r}\}$. There is a minimal odd $m_0 \in \mathbb{N}$ such that

$$p^{m_0} \hat{p}_1^{a_1} \cdots \hat{p}_r^{a_r} = s^2 + dv^2 \tag{3.8}$$

for suitable $a_i \in \{0, 1, \ldots, g_i\}$; $s, v \in \mathbb{Z} \backslash \{0\}$. This minimal odd m_0 satisfies $m_0 \leq m$. Let a relation (3.8) (with minimal odd m_0) be fixed.

5) Let $p \notin \{\hat{q}_1, \ldots, \hat{q}_r\}$. *There is a minimal odd* $m_0' \in \mathbb{N}$ *such that*

$$p^{m_0'} \hat{q}_1^{a_1'} \cdots \hat{q}_r^{a_r'} = (s')^2 + d(v')^2 \tag{3.9}$$

for suitable $a_i' \in \{0, 1, \ldots, g_i'\}$; $s', v' \in \mathbb{Z} \backslash \{0\}$. *This minimal odd* m_0' *satisfies* $m_0' \leq m$. *Let a relation (3.9) (with minimal odd* m_0'*) be fixed.*
6) Let $p \notin \{\hat{q}_1, \ldots, \hat{q}_r\}$. *Then, with the above notation,*

$$\left(\frac{\varepsilon_d}{p}\right) = 1 \quad \Leftrightarrow \quad 4 \mid v'.$$

7) Let $\{\hat{p}_1, \ldots, \hat{p}_r, \hat{q}_1, \ldots, \hat{q}_r\} \not\ni p \equiv 1 \pmod 8$. *Then, with the above notation,*

$$\left(\frac{\varepsilon_d}{p}\right)_4 = 1 \quad \Leftrightarrow \quad 4 \mid v' \ \wedge \ ((2 \mid b \ \vee \ 8 \mid v) \ \vee \ (2 \nmid b \ \vee \ 8 \nmid v)).$$

Proof. 1)+2) The two maps

$$H/(H \cap S_{(1)}) \longrightarrow A_{(2)}/(A_{(2)} \cap S_{(1)}),$$
$$\mathcal{A}(H \cap S_{(1)}) \ \mapsto \ \mathcal{A}(A_{(2)} \cap S_{(1)})$$

and

$$H_\varepsilon/(H_\varepsilon \cap S_{(1)}) \longrightarrow A_{(2)}/(A_{(2)} \cap S_{(1)}),$$
$$\mathcal{A}(H_\varepsilon \cap S_{(1)}) \ \mapsto \ \mathcal{A}(A_{(2)} \cap S_{(1)})$$

are clearly well defined and injective. By lemma 2.13 they must be surjective. Hence 1) (resp. 2)) follows from the fact that every coset of $H/(H \cap S_{(1)})$ (resp. $H_\varepsilon/(H_\varepsilon \cap S_{(1)})$) contains infinitely many prime ideals.
3) None of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_r$ is a principal ideal, and hence none of them is above an inert prime number; this proves 3).
4) Let $\mathfrak{p}$ be one of the two prime ideals in $\mathbb{Q}(\sqrt{-d})$ above p. Since

$$\mathfrak{p}^m(A_{(2)} \cap S_{(1)}) \in Syl_2(A_{(2)}/(A_{(2)} \cap S_{(1)})),$$

there are $k_i \in \{0, 1, \ldots, g_i\}$; $e, f \in \mathbb{Z}$ such that

$$\mathfrak{p}^m \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r} = (e + f\sqrt{-d}).$$

Taking norms we get

$$p^m \hat{p}_1^{k_1} \cdots \hat{p}_r^{k_r} = e^2 + df^2$$

So we can consider a relation (3.8) with minimal odd m_0 and $s, v \in \mathbb{Z}$; as m_0 is odd, $p, \hat{p}_1, \ldots, \hat{p}_r \neq 2$, and $2|d$, we must have $s, v \neq 0$.
5) This is completely analogous to 4).

6)+7) By considering the norm map we get from (3.8) for suitable $b_i, c_i \in \mathbb{N}_0$ with $b_i + c_i = a_i$ that

$$\mathfrak{p}^{x_0}(\mathfrak{p}')^{y_0}\mathfrak{p}_1^{b_1}(\mathfrak{p}_1')^{c_1}\cdots\mathfrak{p}_r^{b_r}(\mathfrak{p}_r')^{c_r} = (s + v\sqrt{-d})$$

where $x_0, y_0 \in \mathbb{N}_0$ with $x_0 + y_0 = m_0$. By changing sign (if necessary) of sv we can assume that $x_0 \geq y_0$. The minimality of m_0 implies that $p \nmid sv$; hence $y_0 = 0$ and $x_0 = m_0$ (otherwise $(p) = \mathfrak{p}\mathfrak{p}' | (s + v\sqrt{-d})$ and so $p|s, v$).

From (3.9) we get (in a similar way) for a suitable choice of sign of $s'v'$ and suitable $b_i', c_i' \in \mathbb{N}_0$ with $b_i' + c_i' = a_i'$ that

$$\mathfrak{q}^{m_0'}\mathfrak{q}_1^{b_1'}(\mathfrak{p}_1')^{c_1'}\cdots\mathfrak{p}_r^{b_r'}(\mathfrak{p}_r')^{c_r'} = (s' + v'\sqrt{-d}).$$

Hence (since $\mathfrak{p}_i' \in H$ and $\mathfrak{q}_i' \in H_\varepsilon$ by proposition 2.10)

$$\begin{aligned}
\mathfrak{p} \in H \quad &\Leftrightarrow \quad \mathfrak{p}^{m_0} \in H \\
&\Leftrightarrow \quad \mathfrak{p}^{m_0}\mathfrak{p}_1^{b_1}(\mathfrak{p}_1')^{c_1}\cdots\mathfrak{p}_r^{b_r}(\mathfrak{p}_r')^{c_r} \in H \\
&\Leftrightarrow \quad (s + v\sqrt{-d}) \in H \\
&\Leftrightarrow \quad 8|v,
\end{aligned}$$

and

$$\begin{aligned}
\mathfrak{p} \in H_\varepsilon \quad &\Leftrightarrow \quad \mathfrak{p}^{m_0'} \in H_\varepsilon \\
&\Leftrightarrow \quad \mathfrak{p}^{m_0'}\mathfrak{q}_1^{b_1'}(\mathfrak{q}_1')^{c_1'}\cdots\mathfrak{q}_r^{b_r'}(\mathfrak{q}_r')^{c_r'} \in H_\varepsilon \\
&\Leftrightarrow \quad (s' + v'\sqrt{-d}) \in H_\varepsilon \\
&\Leftrightarrow \quad 4|v'.
\end{aligned}$$

6) and 7) follow from this. □

Part II

Relative Norms of Units and 4-rank of Class Groups

Chapter 4

Cyclic Extensions of Prime Degree

4.1 General Observations

In this section, we see that the problem about surjectivity of the relative norm map between unit groups for certain cyclic extensions of prime degree is related to the ambiguous ideals of the extension.

Definition 4.1. Let L/K be a cyclic extension of number fields with Galois group $Gal(L/K) =< \sigma >$.

An ideal $\mathfrak{a}$ of L is called ambiguous (with respect to K) if it is fixed by σ: $\sigma(\mathfrak{a}) = \mathfrak{a}$.

An ideal class $[\mathfrak{a}]$ of L is called ambiguous (with respect to K) if it is fixed by σ: $\sigma([\mathfrak{a}]) = [\mathfrak{a}]$. The group of ambiguous ideal classes is denoted by $Am(L/K)$.

An ideal class $[\mathfrak{a}]$ of L is called strongly ambiguous (with respect to K) if it contains an ambiguous ideal. The group of strongly ambiguous ideal classes is denoted by $Am_s(L/K)$. Clearly, $Am_s(L/K) \subseteq Am(L/K)$.

We begin by citing Holzer [14] (Satz 2, p. 115):

Lemma 4.2. *Let L/K be a cyclic extension of number fields of prime degree. Then the following are equivalent*

1) $\mathcal{O}_K^* \cap N_{L/K}(L^*) = N_{L/K}(\mathcal{O}_L^*)$,
i.e. every unit of $\mathcal{O}_K$ which is a relative norm of a number of L is a relative norm of a unit of $\mathcal{O}_L$.

2) $Am_s(L/K) = Am(L/K)$,
i.e. every ambiguous ideal class is strongly ambiguous.

The following lemma is well known and easily proved.

Lemma 4.3. *Let L/K be a quadratic extension of algebraic number fields. Suppose that $2 \nmid h(K)$. Then the 2-Sylow subgroup $Am_2(L/K)$ of the group of ambiguous ideal classes is given by*

$$Am_2(L/K) = \left\{[\mathfrak{a}]_L \in Cl(L) \middle| [\mathfrak{a}]_L^2 = [(1)]_L\right\};$$

and hence

$$|Am_2(L/K)| = [Cl(L) : Cl(L)^2] = 2^{rank_2(Cl(L))}.$$

In particular,

$$2 \mid h(L) \;\Leftrightarrow\; 2 \mid |Am_2(L/K)|.$$

Proposition 4.4. *Let L/K be a cyclic extension of number fields with $[L : K] = l$ a prime. Assume that $l \nmid h(K)$. Let t' be the number of (not necessarily finite) ramified primes of L/K. (By class field theory, we must have $t' \geq 1$.) Let $\mathfrak{p}_1, \dots \mathfrak{p}_t \subseteq \mathcal{O}_L$ be the finite, ramified primes of the extension L/K (possibly $t = 0$). For l odd, suppose that $t' = t$. Then*

$$|\left\{[\mathfrak{p}_1^{a_1} \dots \mathfrak{p}_t^{a_t}]_L \middle| 0 \leq a_i \leq l-1\right\}| \leq l^{t'-1};$$

and the following are equivalent:

1) $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$.

2) $|\left\{[\mathfrak{p}_1^{a_1}, \dots \mathfrak{p}_t^{a_t}]_L \middle| 0 \leq a_i \leq l-1\right\}| = l^{t'-1}$

Proof. Using the ambiguous class number formula (§ 13, lemma 4.1 of [18]),

$$|Am(L/K)| = \frac{h(K) l^{t'-1}}{[\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*]},$$

and the fact that the map $Cl(K) \to Cl(L)$, $[\mathfrak{a}]_K \mapsto [\mathfrak{a}]_L$, is injective (since $l \nmid h(K)$, cf. [20], Corollary p. 190) it is not hard to see that the group $Am_s(L/K)$ of strongly ambiguous ideal classes of L/K is the product of the subgroups

$$\left\{[\mathfrak{p}_1^{a_1}, \dots \mathfrak{p}_t^{a_t}]_L \middle| 0 \leq a_i \leq l-1\right\} \quad \text{and} \quad \left\{[\mathfrak{a}]_L \middle| \; \mathfrak{a} \text{ fractional ideal in } K\right\}$$

where the first factor is the l-Sylow subgroup (allowing the trivial subgroup if $t = 0$) of $Am_s(L/K)$ and the second factor has order $h(K)$.

It follows that

$$\begin{aligned} |\left\{[\mathfrak{p}_1^{a_1},\dots \mathfrak{p}_t^{a_t}]_L \middle| 0 \le a_i \le l-1\right\}|h(K) &= |Am_s(L/K)| \\ &\le |Am(L/K)| \\ &= \frac{h(K)l^{t'-1}}{[\mathcal{O}_K^* : N_{L/K}(L^*)\cap \mathcal{O}_K^*]} \end{aligned}$$

This and lemma 4.2 give:

$$\begin{aligned} & N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^* \\ \Leftrightarrow\quad & N_{L/K}(\mathcal{O}_L^*) = N_{L/K}(L^*)\cap \mathcal{O}_K^* \text{ and } N_{L/K}(L^*)\cap \mathcal{O}_K^* = \mathcal{O}_K^* \\ \Leftrightarrow\quad & |Am_s(L/K)| = |Am(L/K)| \text{ and } N_{L/K}(L^*)\cap \mathcal{O}_K^* = \mathcal{O}_K^* \\ \Leftrightarrow\quad & |\left\{[\mathfrak{p}_1^{a_1},\dots \mathfrak{p}_t^{a_t}]_L \middle| 0 \le a_i \le l-1\right\}| = l^{t'-1} \end{aligned}$$

□

Corollary 4.5. *Let L/K be a cyclic extension of number fields with $[L : K] = l$ a prime number. Assume that $l \nmid h(K)$. Assume that exactly one prime (which is assumed to be finite, if l is odd) of K ramifies in L. Then*

$$N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$$

Remark 4.6. In particular, we get the well-known result that if p is a prime number congruent to 1 modulo 4, then the negative Pell equation $x^2 - py^2 = -1$ is solvable.

4.2 A Sufficient Condition for Surjectivity

In this section, we prove a theorem which is a generalization of theorem 1.19.

Let l be a prime number. Let K be an algebraic number field that contains the l'th roots of unity and assume that $l \nmid h(K)$; let $\pi_1,\dots,\pi_t \in \mathcal{O}_K$, $t \ge 2$, such that $(\pi_1),\dots,(\pi_t)$ are distinct prime ideals. Assume that no prime different from (π_i) is ramified in the extension $K(\sqrt[l]{\pi_i})/K$. Let $\beta_1,\dots,\beta_t \in \{1,\dots,l-1\}$; put $\alpha := \pi_1^{\beta_1}\cdots\pi_t^{\beta_t}$. Let $\mathfrak{p}_i \subseteq \mathcal{O}_{K(\sqrt[l]{\alpha})}$ be the prime ideal above (π_i).

Definition 4.7. Let the notation be as above.
i) We use the Artin symbol to define the $t\times t$ *left Redei matrix* $M = [M_{ij}] = M_{K(\sqrt[l]{\alpha})/K}$ with coefficients in $\mathbb{F}_l$ (the field with l elements) corresponding to the extension $K(\sqrt[l]{\alpha})/K$ in the following way:

For $i \neq j$, we let $M_{ij} := k$ if

$$\left(\frac{K(\sqrt[l]{\alpha}, \sqrt[l]{\pi_j})/K(\sqrt[l]{\alpha})}{\mathfrak{p}_i}\right)(\sqrt[l]{\pi_j})\Big/\sqrt[l]{\pi_j} = e^{\frac{2\pi j}{l}\cdot k}.$$

The diagonal elements of M are then defined by the matrix relation

$$[\beta_1 \cdots \beta_t]M = [0 \cdots 0]. \tag{4.1}$$

ii) For $l = 2$ (and hence $\beta_1 = \cdots = \beta_t = 1$) we define the *right Redei matrix* $M = [M_{ij}] = M_{K(\sqrt[l]{\alpha})/K}$ just as in i) but by replacing the matrix condition (4.1) by:

$$M \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

iii) For $l = 2$ (and $\beta_1 = \cdots = \beta_t = 1$) consider a factorization $\alpha = \alpha_1\alpha_2$ where $\alpha_1 = \prod_{i \in A_1} \pi_i$ and $\alpha_2 = \prod_{i \in A_2} \pi_i$ with disjoint A_1 and A_2 whose union is $\{1, \ldots, t\}$. We think of $\alpha = \alpha_1\alpha_2$ and $\alpha = \alpha_2\alpha_1$ as the same factorization of α; hence there are 2^{t-1} distinct factorizations of α. We say that $\alpha = \alpha_1\alpha_2$ is a factorization of α of type 2 if the right Redei matrix $M = M_{K(\sqrt[l]{\alpha})/K}$ satisfies:

$$\forall i \in A_1 : \sum_{j \in A_2} M_{ij} = 0 \quad \text{and} \quad \forall i \in A_2 : \sum_{j \in A_1} M_{ij} = 0.$$

Clearly, a (left or right) Redei matrix has rank at most $t - 1$ over $\mathbb{F}_l$. Also, the concepts left Redei and right Redei coincide for symmetric matrices.

Remark 4.8. Let $l = 2$. Our definition iii) is a generalization of the concepts in [26]. It is easily seen that

$$\begin{aligned} & \text{the } \mathbb{F}_2\text{-rank of } M_{K(\sqrt[l]{\alpha})/K} \text{ is } t-1-u \\ \Leftrightarrow \quad & \text{the number of factorizations of } \alpha \text{ of type 2 is } 2^u. \end{aligned}$$

Theorem 4.9. *Let l be a prime number. Let K be an algebraic number field that contains the l'th roots of unity and assume that $l \nmid h(K)$; let $\pi_1, \ldots, \pi_t \in \mathcal{O}_K$, $t \geq 2$, such that $(\pi_1), \ldots, (\pi_t)$ are distinct prime ideals. Let $\beta_1, \ldots, \beta_t \in \{1, \ldots, l-1\}$; put $\alpha := \pi_1^{\beta_1} \cdots \pi_t^{\beta_t}$. Assume that no prime different from (π_i) is ramified in the extension $K(\sqrt[l]{\pi_i})/K$.*

Consider the left Redei matrix $M = M_{K(\sqrt[l]{\alpha})/K}$. Assume that $\mathrm{rank}_{\mathbb{F}_l}(M) = t - 1$. Then the relative norm map

$$N_{K(\sqrt[l]{\alpha})/K} : \; \mathcal{O}^*_{K(\sqrt[l]{\alpha})} \to \; \mathcal{O}^*_K$$

is surjective.

Proof. Put $L := K(\sqrt[l]{\alpha})$. Let $\mathfrak{p}_i$ be the prime ideal in $\mathcal{O}_L$ above (π_i). Consider a vector $(\gamma_1, \dots, \gamma_t) \in \mathbb{F}_l^t \backslash \mathbb{F}_l(\beta_1, \dots, \beta_t)$. By proposition 4.4, it is enough to show that $\mathfrak{a} = \mathfrak{p}_1^{\gamma_1} \cdots \mathfrak{p}_t^{\gamma_t}$ is *not* a principal ideal:

The linear map, $\mathbb{F}_l^t \to \mathbb{F}_l^t$, $x \mapsto xM$, has kernel $\mathbb{F}_l(\beta_1, \dots, \beta_t)$. Hence there is a $j \in \{1, \dots, t\}$ such that $\sum_{i=1}^t \gamma_i M_{ij} \neq 0$. We can, by multiplying $\mathfrak{a}$ with a suitable power of $\mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_t^{\beta_t} = (\sqrt[l]{\alpha})$, if necessary, assume that $\gamma_j = 0$. If we put $L' := K(\sqrt[l]{\pi_1}, \dots, \sqrt[l]{\pi_t})$, then we have

$$\begin{aligned} \left(\frac{L'/L}{\mathfrak{a}}\right)(\sqrt[l]{\pi_j}) &= \left(\left(\frac{L'/L}{\mathfrak{p}_1}\right)^{\gamma_1} \circ \cdots \circ \left(\frac{L'/L}{\mathfrak{p}_t}\right)^{\gamma_t}\right)(\sqrt[l]{\pi_j}) \\ &= e^{\frac{2\pi i}{l} \cdot \sum_{i=1}^t \gamma_i M_{ij}} \cdot \sqrt[l]{\pi_j} \\ &\neq \sqrt[l]{\pi_j}. \end{aligned}$$

Since the extension L'/L is unramified, it follows, by class field theory, that $\mathfrak{a}$ is not a principal ideal. □

We shall illustrate the quadratic case in the next chapter; here we give one example for $l = 3$:

Proposition 4.10. *Let p be a prime number congruent to 1 modulo 9; so we can write $p = a^2 + 3b^2$; $a, b \in \mathbb{Z}$. Assume that $3||b$. Then the following two relative norm maps are surjective:*

$$\begin{aligned} N_{K(\sqrt[3]{3p})/K} &: \mathcal{O}^*_{K(\sqrt[3]{3p})} \to \mathcal{O}^*_K, \\ N_{K(\sqrt[3]{3p^2})/K} &: \mathcal{O}^*_{K(\sqrt[3]{3p^2})} \to \mathcal{O}^*_K, \end{aligned}$$

where $K = \mathbb{Q}(\sqrt{-3})$.

Proof. Write $p = \pi\bar{\pi}$, $\pi = a + b\sqrt{-3}$, $\bar{\pi} = a - b\sqrt{-3}$; we can assume that $a \equiv 1 \pmod 9$. Since also $3|b$, it is easy to see that $\left(\frac{\pi}{\bar{\pi}}\right)_3 = \left(\frac{\bar{\pi}}{\pi}\right)_3 = 1$. The fact that $3||\, b$ implies that $(\sqrt{-3})$ is inert in each of $K(\sqrt[3]{\pi})/K$ and $K(\sqrt[3]{\bar{\pi}})/K$.

If we let $\alpha_1 := \sqrt{-3} \cdot \pi \cdot \bar{\pi}$ and $\alpha_2 := \sqrt{-3} \cdot \pi^2 \cdot \bar{\pi}^2$, we therefore have that the left Redei matrices $M_1 = M_{K(\sqrt[3]{\alpha_1})/K}$ and $M_2 = M_{K(\sqrt[3]{\alpha_2})/K}$ have the forms

$$M_1 = \begin{bmatrix} * & x & y \\ * & -x & 0 \\ * & 0 & -y \end{bmatrix}, \quad M_2 = \begin{bmatrix} * & x & y \\ * & x & 0 \\ * & 0 & y \end{bmatrix},$$

where x and y are non-zero. Hence M_1 and M_2 have rank $2 = 3 - 1$ over $\mathbb{F}_3$. By theorem 4.9 it is enough to note that $K(\sqrt[3]{\alpha_1}) = K(\sqrt[3]{3p^2})$ and $K(\sqrt[3]{\alpha_2}) = K(\sqrt[3]{3p})$. □

4.3 4-rank of Class Groups

In this section, we prove a more general version of theorem 1.19.

We shall use the following result which is a version of the Elementary Divisor Theorem:

Lemma 4.11. *Let p be a prime number. Let G be a finite abelian p-group with $rank_p(G) = n$. Let H be a subgroup of G where (necessarily) $rank_p(H) = m \in \{0, 1, \ldots, n\}$. Then there exist $g_1, \ldots, g_n \in G$ and $a_1, \ldots, a_m \in \mathbb{N}$ such that*

$$G = \langle g_1, \ldots, g_n \rangle \qquad \text{and} \qquad H = \langle g_1^{a_1}, \ldots, g_m^{a_m} \rangle.$$

We shall use $e_4(L)$ to denote the 4–rank of the class group of the number field L (cf. definition 1.17).

Theorem 4.12. *Let K be an algebraic number field and assume that $2 \nmid h(K)$; let $\pi_1, \ldots, \pi_t \in \mathcal{O}_K$, $t \geq 2$, such that $(\pi_1), \ldots, (\pi_t)$ are distinct prime ideals. Put $\alpha := \pi_1 \cdots \pi_t$. Assume that no prime different from (π_i) is ramified in the extension $K(\sqrt{\pi_i})/K$. Put $L := K(\sqrt{\alpha})$.*
Assume that every unit of K is the relative norm of a number from L, i.e. $\mathcal{O}_K^* \subseteq N_{L/K}(L)$. So the 2-rank of $Cl(L)$ is $t-1$ (cf. lemma 4.3 and the ambiguous class number formula).
Let the right Redei matrix $M_{L/K}$ have $\mathbb{F}_2$-rank $t-1-u$, $u \geq 0$. Then the following statements hold:

1) If $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$, then $e_4(L) = u$

2) If $N_{L/K}(\mathcal{O}_L^*) \neq \mathcal{O}_K^*$, then we can write

$$rank_2\left(\left\{[\mathfrak{p}_1^{a_1}, \ldots \mathfrak{p}_t^{a_t}]_L \middle| a_i \in \{0,1\}\right\}\right) = t-1-w, \ w \in \{1, \ldots, t-1\}$$

where $\mathfrak{p}_i$ is the prime ideal in L above (π_i).

i) $u - w \leq e_4(L) \leq u$.

ii) Since the 2-rank of $Cl(L)$ is $t-1$, we can choose prime ideals $\tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_w$ in L not dividing (2) such that

$$rank_2\left(\left\{[\mathfrak{p}_1^{a_1}, \ldots \mathfrak{p}_t^{a_t}\tilde{\mathfrak{p}}_1^{\tilde{a}_1}, \ldots \tilde{\mathfrak{p}}_w^{\tilde{a}_w}]_L \middle| a_i, \tilde{a}_j \in \{0,1\}\right\}\right) = t-1,$$

then

$$\forall \alpha = \alpha_1\alpha_2 \textit{ of type } 2 \textit{ and } j \in \{1,\ldots,w\} : \left(\frac{\alpha_1}{\tilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\tilde{\mathfrak{p}}_j}\right) = 1$$

$$\Rightarrow \quad e_4(L) = u.$$

And if, in addition, $u = t - 1$, then

$$\forall \alpha = \alpha_1\alpha_2 \textit{ of type } 2 \textit{ and } j \in \{1,\ldots,w\} : \left(\frac{\alpha_1}{\tilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\tilde{\mathfrak{p}}_j}\right) = 1$$

$$\Leftrightarrow \quad e_4(L) = u.$$

3) In particular, if $rank_{\mathbb{F}_2}(M_{L/K}) = t - 1$ (i.e. if only the trivial factorization of α is of type 2), then the 2-class group of L is elementary abelian.

Proof. First, note that if $N_{L/K}(\mathcal{O}_L^*) \neq \mathcal{O}_K^*$, then by proposition 4.4 we can write

$$rank_2\left(\{[\mathfrak{p}_1^{a_1},\ldots\mathfrak{p}_t^{a_t}]_L \big| a_i \in \{0,1\}\}\right) = t - 1 - w,\ w \in \{1,\ldots,t-1\}$$

where $\mathfrak{p}_i$ is the prime ideal in L above (π_i).

The idea of the proof is the same as in Reichardt [26] but with a few adjustments to our case. Class field theory will be used.

Note first that for a non-trivial factorization $\alpha = \alpha_1\alpha_2$ of α:

$$\alpha = \alpha_1\alpha_2 \ \text{ is of type 2} \quad \Leftrightarrow$$

$$\text{each prime in } L \ \text{ dividing } \ (\alpha) \ \text{ splits totally in } \ K(\sqrt{\alpha_1},\sqrt{\alpha_2}).$$

Put $A :=$ the group of fractional ideals of L and $S :=$ the group of fractional principal ideals of L.

As the 2-rank of $Cl(L)$ is $t - 1 \geq 1$, there is (by class field theory) at least one ideal group H_1 (modulo S) in L of index 2 in A. The corresponding class field L_1 is a quadratic and unramified extension of L and hence has the form $L_1 = K(\sqrt{\alpha_1},\sqrt{\alpha_2})$ where $\alpha = \alpha_1\alpha_2$ is a non-trivial factorization of α. Conversely, for every such non-trivial factorization of α the field $K(\sqrt{\alpha_1},\sqrt{\alpha_2})$ is a quadratic and unramified extension of L and is, therefore, the class field for an ideal group (modulo S) in L of index 2 in A.

By class field theory, $e_4(L) \geq 1$ if and only if there exists an unramified $\mathbb{Z}/4$-extension L_2 of L. If this is the case, there is exactly one field L_1 between L and L_2 such that L_1/L is a quadratic and unramified extension; L_1 must have the form $L_1 = K(\sqrt{\alpha_1},\sqrt{\alpha_2})$; the unique non-trivial factorization $\alpha = \alpha_1\alpha_2$ of α will be called the factorization of α attached to L_2.

We now prove some claims:

a) If the non-trivial factorization $\alpha = \alpha_1\alpha_2$ is attached to L_2 where L_2 is unramified and $\mathbb{Z}/4$ over L, then $\alpha = \alpha_1\alpha_2$ is of type 2.

Let H_2 be the ideal group (modulo S) in L corresponding to L_2. Let cH_2 be a generator of $A/H_2 (\simeq \mathbb{Z}/4)$. Fix an $i \in \{1, \dots, t\}$. Since, in L, $(\pi_i) = \mathfrak{p}_i^2$ and $(\pi_i) \in H_2$, we have $\mathfrak{p}_i \in \langle (cH_2)^2 \rangle =: H_1$. As the class field L_1 corresponding to H_1 is unramified and quadratic over L and contained in L_2, we have that $\mathfrak{p}_i$ splits totally in $L_1 = K(\sqrt{\alpha_1}, \sqrt{\alpha_2})$. Hence $\alpha = \alpha_1\alpha_2$ is of type 2. This proves a).

b) Let the non-trivial factorization $\alpha = \alpha_1\alpha_2$ be of type 2. Let H_1 be the ideal group (modulo S) in L corresponding to $K(\sqrt{\alpha_1}, \sqrt{\alpha_2})$. Then

$$K(\sqrt{\alpha_1}, \sqrt{\alpha_2})/L \text{ is contained in an unramified } \mathbb{Z}/4 - \text{extension}$$

$$\Leftrightarrow \quad rank_2(H_1/S) = t - 1.$$

And we have $\mathfrak{p}_1, \dots, \mathfrak{p}_t \in H_1$.

$G := A/S$ has 2-rank $t-1$; let $G_1 := H_1/S$ have 2-rank $m (\in \{0, 1, \dots, t-1\})$. By lemma 4.11 (applied to 2-Sylow groups) we can write

$$G = \langle g_1 S, \dots, g_{t-1} S \rangle \bar{H}/S, \; g_i \in A$$

and

$$G_1 = \langle (g_1 S)^{a_1}, \dots, (g_m S)^{a_m} \rangle \bar{H}/S, \; a_i \in \mathbb{Z}$$

where $[\bar{H} : S]$ is odd. Note that $G/G_1 \simeq A/H_1 \simeq \mathbb{Z}/2$.

Let $m = t - 1$. We see that (with a suitable numbering)

$$H_1 = \langle g_1^2, \dots, g_{t-1} \rangle \bar{H}.$$

We must have $g_1^2 \notin S$. Put $H_2 := \langle g_1^4, \dots, g_{t-1} \rangle \bar{H}$. Then $A/H_2 \simeq \mathbb{Z}/4$

Let $m < t - 1$. As $G/G_1 \simeq \mathbb{Z}/2$, we must have $m = t - 2$ and (with a suitable numbering) $ord(g_{t-1}S) = 2$ and

$$H_1 = \langle g_1, \dots, g_{t-2} \rangle \bar{H}.$$

From this we see that if $H_1 \supseteq N \supseteq S$ and $[H_1 : N] = 2$, then $A/N \not\simeq \mathbb{Z}/4$. (For $A = H_1 \cup g_{t-1}H_1$.) This proves the first part of b). The second part is clear since each $\mathfrak{p}_i$ splits totally in $K(\sqrt{\alpha_1}, \sqrt{\alpha_2})$.

c) Let the non-trivial factorization $\alpha = \alpha_1\alpha_2$ be of type 2. If $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$, then $K(\sqrt{\alpha_1}, \sqrt{\alpha_2})/L$ is contained in an unramified $\mathbb{Z}/4$–extension.

This follows from b) and proposition 4.4.

d) Assume that $N_{L/K}(\mathcal{O}_L^*) \neq \mathcal{O}_K^*$ and that (cf. proposition 4.4)

$$rank_2\left(\left\{[\mathfrak{p}_1^{a_1},\dots\mathfrak{p}_t^{a_t}]_L \middle| a_i \in \{0,1\}\right\}\right) = t-1-w,\ \ w \geq 1.$$

If prime ideals $\tilde{\mathfrak{p}}_1,\dots,\tilde{\mathfrak{p}}_w$ in L not dividing (2) are chosen such that

$$rank_2\left(\left\{[\mathfrak{p}_1^{a_1},\dots\mathfrak{p}_t^{a_t}\tilde{\mathfrak{p}}_1^{\tilde{a}_1},\dots\tilde{\mathfrak{p}}_w^{\tilde{a}_w}]_L \middle| a_i,\tilde{a}_j \in \{0,1\}\right\}\right) = t-1,$$

then, for a non-trivial factorization $\alpha = \alpha_1\alpha_2$ of type 2,

$$K(\sqrt{\alpha_1},\sqrt{\alpha_2})/L \text{ is contained in an unramified } \mathbb{Z}/4 - \text{extension} \quad \Leftrightarrow$$

$$\forall j \in \{1,\dots,w\}: \left(\frac{\alpha_1}{\tilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\tilde{\mathfrak{p}}_j}\right) = 1.$$

Let H_1 be as in b). Then d) follows from:

$$\begin{array}{ll} & K(\sqrt{\alpha_1},\sqrt{\alpha_2})/L \text{ is contained in an unramified } \mathbb{Z}/4 - \text{extension} \\ \Leftrightarrow & \forall j \in \{1,\dots,w\}: \mathfrak{p}_j \in H_1 \\ \Leftrightarrow & \forall j \in \{1,\dots,w\}: \mathfrak{p}_j \text{ splits totally in } K(\sqrt{\alpha_1},\sqrt{\alpha_2}) \\ \Leftrightarrow & \forall j \in \{1,\dots,w\}: \left(\frac{\alpha_1}{\tilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\tilde{\mathfrak{p}}_j}\right) = 1. \end{array}$$

The proof of the theorem can now be finished as follows:
Put

$$\begin{array}{rcl} n & := & \text{the number of non-trivial factorizations } \alpha = \alpha_1\alpha_2 \text{ of type 2 where} \\ & & K(\sqrt{\alpha_1},\sqrt{\alpha_2})/L \text{ is contained in an unramified } \mathbb{Z}/4 - \text{extension} \\ & = & \text{the number of non-trivial factorizations } \alpha = \alpha_1\alpha_2 \text{ where} \\ & & K(\sqrt{\alpha_1},\sqrt{\alpha_2})/L \text{ is contained in an unramified } \mathbb{Z}/4 - \text{extension} \\ & = & \text{the number of subgroups of } G := A/S \text{ of index} \\ & & 2 \text{ containing a subgroup in } G \text{ with factor group } \mathbb{Z}/4 \\ & = & 2^{e_4(G)} - 1 \\ & = & 2^{e_4(L)} - 1; \end{array}$$

here the third equality sign follows from class field theory and the fourth is group theory of finite abelian groups.

From a) we get

$$n \leq 2^u - 1.$$

For a given $j \in \{1, \dots, w\}$ we have

$$x_j := \left| \left\{ \alpha = \alpha_1\alpha_2 \text{ of type } 2 \middle| \left(\frac{\alpha_1}{\tilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\tilde{\mathfrak{p}}_j}\right) = 1 \right\} \right| \in \{2^{u-1}, 2^u\};$$

in particular, $x_j = 2^u$ if $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$. Since

$$n + 1 = \left| \left\{ \alpha = \alpha_1\alpha_2 \text{ of type } 2 \middle| \forall j \in \{1, \dots, w\} : \left(\frac{\alpha_1}{\tilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\tilde{\mathfrak{p}}_j}\right) = 1 \right\} \right|,$$

we conclude that

$$n + 1 \geq 2^{u-y}$$

where y is the number of j with $x_j = 2^{u-1}$, and we find that for $u = t - 1$

$$n + 1 = 2^u \quad \Leftrightarrow \quad x_1 = \cdots = x_w = 2^u.$$

This completes the proof of the theorem. □

Chapter 5

Quadratic Extensions

5.1 Quadratic Extensions of $\mathbb{Q}(i)$

Let $(\pi_1), \ldots, (\pi_t)$ be distinct prime ideals in $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. Put $\alpha := \pi_1, \ldots, \pi_t$. Since we are asking whether $x^2 - \alpha y^2 = i$ is solvable in $\mathbb{Z}[i]$, we shall assume that the necessary condition for solvability,

$$\forall j \in \{1, \ldots, t\} : \; N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi_j) \equiv 1 \pmod 8,$$

is fulfilled. This means that $i \in \mathcal{O}^*_{\mathbb{Q}(i)}$ is the relative norm of a *number* in $\mathbb{Q}(i, \sqrt{\alpha})$, and so this is also a necessary (and sufficient) condition for

$$rank_2(CL(\mathbb{Q}(i, \sqrt{\alpha}))) = t - 1$$

(cf. lemma 4.3 and the ambiguous class number formula).

We begin by considering the case where $\alpha := d = \pi_1 \cdots \pi_t$ where $d \neq \pm 1$ is a square-free rational integer. Let $\bar{\mathfrak{p}_i}$ be the prime ideal in $L := K(\sqrt{d})$ above (π_i).

Remark 5.1. According to [13],

$$rank_2 \left(\left\{ [\bar{\mathfrak{p}_1}^{a_1} \cdots \bar{\mathfrak{p}_t}^{a_t}]_L \middle| a_i \in \{0, 1\} \right\} \right) \in \{t - 2, t - 1\}$$

and the following statements are equivalent:

1) $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$
2) $\exists \varepsilon \in \mathcal{O}^*_{\mathbb{Q}(\sqrt{d})} \; \exists \gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} : \gamma^2 = 2\varepsilon$
3) $rank_2 \left(\left\{ [\bar{\mathfrak{p}_1}^{a_1}, \ldots \bar{\mathfrak{p}_t}^{a_t}]_L \middle| a_i \in \{0, 1\} \right\} \right) = t - 1$

Note that the equivalence of 1) and 3) also follows from Proposition 4.4

From the equivalence of 1) and 2) we deduce a *rational* (and complete) criterion for i being in $N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$:

Theorem 5.2. *1)* $i \in N_{\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{2})})$.

Let $d \in \mathbb{Z}\backslash\{\pm 1, 2\}$ *be square-free.*

2) If $d \equiv 1 \pmod 4$*, then* $i \notin N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$.

3) If the negative Pell equation $x^2 - dy^2 = -1$ *is solvable (in* $\mathbb{Z}$*), then* $i \notin N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$.

4) If $d \not\equiv 1 \pmod 4$ *and* $x^2 - dy^2 = -1$ *is not solvable (in* $\mathbb{Z}$*), then:*

$$i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})}) \;\Leftrightarrow\; \exists x, y \in \mathbb{Z} : x^2 - dy^2 = \pm 2.$$

Proof. 1) This is immediate from remark 5.1.

2) Assume that $\gamma^2 = 2\varepsilon, \gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $\varepsilon \in \mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}$; write $\gamma = \frac{x+y\sqrt{d}}{2}$. We see that $x^2 - dy^2 = \pm 8$. Since also

$$2\varepsilon = \gamma^2 = \pm 2 + \frac{y^2 d + xy\sqrt{d}}{2},$$

we conclude that $2 \mid x, y$. But an equation $(x')^2 - d(y')^2 = \pm 2$ is impossible modulo 4.

3) Let $x^2 - dy^2 = -4$ be solvable and let ε be a fundamental unit of $\mathbb{Q}(\sqrt{d})$ which has norm -1. If $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then we have an equation $\gamma^2 = \pm 2\varepsilon^k$ with $k \in \{0, 1\}$. As $\sqrt{2} \notin \mathbb{Q}(\sqrt{d})$, we must have $k = 1$. This gives the following contradiction:

$$0 < (N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\gamma))^2 = N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(2\varepsilon) = -4.$$

4) As $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$, the implication "⇒" is clear.
So assume that $x^2 - dy^2 = 2(-1)^k$; put $\gamma := x + y\sqrt{d}$. Just note that

$$\gamma^2 = x^2 + dy^2 + 2xy\sqrt{d} = 2((-1)^k + dy^2 + xy\sqrt{d})$$

and

$$\begin{aligned} N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}((-1)^k + dy^2 + xy\sqrt{d}) &= 1 + d^2y^4 + 2dy^2(-1)^k - dx^2y^2 \\ &= 1 + dy^2(dy^2 + 2(-1)^k - x^2) = 1. \end{aligned}$$

□

Remark 5.3. Let $d \in \mathbb{Z}\backslash\{\pm 1, 2\}$ be square-free and assume that $d \not\equiv 1 \pmod 4$ and that $x^2 - dy^2 = -1$ not solvable (in $\mathbb{Z}$). If $q_1, \dots q_c \equiv 3 \pmod 4$ are (some of the) prime factors of d and if $\exists x, y \in \mathbb{Z} : x^2 - dy^2 = \pm 2$, then, clearly, $q_1 \equiv \cdots \equiv q_c \pmod 8$ and exactly one of the equations is solvable; in that case, $x^2 - dy^2 = 2$ is solvable if $q_i \equiv 7 \pmod 8$ and $x^2 - dy^2 = -2$ is solvable if $q_i \equiv 3 \pmod 8$.

Corollary 5.4. *For a prime number $p \equiv 1 \pmod 8$ with the prime factorization $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$ we have*

$$\left(\frac{\pi}{\bar{\pi}}\right) = 1.$$

Proof. We use theorem 4.9. The assertion corollary follows from the fact that the matrix $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ has rank 1 (over $\mathbb{F}_2$) and that $i \notin N_{\mathbb{Q}(i,\sqrt{p})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{p})})$. □

Corollary 5.5. *Let $q \equiv 3 \pmod 4$ be a prime number. Then*

$$i \in N_{\mathbb{Q}(i,\sqrt{q})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{q})}) \quad \textit{and} \quad i \in N_{\mathbb{Q}(i,\sqrt{2q})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{2q})}).$$

Proof. It is well known that one of the equations $x^2 - qy^2 = \pm 2$ and one of the equations $x^2 - 2qy^2 = \pm 2$ is solvable (see for instance [21]). □

Lemma 5.6. *Let K'/K be an abelian and unramified extension of number fields. Let l be a prime number and let $k \in \mathbb{N}_0$. Consider an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$. Suppose that*

i) $l^k \parallel [K' : K]$;

ii) $l^{k+1} \nmid h(K)$;

iii) $\left(\frac{K'/K}{\mathfrak{a}}\right) = id_{K'}$;

iv) $\mathfrak{a}^{l^m}$ *is a principal ideal in K for some $m \in \mathbb{N}_0$.*

Then $\mathfrak{a}$ is a principal ideal.
So, in particular, if $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal that splits totally in the l-class field of K and whose ideal class in $Cl(K)$ has l-power order, then $\mathfrak{p}$ is a principal ideal.

Proof. Let $\tilde{K}$ be the Hilbert class field of K and put $\sigma := \left(\frac{\tilde{K}/K}{\mathfrak{a}}\right)$. According to class field theory it is enough to show that $\sigma = id_{\tilde{K}}$.

From iv) we get $\sigma^{l^m} = \left(\frac{\tilde{K}/K}{\mathfrak{a}^{l^m}}\right) = id_{\tilde{K}}$. By iii), $\sigma \in Gal(\tilde{K}/K')$. As

$$|Gal(\tilde{K}/K')| = \frac{h(K)}{[K' : K]}$$

is not divisible by l (by i) and ii)), we have $\sigma = id_{\tilde{K}}$. □

Proposition 5.7. *Let $a, b \in \mathbb{N}_0$ and let $q_1, \dots, q_a, p_1, \dots, p_b$ be prime numbers with $p_1 \equiv \dots \equiv p_b \equiv 1 \pmod 8$ and $q_1 \equiv \dots \equiv q_a \equiv 3 \pmod 8$ or $q_1 \equiv \dots \equiv q_a \equiv 7 \pmod 8$. Suppose that $D \in \mathbb{N}$ is one of the following:*

i) $D = 2q_1 \cdots q_a p_1 \cdots p_b$ with $q_1 \equiv \dots \equiv q_a \equiv 7 \pmod 8$ (possibly $a = 0$); or
ii) $D = q_1 \cdots q_a p_1 \cdots p_b$ with a odd.

If the 2–class group $Cl_2(\mathbb{Q}(\sqrt{D}))$ is elementary abelian, then the following (equivalent) statements hold:

1) $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{D})})$;
2) one of the equations $x^2 - Dy^2 = \pm 2$ is solvable in $\mathbb{Z}$.

Proof. Let $K := \mathbb{Q}(\sqrt{D})$ have an elementary abelian 2-class group and let $\mathfrak{p}_0 \subseteq \mathcal{O}_K$ be the prime ideal above 2. It is enough to show that $\mathfrak{p}_0$ is a principal ideal:

i) $\mathfrak{p}_0$ splits totally in $K(\sqrt{-q_i})$ and in $K(\sqrt{p_j})$, and hence $\mathfrak{p}_0$ splits totally in $K(\sqrt{-q_1}, \dots, \sqrt{-q_a}, \sqrt{p_1}, \dots, \sqrt{p_b}) \cap \mathbb{R}$ which is the 2–class field of K.

ii) Let a be odd. $\mathfrak{p}_0$ splits totally in $K(\sqrt{p_j})$. If $q_i \equiv 7 \pmod 8$, then, clearly, $\mathfrak{p}_0$ splits totally in $K(\sqrt{-q_i})$. If $q_i \equiv 3 \pmod 8$, then

$$-q_1 \cdots q_{i-1} q_{i+1} \cdots q_a p_1 \cdots p_b \equiv -(3^2)^{\frac{a-1}{2}} \cdot 1 \cdots 1 \equiv 7 \pmod 8,$$

and so $\mathfrak{p}_0$ splits totally in $K(\sqrt{-q_1 \cdots q_{i-1} q_{i+1} \cdots q_a p_1 \cdots p_b}) = K(\sqrt{-q_i})$. Hence $\mathfrak{p}_0$ splits totally in $K(\sqrt{-q_1}, \dots, \sqrt{-q_a}, \sqrt{p_1}, \dots, \sqrt{p_b}) \cap \mathbb{R}$ which is the 2-class field of K.

In both i) and ii), we conclude that $\mathfrak{p}_0$ is a principal ideal, by lemma 5.6. □

We give an example of the result in proposition 5.7:

Corollary 5.8. *1) Let q_1, q_2, q_3 be prime numbers with $q_1 \equiv q_2 \equiv q_3 \equiv 3 \pmod 8$ or $q_1 \equiv q_2 \equiv q_3 \equiv 7 \pmod 8$ such that $\left(\frac{q_1}{q_2}\right) = \left(\frac{q_2}{q_3}\right) = \left(\frac{q_3}{q_1}\right)$.*

Then $i \in N_{\mathbb{Q}(i,\sqrt{q_1q_2q_3})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{q_1q_2q_3})})$ and the equation $x^2 - q_1q_2q_3y^2 = (-1)^{\frac{q_1^2-1}{8}} \cdot 2$ is solvable in $\mathbb{Z}$.

2) If $q \equiv 3 \pmod 4$, $p_1 \equiv p_2 \equiv 1 \pmod 8$ are prime numbers with $\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right) = \left(\frac{p_1}{p_2}\right) = -1$, then $i \in N_{\mathbb{Q}(i,\sqrt{qp_1p_2})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{qp_1p_2})})$ and the equation
$x^2 - qp_1p_2y^2 = (-1)^{\frac{q^2-1}{8}} \cdot 2$ is solvable in $\mathbb{Z}$.

Proof. It is easily checked that even the strict 2-class group of each of the fields $\mathbb{Q}(\sqrt{q_1q_2q_3})$ and $\mathbb{Q}(\sqrt{qp_1p_2})$ is elementary abelian. □

Lemma 5.9. *Let K be a quadratic number field with discriminant D, let q and p_1, p_2 be prime numbers such that (q) is inert in K and p_1, p_2 are split with prime (principal) ideal factorizations*

$$(p_1) = (\pi_1)(\tilde{\pi}_1) \text{ and } (p_2) = (\pi_2)(\tilde{\pi}_2)$$

in K. Assume that each of π_1 and π_2 is congruent to a square modulo 4 in $\mathcal{O}_K$. Then the following statements about quadratic residue symbols hold:

1) $\left(\frac{q}{\pi_i}\right) = \left(\frac{q}{\tilde{\pi}_i}\right) = \left(\frac{q}{p_i}\right)$ where the last symbol is an ordinary (rational) Legendre symbol.

2) $\left(\frac{\tilde{\pi}_1}{\pi_2}\right) = \left(\frac{\pi_1}{\tilde{\pi}_2}\right)$;

3) If the Legendre symbol $\left(\frac{p_i}{p_2}\right)$ has the value 1, then $\left(\frac{\pi_1}{\pi_2}\right) = \left(\frac{\tilde{\pi}_1}{\pi_2}\right)$ and $\left(\frac{\pi_1}{\tilde{\pi}_2}\right) = \left(\frac{\tilde{\pi}_1}{\tilde{\pi}_2}\right)$; if the Legendre symbol $\left(\frac{p_i}{p_2}\right)$ has the value -1, then $\left(\frac{\pi_1}{\pi_2}\right) \neq \left(\frac{\tilde{\pi}_1}{\pi_2}\right)$ and $\left(\frac{\pi_1}{\tilde{\pi}_2}\right) \neq \left(\frac{\tilde{\pi}_1}{\tilde{\pi}_2}\right)$.

If $K \not\subseteq \mathbb{R}$, each of these quadratic residue symbols retains its value when reversed.

Proof. 1), 2) and 3) are clear. The last claim follows from the Quadratic Reciprocity Law in quadratic fields (theorem 165 of [12]). □

The (left or right) Redei matrices we encounter in the rest of this chapter will be symmetric because of the Quadratic Reciprocity Law in quadratic fields.

We shall now give some applications of theorem 4.12 for $K = \mathbb{Q}(i)$ and $\alpha := d = \pi_1 \cdots \pi_t$ where d is a rational integer.

Note that if $q \equiv 3 \pmod 4$ is a prime number and $a \in \mathbb{Z}$, then, in $\mathcal{O}_K = \mathbb{Z}[i]$, a is a quadratic residue modulo q.

Recall that $e_4(L)$ denotes the 4–rank of the class group of the number field L.

Also, recall that if the odd d satisfies that $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then $d \equiv 3 \pmod 4$.

The first application is immediate:

Theorem 5.10. *Let $q_1, \ldots, q_t \equiv 3 \pmod 4$ be prime numbers. Put $d := q_1 \cdots q_t$. Then the following statements hold:*

1) $e_4(\mathbb{Q}(i, \sqrt{d})) \in \{t-2, t-1\}$.

2) If $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then t is odd and

$$e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1;$$

in particular, $e_4(\mathbb{Q}(i, \sqrt{d}))$ is even.

Proof. The right Redei matrix $M_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}$ is the zero-matrix. □

Theorem 5.11. *Let* $q_1, \ldots, q_t \equiv 3 \pmod 4$, $p \equiv 1 \pmod 8$ *be prime numbers. Put* $d := q_1 \cdots q_t p$. *Then the following statements hold:*

1) $e_4(\mathbb{Q}(i, \sqrt{d})) \in \{t-2, t-1, t, t+1\}$.

2) If $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, *then* t *is odd and*

$$e_4(\mathbb{Q}(i, \sqrt{d})) \in \{t-1, t+1\};$$

in particular, $e_4(\mathbb{Q}(i, \sqrt{d}))$ *is even.*

Proof. In $\mathbb{Q}(i)$, let the prime factorization of p be $p = \pi\bar{\pi}$ where we can assume that $\pi \equiv \bar{\pi} \equiv 1 \pmod 4$. We only have to prove that the number of factorizations of $\alpha = q_1 \cdots q_t \pi\bar{\pi}$ of type 2 is 2^{t-1} or 2^{t+1}; the other assertions follow from this.

We can write

$$\alpha = q_1 \cdots q_a q_1' \cdots q_b' \pi\bar{\pi}$$

where $\left(\frac{\pi}{q_i}\right) = \left(\frac{\bar{\pi}}{q_i}\right) = 1$ and $\left(\frac{\pi}{q_j'}\right) = \left(\frac{\bar{\pi}}{q_j'}\right) = -1$.

Consider a factorization $\alpha = \alpha_1\alpha_2$ of α.

Assume that $\pi | \alpha_1$ and $\bar{\pi} | \alpha_2$. If $b > 0$, then (for example) $q_1' | \alpha_1$ and hence $\left(\frac{\alpha_2}{q_1'}\right) = \left(\frac{\bar{\pi}}{q_1'}\right) = -1$ and so $\alpha = \alpha_1\alpha_2$ is not of type 2.
If $b = 0$, then, clearly, $\alpha = \alpha_1\alpha_2$ is of type 2; and there are 2^t of these factorizations of type 2.

For factorizations of the form

$$\alpha_1 = q_{i_1} \cdots q_{i_c} q_{j_1}' \cdots q_{j_d}',$$

$$\alpha_2 = q_{i_{c+1}} \cdots q_{i_a} q_{j_{d+1}}' \cdots q_{j_b}' \pi\bar{\pi}$$

where $\left(\frac{\pi}{q_{i_k}}\right) = \left(\frac{\bar{\pi}}{q_{i_k}}\right) = 1$ and $\left(\frac{\pi}{q_{j_k}'}\right) = \left(\frac{\bar{\pi}}{q_{j_k}'}\right) = -1$ it easily seen that

$$\alpha = \alpha_1\alpha_2 \text{ is of type 2 } \Leftrightarrow \ 2|d.$$

Hence

$$\begin{aligned} & \text{the number of factorizations of type 2 of this kind} \\ = \ & (\text{number of subsets of } \{1, \ldots, b\} \text{ with an even number of elements})\cdot \\ & (\text{number of subsets of } \{1, \ldots, a\}) \\ = \ & \begin{cases} 1 \cdot 2^a = 2^t, & if\ b = 0 \\ 2^{b-1} \cdot 2^a = 2^{t-1}, & if\ b > 0 \end{cases} \end{aligned}$$

Therefore, the total number of factorizations of type 2 is

$$\begin{cases} 2^t + 2^t = 2^{t+1}, & if\ b = 0 \\ 0 + 2^{t-1} = 2^{t-1}, & if\ b > 0 \end{cases}.$$

□

Theorem 5.12. *Let $q_1, \ldots, q_t \equiv 3 \pmod 4$, $p_1, \ldots, p_a \equiv 1 \pmod 8$ be prime numbers and suppose that all the Legendre symbols $\left(\frac{q_i}{p_j}\right)$ and $\left(\frac{p_k}{p_j}\right)$ are equal to 1. Put $d := q_1 \cdots q_t p_1 \cdots p_a$. Then the following statements hold:*

1) $e_4(\mathbb{Q}(i, \sqrt{d})) \in \{t + a - 2, \ldots, t + 2a - 1\}$.

2) If $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then t is odd and $e_4(\mathbb{Q}(i, \sqrt{d}))$ is even.

Proof. We have

$$\alpha = q_1 \cdots q_t \pi_1 \bar{\pi}_1 \cdots \pi_a \bar{\pi}_a;$$

here the prime factorization of p_i is $p_i = \pi_i \bar{\pi}_i$ where we can assume that $\pi \equiv \bar{\pi} \equiv 1 \pmod 4$.

Put $\beta := \pi_1 \bar{\pi}_1 \cdots \pi_a \bar{\pi}_a$. Since, clearly,

$$\alpha = (q_{i_1} \cdots q_{i_c} \beta_1)(q_{i_{c+1}} \cdots q_{i_t} \beta_2) \text{ is of type 2} \quad \Leftrightarrow \quad \beta = \beta_1 \beta_2 \text{ is of type 2}$$

(because the Legendre symbols $\left(\frac{q_i}{p_j}\right)$ are equal to 1), the number of factorizations of type 2 of α is 2^t multiplied by the number of factorizations of type 2 of β. The right Redei matrix $M_{\mathbb{Q}(i,\sqrt{\beta})/\mathbb{Q}(i)}$ is a block matrix built of 2×2 blocks of the form $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$ (because the Legendre symbols $\left(\frac{p_k}{p_j}\right)$ are equal to 1). If we replace each such block with the entry x, we get an anti-symmetric $a \times a$ matrix of the same $\mathbb{F}_2$-rank as $M_{\mathbb{Q}(i),\sqrt{\beta})/\mathbb{Q}(i)}$. By § 91 of [29], this rank is *even*. Hence the number of factorizations of type 2 of α is of the form $2^t \cdot 2^{2a-1-2k}$ where $2k \in \{0, 1, \ldots, a\}$. The theorem follows. □

Let d be a product of t prime numbers congruent to 3 modulo 4. As noted in theorem 5.10, $e_4(\mathbb{Q}(i, \sqrt{d})) = t - 2$ or $t - 1$. So, it would be natural to ask if we, just by looking at the prime factors of d modulo 8, can decide exactly when the case $e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1$ occurs? This is done in the next theorem.

Remark 5.13. Let $d > 1$ be a square-free integer. Consider the natural map

$$\begin{aligned}\phi : Cl(\mathbb{Q}(\sqrt{d})) \times Cl(\mathbb{Q}(\sqrt{-d})) &\to Cl(\mathbb{Q}(i,\sqrt{d})),\\ ([\mathfrak{a}]_{\mathbb{Q}(\sqrt{d})}, [\mathfrak{b}]_{\mathbb{Q}(\sqrt{-d})}) &\mapsto [\mathfrak{a}]_{\mathbb{Q}(i,\sqrt{d})}[\mathfrak{b}]_{\mathbb{Q}(i,\sqrt{d})}.\end{aligned}$$

1) In [17], it is proved that the kernel and the co-kernel of ϕ are elementary abelian 2-groups.

2) It follows from [13] that when d is a product of prime numbers congruent to 3 modulo 4, the image of ϕ is exactly the subgroup of $Cl(\mathbb{Q}(i,\sqrt{d}))$ consisting of squares of ideal classes. (More precisely, this follows from the fact that, in this case, the concepts 'Hauptgeschlecht' and 'Geschlechter der Hauptart' coincide for the extension $\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)$; cf. the discussion at the end of section 1.3.)

For the (unique) factorization $D = D_1 \cdots D_m$ of the discriminant D of a quadratic field K as a product of prime discriminants D_i, let χ_i be the genus character of the strict class group $Cl_s(K)$ corresponding to D_i. A strict ideal class $C \in Cl_s(K)$ is the square of a strict class if and only if at least $m-1$ of $\chi_1(C), \ldots, \chi_m(C)$ are equal to 1 (since $\chi_1 \cdots \chi_m = 1$); see [30]. We can now state and prove:

Theorem 5.14. *Let $t \in \mathbb{N}$. Let the positive integer d have the prime factorization*

$$d = q_1 \cdots q_s q_{s+1} \cdots q_t$$

with prime numbers $q_1 \equiv \cdots \equiv q_s \equiv 3,\ q_{s+1} \equiv \cdots \equiv q_t \equiv 7 \pmod 8$.

1) If $s = 0$, then $e_4(\mathbb{Q}(i,\sqrt{d})) = t-1$.

2) If $s = t$, then $e_4(\mathbb{Q}(i,\sqrt{d})) = \begin{cases} t-1, & if\ 2 \not| t \\ t-2, & if\ 2|t \end{cases}$

3) If $0 < s < t$, then

$$\begin{aligned} & e_4(\mathbb{Q}(i,\sqrt{d})) = t-1 \\ \Leftrightarrow\quad & \forall i \in \{1,\ldots,s\} : \left(\tfrac{q_{s+1}\cdots q_t}{q_i}\right) = (-1)^{t-1} \\ & and\ \ \forall j \in \{s+1,\ldots,t\} : \left(\tfrac{q_1\cdots q_s}{q_j}\right) = 1 \end{aligned}$$

where the above symbols are the ordinary Legendre symbols.

Proof. First note that for $t = 1$ the class number of $\mathbb{Q}(i,\sqrt{d})$ is odd, so the assertion is true in this case. So suppose that $t \geq 2$. Put

$$K_1 := \mathbb{Q}(\sqrt{d}) \qquad \text{and} \qquad K_2 := \mathbb{Q}(\sqrt{-d}).$$

In this proof, we shall use a superscript ’s’ to denote strict ideal classes: $[\mathfrak{a}]^s_{K_i} \in Cl_s(K_i)$. The (ramified) primes in K_1 and in K_2 above $q_1, \ldots, q_s, q_{s+1}, \ldots, q_t$ are inert in $L := \mathbb{Q}(i, \sqrt{d})$. Put $q_0 := 2$. In K_1 resp. K_2, we shall denote the prime above q_i by $\mathfrak{p}_j$ resp. $\mathfrak{q}_j$ for $j = 0, \ldots, t$. Note that $[\mathfrak{p}_0]_L = [\mathfrak{q}_0]_L = [(1+i)]_L = 1$ and $[\mathfrak{p}_i]_L = [\mathfrak{q}_i]_L$ for $i = 1, \ldots, t$.

Note that if $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then t is odd and $e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1$ and $s = 0$ or $s = t$. If t is odd, then:

$$\mathfrak{p}_0 \text{ is a principal ideal } \Rightarrow\ x^2 - dy^2 = \pm 2 \text{ is solvable } \Rightarrow\ e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1.$$

Let t be odd and assume that $x^2 - dy^2 = \pm 2$ is not solvable; so $\mathfrak{p}_0$ is not a principal ideal. Then we have (with ϕ as above):

$$\begin{aligned}
& e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1 \\
\Leftrightarrow\ & rank_2(Im(\phi)) = t - 1 \\
\Leftrightarrow\ & \exists y \in Im(\phi) \backslash \left\{ [\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_L \middle| a_i \in \{0,1\} \right\} :\ ord(y) = 2 \\
\Leftrightarrow\ & \exists x \in Cl(K_1) \times Cl(K_2) :\ ord(x) = 4 \text{ and } ord(\phi(x)) = 2 \\
\Leftrightarrow\ & \exists z \in Cl(K_1) \times Cl(K_2) :\ z \text{ is a square, } ord(z) = 2 \text{ and } \phi(z) = 1 \\
\Leftrightarrow\ & \exists a_0, a_1, \ldots, a_t, b_1, \ldots, b_t \in \{0,1\} :\ ([\mathfrak{p}_0^{a_0} \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_{K_1}, [\mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_t^{b_t}]_{K_2}) \text{ is} \\
& \text{a square in } Cl(K_1) \times Cl(K_2) \text{ of order 2 and } [\mathfrak{p}_1^{a_1} \mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_t^{a_t} \mathfrak{q}_t^{b_t}]_L = 1 \\
\Leftrightarrow\ & ([\mathfrak{p}_0 \mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}, [\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) \text{ is a square in } Cl(K_1) \times Cl(K_2) \text{ of order 2.}
\end{aligned}$$

The first ”$\Leftrightarrow$” follows from remark 5.13 2). The third ”$\Leftrightarrow$” follows from remark 5.13 1) (about the kernel of ϕ).

The last ”$\Rightarrow$” requires a proof: Assume that

$$z_1 := [\mathfrak{p}_0^{a_0} \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_{K_1} \in Cl(K_1) \text{ and } z_2 := [\mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_t^{b_t}]_{K_2} \in Cl(K_2)$$

are squares with $ord((z_1, z_2)) = 2$ and $[\mathfrak{p}_1^{a_1} \mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_t^{a_t} \mathfrak{q}_t^{b_t}]_L = 1$.

We have

$$rank_2 \left(\left\{ [\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_t^{x_t}]_{K_1} \middle| x_i \in \{0,1\} \right\} \right) \in \{t-2, t-1\};$$

Let r be this 2-rank. (For t even it is always the case that $r = t - 2$.)

Consider the equation $[\mathfrak{p}_1^{a_1} \mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_t^{a_t} \mathfrak{q}_t^{b_t}]_L = 1$, i.e. $[\mathfrak{p}_1^{a_1+b_1} \cdots \mathfrak{p}_t^{a_t+b_t}]_L = 1$.

If $r = t - 2$, then, by remark 5.1, we must have $[\mathfrak{p}_1^{a_1+b_1} \cdots \mathfrak{p}_t^{a_t+b_t}]_{K_1} = 1$, i.e. $[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_{K_1} = [\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_t^{b_t}]_{K_1}$; hence we can assume that $(a_1, \ldots, a_t) = (b_1, \ldots, b_t)$.

In the case we are considering, i.e. t odd, another way, which covers both of the cases $r = t-2$ and $r = t-1$, of realizing that we can assume that $(a_1, \dots, a_t) = (b_1, \dots, b_t)$ is the following: As $\mathfrak{p}_0$ is not a principal ideal, then the map

$$\left\{[\mathfrak{p}_0^{x_0}\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}]_{K_1}\big|x_i \in \{0,1\}\right\} \;\to\; \left\{[\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}]_L\big|x_i \in \{0,1\}\right\},$$

$$[\mathfrak{p}_0^{x_0}\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}] \;\mapsto\; [\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}]_L$$

has kernel $\{1, [\mathfrak{p}_0]_{K_1}\}$. Hence $[\mathfrak{p}_1^{a_1+b_1}\cdots\mathfrak{p}_t^{a_t+b_t}]_{K_1} = [\mathfrak{p}_0]_{K_1}^{\gamma}$ for a $\gamma \in \{0,1\}$, and this implies that $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1} = [\mathfrak{p}_0^{a_0+\gamma}\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_t^{b_t}]_{K_1}$; and we can assume that $(a_1, \dots, a_t) = (b_1, \dots, b_t)$.

Since $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}$ is a square in $Cl(K_1)$, we have that $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^s$ or $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1+1}\cdots\mathfrak{p}_t^{a_t+1}]_{K_1}^s$ is a square in $Cl_s(K_1)$. As $z_2 = z_2 \cdot [\mathfrak{q}_1\cdots\mathfrak{q}_t]_{K_2}$, we can assume that $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^s$ is a square in $Cl_s(K_1)$.

Let $\chi_k^{(1)}$ resp. $\chi_k^{(2)}$ be the k'th genus character of K_1 resp. K_2 ($\chi_0^{(i)}$ corresponds to the prime discriminant -4 if 2 is ramified in $K_i/\mathbb{Q}$).

If $(a_1, \dots, a_t) = (0, \dots, 0)$, then $ord((z_1, z_2)) = 2$ implies that $a_0 = 1$; hence $[\mathfrak{p}_0]_{K_1}^s = [\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^s$ is a square in $Cl_s(K_1)$. As

$$\chi_i^{(1)}([\mathfrak{p}_0]_{K_1}^s) = \left(\frac{-q_i}{2}\right),\ i = 1, \dots t,$$

we conclude that $q_1 \equiv \cdots \equiv q_t \equiv 7 \pmod 8$, i.e. $s = 0$, and so "$\Rightarrow$" is proved in this case.

Let $(a_1, \dots, a_t) \neq (0, \dots, 0)$ and consider a $j \in \{1, \dots, t\}$ with $a_j = 1$. We have

$$1 = \chi_j^{(1)}([\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^s) = \prod_{\substack{i=0\\i\neq j}}^{t} \chi_j^{(1)}([\mathfrak{p}_i^{a_i}]_{K_1}^s) \cdot \prod_{\substack{k=0\\k\neq j}}^{t} \chi_k^{(1)}([\mathfrak{p}_j]_{K_1}^s)$$

and

$$1 = \chi_j^{(2)}([\mathfrak{q}_1^{a_1}\cdots\mathfrak{q}_t^{a_t}]_{K_2}) = \prod_{\substack{i=1\\i\neq j}}^{t} \chi_j^{(2)}([\mathfrak{q}_i^{a_i}]_{K_2}) \cdot \prod_{\substack{k=1\\k\neq j}}^{t} \chi_k^{(2)}([\mathfrak{q}_j]_{K_2}).$$

For $i, k \in \{1, \dots, t\},\ i \neq k$, we have

$$\chi_k^{(1)}([\mathfrak{p}_i]_{K_1}^s) = \left(\frac{-q_k}{q_i}\right) = \chi_k^{(2)}([\mathfrak{q}_i]_{K_2}).$$

This and the above equations imply that

$$1 = \chi_j^{(1)}([\mathfrak{p}_0^{a_0}]_{K_1}^s) \cdot \chi_0^{(1)}([\mathfrak{p}_j]_{K_1}^s) = \left(\frac{-q_j}{2}\right)^{a_0} \cdot \left(\frac{-4}{q_j}\right) = \left(\frac{-q_j}{2}\right)^{a_0} \cdot (-1),$$

and hence $a_0 = 1$ and $q_j \equiv 3 \pmod 8$. In particular, $a_{s+1} = \cdots = a_t = 0$.

Assume now that $j \in \{1, \ldots, s\}$ and $a_j = 0$. Then

$$1 = \chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s}]_{K_1}^s) = \chi_j^{(1)}([\mathfrak{p}_0]_{K_1}^s) \cdot \prod_{\substack{i=1\\ i\neq j}}^{s} \chi_j^{(1)}([\mathfrak{p}_i^{a_i}]_{K_1}^s)$$

and

$$1 = \chi_j^{(2)}([\mathfrak{q}_1^{a_1} \cdots \mathfrak{q}_s^{a_s}]_{K_2}) = \prod_{\substack{i=1\\ i\neq j}}^{s} \chi_j^{(2)}([\mathfrak{q}_i^{a_i}]_{K_2})$$

which implies that $1 = \chi_j^{(1)}([\mathfrak{p}_0]_{K_1}^s) = \left(\frac{-q_j}{2}\right) = -1$ which is a contradiction; hence $a_1 = \cdots = a_s = 1$. This completes the proof of "⇒".

For t even it is proved in a similar way (without the assumption about $\mathfrak{p}_0$ not being principal) that

$$\begin{aligned} &e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1 \\ \Leftrightarrow \quad &([\mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}, [\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) \text{ is a square in } Cl(K_1) \times Cl(K_2) \text{ of order 2.}\end{aligned}$$

We now go through the cases of the theorem:

1) $q_1 \equiv \cdots \equiv q_t \equiv 7 \pmod 8$:

Let t be odd: If $\mathfrak{p}_0$ is a principal ideal, we are done; so assume that $\mathfrak{p}_0$ is not a principal ideal, i.e. $ord([\mathfrak{p}_0]_{K_1}) = 2$. We just have to note that

$$\chi_j^{(1)}([\mathfrak{p}_0]_{K_1}^s) = \left(\frac{-q_j}{2}\right) = 1, \; j = 1, \ldots t.$$

Let t be even: We have $ord([\mathfrak{q}_0]_{K_1}) = 2$ since $\mathfrak{q}_1 \cdots \mathfrak{q}_t$ is the only non-trivial principal ideal in $\left\{\mathfrak{q}_0^{x_0}\mathfrak{q}_1^{x_1} \cdots \mathfrak{q}_t^{x_t} \middle| x_i \in \{0, 1\}\right\}$. Note that

$$\chi_j^{(2)}([\mathfrak{q}_0]_{K_1}) = \left(\frac{-q_j}{2}\right) = 1, \; j = 1, \ldots t.$$

2) $q_1 \equiv \cdots \equiv q_t \equiv 3 \pmod 8$:

Let t be odd: If $\mathfrak{p}_0$ is a principal ideal, we are done; so we can assume that

$ord([\mathfrak{p}_0]_{K_1}) = 2$. Note that $[\mathfrak{p}_0]_{K_1} = [\mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_t]_{K_1}$. For $j = 1, \ldots, t$ we have

$$\begin{aligned}
\chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_t]^s_{K_1}) &= \prod_{\substack{i=0\\ i\neq j}}^{t} \chi_j^{(1)}([\mathfrak{p}_i]^s_{K_1}) \cdot \prod_{\substack{k=0\\ k\neq j}}^{t} \chi_k^{(1)}([\mathfrak{p}_j]^s_{K_1}) \\
&= \left(\frac{-q_j}{2}\right) \prod_{\substack{i=1\\ i\neq j}}^{t} \left(\frac{-q_j}{q_i}\right) \cdot \left(\frac{-4}{q_j}\right) \prod_{\substack{k=1\\ k\neq j}}^{t} \left(\frac{-q_k}{q_j}\right) \\
&= (-1)\cdot(-1)\cdot(-1)^{t-1}\cdot(-1)^{t-1} \prod_{\substack{m=1\\ m\neq j}}^{t} \left(\left(\frac{q_j}{q_m}\right)\left(\frac{q_m}{q_j}\right)\right) \\
&= (-1)\cdot(-1)\cdot(-1)^{t-1}\cdot(-1)^{t-1}\cdot(-1)^{t-1} = 1
\end{aligned}$$

and

$$\chi_j^{(2)}([\mathfrak{q}_1 \cdots \mathfrak{q}_t]_{K_2}) = \chi_j^{(2)}(1) = 1,$$

as required.

Let t be even: As

$$\begin{aligned}
\chi_1^{(2)}([\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_t]_{K_2}) &= \prod_{\substack{i=0\\ i\neq 1}}^{t} \chi_1^{(2)}([\mathfrak{q}_i]_{K_2}) \cdot \prod_{\substack{k=0\\ k\neq 1}}^{t} \chi_k^{(2)}([\mathfrak{q}_1]^s_{K_1}) \\
&= \left(\frac{-q_1}{2}\right) \prod_{i=2}^{t} \left(\frac{-q_1}{q_i}\right) \cdot \left(\frac{-4}{q_1}\right) \prod_{k=2}^{t} \left(\frac{-q_k}{q_1}\right) \\
&= (-1)\cdot(-1)\cdot(-1)^{t-1}\cdot(-1)^{t-1} \prod_{m=2}^{t} \left(\left(\frac{q_1}{q_m}\right)\left(\frac{q_m}{q_1}\right)\right) \\
&= (-1)\cdot(-1)\cdot(-1)^{t-1}\cdot(-1)^{t-1}\cdot(-1)^{t-1} = -1,
\end{aligned}$$

$[\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_t]_{K_2}$ is not a square in $Cl(K_2)$, as required.

3) $q_1 \equiv \cdots \equiv q_s \equiv 3,\ q_{s+1} \equiv \cdots \equiv q_t \equiv 7 \pmod 8$ and $0 < s < t$:

First note that $ord([\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) = 2$ for t odd and that $ord([\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) = 2$ for t even.

Let $j \in \{1, \dots, s\}$. For t odd we have

$$\begin{aligned}
& \chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}^s) \\
= \; & \prod_{\substack{i=0 \\ i \neq j}}^{s} \chi_j^{(1)}([\mathfrak{p}_i]_{K_1}^s) \cdot \prod_{\substack{k=0 \\ k \neq j}}^{t} \chi_k^{(1)}([\mathfrak{p}_j]_{K_1}^s) \\
= \; & \left(\frac{-q_j}{2}\right) \prod_{\substack{i=1 \\ i \neq j}}^{s} \left(\frac{-q_j}{q_i}\right) \cdot \left(\frac{-4}{q_j}\right) \prod_{\substack{k=1 \\ k \neq j}}^{t} \left(\frac{-q_k}{q_j}\right) \\
= \; & (-1) \cdot (-1) \cdot (-1)^{s-1} \cdot (-1)^{t-1} \prod_{\substack{m=1 \\ m \neq j}}^{s} \left(\left(\frac{q_j}{q_m}\right) \left(\frac{q_m}{q_j}\right) \right) \cdot \left(\frac{q_{s+1} \cdots q_t}{q_j}\right) \\
= \; & (-1)^{t-1} \left(\frac{q_{s+1} \cdots q_t}{q_j}\right).
\end{aligned}$$

Similar computations show that $\chi_j^{(2)}([\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) = (-1)^{t-1} \left(\frac{q_{s+1} \cdots q_t}{q_j}\right)$ for t odd and $\chi_j^{(1)}([\mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}^s) = \chi_j^{(2)}([\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) = (-1)^{t-1} \left(\frac{q_{s+1} \cdots q_t}{q_j}\right)$ for t even.

Finally, let $j \in \{s+1, \dots, t\}$. Then it is easily seen that $\chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}^s) = \chi_j^{(2)}([\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) = \left(\frac{q_1 \cdots q_s}{q_j}\right)$ for t odd and $\chi_j^{(1)}([\mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}^s) = \chi_j^{(2)}([\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) = \left(\frac{q_1 \cdots q_s}{q_j}\right)$ for t even. The assertion in 3) of the theorem follows from this. This completes the proof of the theorem. □

Before we give an application of theorem 4.9, we prove the following

Lemma 5.15. *Let $a, b \in \mathbb{N}_0$. Consider the $(2a+2b+1) \times (2a+2b+1)$ matrix over $\mathbb{F}_2$:*

$$M = \left[\begin{array}{cccccc}
0 & 1 & \cdots & \cdots & \cdots & 1 \\
1 & & & | & & \\
\vdots & & M_{11} & | & M_{12} & \\
\vdots & - & - & + & - & - \\
\vdots & & M_{21} & | & M_{22} & \\
1 & & & | & &
\end{array} \right]$$

where M_{11} is a $2a \times 2a$ matrix, M_{12} is a $2a \times 2b$ matrix, M_{21} is a $2b \times 2a$ matrix and M_{22} is a $2b \times 2b$ matrix; these four matrices are constructed as block-matrices built of 2×2 matrices in the following way:

M_{11} has the form

$$\begin{bmatrix} \begin{bmatrix} * & x_1 \\ x_1 & * \end{bmatrix} & & \\ & \ddots & \\ & & \begin{bmatrix} * & x_a \\ x_a & * \end{bmatrix} \end{bmatrix}$$

with $\begin{bmatrix} * & x_i \\ x_i & * \end{bmatrix}$-blocks on the main diagonal, $x_i \in \mathbb{F}_2$, and where every other block is of the form $\begin{bmatrix} y & y+1 \\ y+1 & y \end{bmatrix}$, $y \in \mathbb{F}_2$ (not necessarily the same y).

Every block of M_{12} or of M_{21} is of the form $\begin{bmatrix} z & z \\ z & z \end{bmatrix}$, $z \in \mathbb{F}_2$ (not necessarily the same z).

M_{22} comes in two types:
I) Every block on the main diagonal of M_{22} is of the form $\begin{bmatrix} * & x \\ x & * \end{bmatrix}$, $x \in \mathbb{F}_2$ (not necessarily the same x), and every other block is of the form
$\begin{bmatrix} y & y \\ y & y \end{bmatrix}$, $y \in \mathbb{F}_2$ (not necessarily the same y).

II) Every block on the main diagonal of M_{22} is of the form $\begin{bmatrix} * & x \\ x & * \end{bmatrix}$, $x \in \mathbb{F}_2$ (not necessarily the same x), and every other block is of the form
$\begin{bmatrix} z & z+1 \\ z+1 & z \end{bmatrix}$, $z \in \mathbb{F}_2$ (not necessarily the same z).

Finally, and in all cases, the entries on the main diagonal of M are chosen such that all column sums of M are 0.

Then the following statements hold:

i) If a is even and if M_{22} is of type I, then M has maximal $\mathbb{F}_2$-rank, namely $2a+2b$.

ii) If both a and b are even and if M_{22} is of type II, then M has maximal $\mathbb{F}_2$-rank, $2a+2b$.

Proof. Put $t := 1 + 2(a+b)$. Note that

$$\begin{array}{cl} & M \text{ has maximal } \mathbb{F}_2\text{-rank} \\ \Leftrightarrow & ker(x \mapsto xM) = \{[0,\dots,0],[1,\dots,1]\} \\ \Leftrightarrow & \forall A \subsetneq \{1,\dots t\},\ A \neq \emptyset,\ \exists j \in \{1,\dots t\} : \displaystyle\sum_{i \in A} m_{ij} = 1. \end{array}$$

(Note that $\sum_{i\in A} m_{ij} = 1$ if and only if $\sum_{i \in \complement A} m_{ij} = 1$ where $\complement A = \{1,\dots t\} \backslash A$.) If for $\emptyset \neq A \subsetneq \{1,\dots t\}$ $\exists j \in \{1,\dots t\}$: $\sum_{i\in A} m_{ij} = 1$, then we say that *column j works for A* if $j \in \complement A$ and that *column j works for $\complement A$* if $j \in A$. (This usage just focuses on the fact that we do not want to sum over diagonal elements of M.)

Let $1 \in A \subsetneq \{1,\dots,t\}$.

If $2 \mid |A|$, then column 1 of M works for $\complement A$; so suppose that $2 \nmid |A|$. Put $A_1 := A \cap \{1,\dots,2a+1\}$ and $A_2 := A \cap \{2a+2,\dots,t\}$. For a subset $B \subseteq \{1,\dots,t\}$ we let $M(B)$ denote the sub-matrix of M consisting of the rows of M with a row number in B; for $i \in \{1,\dots,t\}$ let $M(B)_i$ be the i'th column of $M(B)$ and put

$$m_i := \begin{cases} 1, & \text{if the diagonal block of } M \text{ in the columns } 2i, 2i+1 \text{ is } \begin{bmatrix} * & 1 \\ 1 & * \end{bmatrix} \\ 0, & \text{if the diagonal block of } M \text{ in the columns } 2i, 2i+1 \text{ is } \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix} \end{cases};$$

We treat two cases separately:

1) $\exists i_0 \in \{1,\dots,a+b\} : |\{2i_0, 2i_0+1\} \cap A| = 1$:

Assume (for example) that $2i_0 \in A \not\ni 2i_0+1$. There are now two possibilities:

1') $i_0 \in \{1,\dots,a\}$ (and similarly if $i_0 \in \{1,\dots,a+b\}$ and M_{22} is of type II):

Put

$$n_1 := \text{number of “1“s in } M(A_1 \backslash \{2i_0\})_{2i_0+1};$$

$$\begin{aligned} n_2 &:= \text{number of “0“s in } M(\{2,\dots,2a+1\} \backslash (A_1 \cup \{2i_0\}))_{2i_0+1} \\ &= (\text{number of “1“s in } M(\{2,\dots,2a+1\} \backslash A_1)_{2i_0}) - m_{i_0}; \end{aligned}$$

$$\begin{aligned} n_3 &:= \text{number of “1“s in } M(A_2)_{2i_0+1} \\ &\equiv \text{number of “1“s in } M(\{2a+2,\dots,t\} \backslash A_2)_{2i_0} \pmod 2. \end{aligned}$$

Note that $n_1 \equiv n_2 \pmod 2$ (since $2|a$).

Assume that column $2i_0+1$ does *not* work for A. As $1 \in A$, we have

$$1 + n_1 + n_3 + m_{i_0} \equiv 0 \pmod 2;$$

therefore

$$\begin{aligned} & \text{number of “1“}s \text{ in } M(\complement A)_{2i_0} \\ = \ & (\text{number of “1“}s \text{ in } M(\{1,\dots,2a+1\}\backslash A_1)_{2i_0}) \\ & +(\text{number of “1“}s \text{ in } M(\{2a+2,\dots,t\}\backslash A_2)_{2i_0}) \\ = \ & (n_2 + m_{i_0}) + n_3 \\ \equiv \ & n_1 + n_3 + m_{i_0} \\ \equiv \ & 1 \pmod 2. \end{aligned}$$

Hence column $2i_0$ works for $\complement A$. The second possibility is

1”) $i_0 \in \{a+1,\dots,a+b\}$ and M_{22} is of type I:

Let k be the number of $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$–blocks in the columns $2i_0, 2i_0+1$ of M, which are different from the main diagonal block in these columns, and having exactly one row with a number in A.

Assume that column $2i_0+1$ does *not* work for A. Since $1 \in A$, this means that $k + m_{i_0}$ is odd. But then column $2i_0$ works for $\complement A$.

2) $\forall i \in \{1,\dots,a+b\} : 2 \mid |\{2i, 2i+1\} \cap A|$:

Choose an $i_0 \in \{1,\dots,a+b\}$ with $\{2i_0, 2i_0+1\} \cap A = \emptyset$.

If $i_0 \in \{a+1,\dots,a+b\}$ and M_{22} is of type I, then column $2i_0$ works for A.

So we only need to consider the case $i_0 \in \{1,\dots,a\}$ (as the case where $i_0 \in \{a+1,\dots,a+b\}$ and M_{22} is of type II is completely similar). If there is an *even* number of $j \in \{1,\dots,a\}$ with $2j, 2j+1 \in A$, then column $2i_0$ works for A. If there is an *odd* number of $j \in \{1,\dots,a\}$ with $2j, 2j+1 \in A$ and if j_0 is such a j, then column $2j_0$ works for $\complement A$. □

We can now give the promised application of theorem 4.9 (and theorem 4.12, for the claim about 2–class groups):

Theorem 5.16. *Let $a, b \in \mathbb{N}_0$ and let a be even.*
Let $q \equiv 3 \pmod 4, p_1 \equiv \cdots \equiv p_a \equiv p'_1 \equiv \cdots \equiv p'_b \equiv 1 \pmod 8$ be prime numbers such that:

1) $\left(\frac{q}{p_1}\right) = \cdots = \left(\frac{q}{p_a}\right) = \left(\frac{q}{p'_1}\right) = \cdots = \left(\frac{q}{p'_b}\right) = -1$*;*

2) for $i, j \in \{1, \dots, a\}, i \neq j$: $\left(\frac{p_i}{p_j}\right) = -1$*;*

3) for $i \in \{1, \dots, a\}, u \in \{1, \dots, b\}$: $\left(\frac{p_i}{p'_u}\right) = 1$*;*

4) for $u, v \in \{1, \dots, b\}, u \neq v$:
i) all the Legendre symbols $\left(\frac{p'_u}{p'_v}\right)$ have the value 1; or
ii) b is even and all the Legendre symbols $\left(\frac{p'_u}{p'_v}\right)$ have the value -1.

Then $i \in N_{\mathbb{Q}(i,\sqrt{qp_1\cdots p_a p'_1\cdots p'_b})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{qp_1\cdots p_a p'_1\cdots p'_b})})$ and the 2-class group $Cl_2(\mathbb{Q}(i, \sqrt{qp_1 \cdots p_a p'_1 \cdots p'_b}))$ is elementary abelian.

(And one of the equations $x^2 - qp_1 \cdots p_a p'_1 \cdots p'_b y^2 = \pm 2$ is solvable in $\mathbb{Z}$).

Proof. We can write $p_i = \pi_i \bar{\pi}_i$ and $p'_u = \pi'_u \bar{\pi}'_u$ where $(\pi_i), (\bar{\pi}_i), (\pi'_u), (\bar{\pi}'_u)$ are prime ideals of $K := \mathbb{Q}(i)$ and $\pi_i \equiv \pi'_i \equiv \pi_u \equiv \pi'_u \equiv 1 \pmod 4$. Then

$$\alpha = d = q\pi_1\bar{\pi}_1 \cdots \pi_a\bar{\pi}_a\pi'_1\bar{\pi}'_1 \cdots \pi_b\bar{\pi}_b.$$

Note that for $\gamma \in \{q, \pi_1, \bar{\pi}_1, \cdots, \pi_a, \bar{\pi}_a, \pi'_1, \bar{\pi}'_1, \cdots, \pi_b, \bar{\pi}_b\}$, the prime ideal $(1+i)$ and hence every prime of K different from (γ) is unramified in the extension $K(\sqrt{\gamma})/K$. So by theorem 4.9 it is enough to show that the (left or right) Redei matrix $M_{\mathbb{Q}(i,\sqrt{\alpha})/\mathbb{Q}(i)}$ has maximal rank: This follows immediately from lemma 5.9 and lemma 5.15. □

Note that the result in 2) of corollary 5.8 also follows by putting $a = 2$ and $b = 0$ in theorem 5.16.

We now investigate the case where $(\alpha) = (\pi)$ is a prime of $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. By the above, we only need to consider the split case, i.e. π has the form $\pi = a+bi; a, b \in \mathbb{Z}$, where $N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi) = a^2 + b^2 \equiv 1 \pmod 8$ is a prime number; hence $4 \mid ab$.

The following lemma is from the unpublished paper [19].

Lemma 5.17. *Let $\pi = a + bi$ be a prime of $\mathbb{Z}[i]$ with $2|a$ and $a + b \equiv \pm 1 \pmod 8$. Then*

$$4|h(Cl(\mathbb{Q}(i, \sqrt{\pi}))) \quad \Leftrightarrow \quad 8|a.$$

Proof. For the convenience of the reader, we sketch the proof from [19]:
Put $K := \mathbb{Q}(i, \sqrt{\pi})$ and $L := \mathbb{Q}(\sqrt{i}, \sqrt{\pi})$. As L/K is unramified, we have $2 \mid h(K)$. Since also the 2–class group $Cl_2(\mathbb{Q}(i, \sqrt{\pi}))$ is cyclic, we have

$$4 \mid h(K) \quad \Leftrightarrow \quad 2 \mid h(L).$$

By the ambiguous class number formula, applied to the extension L/F where $F = \mathbb{Q}(\sqrt{i})$, we have

$$2 \mid h(L) \quad \Leftrightarrow \quad [\mathcal{O}_F^* : N_{L/F}(L^*) \cap \mathcal{O}_F^*] = 1$$

since $h(F)$ is odd. A calculation of this index gives the result. □

Theorem 5.18. *Let $\pi = a + bi$ be a prime of $\mathbb{Z}[i]$.*
i) If $4 \mid b$, then $i \in N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$.
ii) If $4 \mid a$ and $a + b \equiv \pm 3 \pmod 8$, then $i \in N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$.
iii) If $4||a$ and $a + b \equiv \pm 1 \pmod 8$, then $i \notin N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$.

Proof. i) By [13], (π) is the only ramified prime ideal of the extension $\mathbb{Q}(i, \sqrt{\pi})/\mathbb{Q}(i)$. Hence the assertion follows from corollary 4.5.

ii) By [13], there are exactly two ramified primes of the extension $\mathbb{Q}(i, \sqrt{\pi})/\mathbb{Q}(i)$, namely (π) and $(1 + i)$. Let $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{Q}(i,\sqrt{\pi})}$ be the prime ideal above $(1 + i)$. By proposition 4.4, it is enough to show that $\mathfrak{p}$ is not principal:

As $(1 + i)$ is inert in $\mathbb{Q}(i, \sqrt{i\pi})$ (by [13]), $\mathfrak{p}$ is inert in $L := \mathbb{Q}(\sqrt{i}, \sqrt{\pi})$. Since the extension $L/\mathbb{Q}(i, \sqrt{\pi})$ is unramified, it follows from class field theory that $\mathfrak{p}$ is not principal.

iii) As $2||h(Cl(\mathbb{Q}(i, \sqrt{\pi})))$ (by lemma 5.17) and $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})/\mathbb{Q}(i, \sqrt{\pi})$ is unramified, $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})$ must be the 2-class field of $\mathbb{Q}(i, \sqrt{\pi})$. By [13], $(1 + i)$ splits totally in $\mathbb{Q}(i, \sqrt{i\pi})$ and $(1 + i)$ is ramified in $\mathbb{Q}(i, \sqrt{\pi})$. Hence the prime $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{Q}(i,\sqrt{\pi})}$ above $(1 + i)$ splits totally in $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})$; so $\mathfrak{p}$ must be principal. Since $N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi) \equiv 1 \pmod 8$, the prime (π) splits totally in $\mathbb{Q}(\sqrt{i})$; hence the prime $\mathfrak{p}_1 \subseteq \mathcal{O}_{\mathbb{Q}(i,\sqrt{\pi})}$ above (π) splits totally in $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})$; so $\mathfrak{p}_1$ is also principal. The theorem now follows from proposition 4.4. □

Remark 5.19. In the remaining case, $8|a$ and $a + b \equiv \pm 1 \pmod 8$, there seems to be no simple answer. For example, for some π of this kind it *is* true that $i \in N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$ and for some π this is false.

5.2 Quadratic Base Field with One Ramified Prime

Theorem 5.16 has the following analogue for quadratic fields with discriminant D of the form $D = -q$ where $q \equiv 3 \pmod 4$ is a prime number:

Theorem 5.20. *Let $q \equiv 3 \pmod 4$ be a prime number and let $a, b \in \mathbb{N}_0$ where a is even. Let $p, p_1, \dots, p_a, p'_1, \dots, p'_b$ be odd prime numbers with $p_1 \equiv \cdots \equiv p_a \equiv p'_1 \equiv \cdots \equiv p'_b \equiv 1 \pmod 4$. Assume that*

$$\left(\frac{-q}{p}\right) = -1, \quad p_i = \mu_i^2 + q\nu_i^2, \quad p'_j = (\mu'_j)^2 + q(\nu'_j)^2 \quad \textit{for some} \;\; \mu_i, \nu_i, \mu'_j, \nu'_j \in \mathbb{Z}$$

and

1) $\left(\frac{p}{p_1}\right) = \cdots = \left(\frac{p}{p_a}\right) = \left(\frac{p}{p'_1}\right) = \cdots = \left(\frac{p}{p'_b}\right) = -1$*;*

2) for $i, j \in \{1, \dots, a\}, i \neq j$: $\left(\frac{p_i}{p_j}\right) = -1$*;*

3) for $i \in \{1, \dots, a\}, u \in \{1, \dots, b\}$: $\left(\frac{p_i}{p'_u}\right) = 1$*;*

4) for $u, v \in \{1, \dots, b\}, u \neq v$:
 i) all the Legendre symbols $\left(\frac{p'_u}{p'_v}\right)$ have the value 1; or
 ii) b is even and all the Legendre symbols $\left(\frac{p'_u}{p'_v}\right)$ have the value -1.

Put $p^* := (-1)^{\frac{p-1}{2}}p$.
Then $N_{\mathbb{Q}(\sqrt{-q},\sqrt{p^*p_1\cdots p_a p'_1\cdots p'_b})/\mathbb{Q}(\sqrt{-q})}(\mathcal{O}^*_{\mathbb{Q}(\sqrt{-q},\sqrt{p^*p_1\cdots p_a p'_1\cdots p'_b})}) = \mathcal{O}^*_{\mathbb{Q}(\sqrt{-q})}$ and the 2-class group $Cl_2(\mathbb{Q}(\sqrt{-q}, \sqrt{p^*p_1 \cdots p_a p'_1 \cdots p'_b}))$ is elementary abelian.

Proof. This is analogous to the proof of theorem 5.16; the only thing which is not obvious is the fact that we can choose factorizations of p_i and p'_u such that the first (and hence also the other) factor is congruent to a square modulo 4 in $\mathcal{O}_{\mathbb{Q}(\sqrt{-q})}$:

Consider a prime number $p = w^2 + qz^2 \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 8$, then $4 \mid z$ and we choose the sign of w so that $w \equiv 1 \pmod 4$; then

$$w + z\sqrt{-q} = 1 + 4(\frac{w-1}{4} + \frac{z}{4}\sqrt{-q}) \equiv 1 \pmod 4.$$

If $p \equiv 5 \pmod 8$, then $2||z$ and we choose the sign of w so that $w \equiv 3 \pmod 4$; then

$$w + z\sqrt{-q} = 1 + 4\frac{\frac{w-1}{2} + \frac{z}{2}\sqrt{-q}}{2} \equiv 1 \pmod 4.$$

This completes the proof. □

Appendix A

Class Field Theory

We give here the necessary definitions and results from class field theory. The theorems are stated without proofs. The appendix is based on [9] and the appendix in [28].

A.1 Congruences and Ideal Groups

Let K be a number field. Let $\mathscr{M}^{(0)} = \prod \mathscr{P}_i^{e_i}$ be an integral ideal in K ($\mathscr{P}_i$ prime ideal) and let $\mathscr{M}_\infty = \prod \phi_j$ be a formal square-free (possibly empty) product of real infinite primes (i.e. embeddings $\phi_j : K \to \mathbb{R}$). The formal product $\mathscr{M} = \mathscr{M}^{(0)}\mathscr{M}_\infty$ is called a divisor of K.

Definition A.1. For $\alpha, \beta \in K$ define $\alpha \equiv \beta \pmod{\mathscr{M}}$ to mean:
(i) $(\alpha - \beta) = \mathscr{A}\mathscr{B}^{-1}$ for coprime integral ideals $\mathscr{A}, \mathscr{B}$ with $\mathscr{M}^{(0)} | \mathscr{A}$,
(ii) $\phi_j(\alpha/\beta) > 0$ for all ϕ_j in $\mathscr{M}_\infty$.

Note that i) is clearly equivalent to (i') $\forall i : e_i \geq 1 \Rightarrow v_{\mathscr{P}_i}(\alpha - \beta) \geq e_i$ where $v_{\mathscr{P}_i}$ is the $\mathscr{P}_i$-adic valuation in K.

It is elementary to show that $\alpha_1 \equiv \beta_1, \alpha_2 \equiv \beta_2 \pmod{\mathscr{M}} \Rightarrow \alpha_1\alpha_2 \equiv \beta_1\beta_2 \pmod{\mathscr{M}}$ and that for $\alpha \neq 0$: $\alpha \equiv 1 \pmod{\mathscr{M}} \Rightarrow 1/\alpha \equiv 1 \pmod{\mathscr{M}}$. The last statement ensures that the relation in the following definition is symmetric.

Definition A.2. For $\alpha, \beta \in K \backslash \{0\}$ define $\alpha \equiv \beta$ $(mod^* \mathscr{M})$ to mean that $\alpha/\beta \equiv 1 \pmod{\mathscr{M}}$.

A fractional ideal $\mathscr{A}\mathscr{B}^{-1}$ in K ($\mathscr{A}, \mathscr{B}$ coprime integral ideals) is said to be relatively prime to $\mathscr{M}$ if $\mathscr{A}$ and $\mathscr{B}$ are relatively prime to $\mathscr{M}^{(0)}$. So, for $\alpha, \beta \in K\backslash\{0\}$ with (α), (β) relatively prime to $\mathscr{M}$ we clearly have: $\alpha \equiv \beta \pmod{\mathscr{M}} \Leftrightarrow \alpha \equiv \beta$ $(mod^* \mathscr{M})$.

Definition A.3. $A_{\mathscr{M}} = A_{\mathscr{M}}(K) = \{\mathscr{F} | \mathscr{F}$ frac. ideal in K rel. prime to $\mathscr{M}$ $\}$, $S_{\mathscr{M}} = S_{\mathscr{M}}(K) = \{(\alpha) | \alpha \in K,\ \alpha \equiv 1 \pmod{\mathscr{M}}\}$.

$A_{\mathscr{M}}$ is an abelian group, and $S_{\mathscr{M}}$ is (by the above) a subgroup of $A_{\mathscr{M}}$. One can show that the factor group $A_{\mathscr{M}}/S_{\mathscr{M}}$ is finite.

A group H with $A_{\mathscr{M}} \supseteq H \supseteq S_{\mathscr{M}}$ is called an ideal group (modulo $\mathscr{M}$), and $\mathscr{M}$ is called a congruence module for H. The factor group $A_{\mathscr{M}}/H$ is called a (generalized) class group. $A_{(1)}/S_{(1)}$ is, of course, the usual class group for K. If ∞ denotes the product of the real embeddings of K, then $A_{(1)}/S_{\infty}$ is called the strict class group for K. It can easily be shown that every coset in $A_{\mathscr{M}}/H$ is represented by an integral ideal (in $A_{\mathscr{M}}$).

Proposition A.4. *Every coset of $A_{\mathscr{M}}/H$ contains an integral ideal in $A_{\mathscr{M}} \cap A_{\mathscr{T}} = A_{\mathscr{M}\mathscr{T}}$ for any given integral ideal $\mathscr{T}$. Therefore, with the obvious map,*

$$A_{\mathscr{M}\mathscr{T}}/(A_{\mathscr{M}\mathscr{T}} \cap H) \simeq A_{\mathscr{M}}/H.$$

A.2 The Main Theorems

Let L be a number field containing K and let $N_{L/K}\colon A_{(1)}(L) \to A_{(1)}(K)$ denote the relative norm map.

Definition A.5. An infinite prime $\mathfrak{P}$ (i.e. an embedding $K \to \mathbb{C}$) is unramified in L if either 1) $\mathfrak{P}$ is not real, or 2) $\mathfrak{P}$ is real and $\mathfrak{P}$ cannot be prolonged to a non-real embedding $L \to \mathbb{C}$.

Theorem A.6. *Let L/K be a finite abelian extension. Then there exists a divisor $\mathfrak{f}$ of K such that the following hold:*
(i) a prime $\mathfrak{P}$ (finite or infinite) in K ramifies in $L \Leftrightarrow \mathfrak{P}|\mathfrak{f}$.

(ii) If $\mathscr{M}$ is a divisor of K with $\mathfrak{f}|\mathscr{M}$, then the subgroup $H = N_{L/K}(A_{\mathscr{M}}(L))S_{\mathscr{M}}(K)$ of $A_{\mathscr{M}}(K)$ is such that $A_{\mathscr{M}}(K) \supseteq H \supseteq S_{\mathscr{M}}(K)$ and

$$A_{\mathscr{M}}(K)/H \simeq Gal(L/K).$$

Definition A.7. The minimal divisor $\mathfrak{f}$ making (i) and (ii) in theorem A.6 true is called the conductor of L/K and is denoted by $\mathfrak{f}_{L/K}$.

Remark A.8. One can show (with the notation as in theorem A.6 where, in particular, H depends on $\mathscr{M}$) that
a) if L_1/K, L_2/K are abelian with $L_1 \subseteq L_2$, then $\mathfrak{f}_{L_1/K}|\mathfrak{f}_{L_2/K}$;

b) if exactly one finite prime $\mathfrak{p}$ in K ramifies in L and if $\mathscr{M}$ is chosen as some power of $\mathfrak{p}$ times ∞ (the product of the real embeddings of K), then

$$H \supseteq S_{\mathfrak{p}^m\infty} \;\Rightarrow\; \mathfrak{f}^{(0)}_{L/K} | \mathfrak{p}^m$$

where $\mathfrak{f}^{(0)}_{L/K}$ is the finite part of $\mathfrak{f}_{L/K}$;
c) $H \supseteq A_{\mathscr{M}}(K) \cap S_{\mathfrak{f}_{L/K}}(K)$;
d) if some finite prime of K ramifies in L, then $H \not\supseteq A_{\mathscr{M}}(K) \cap S_{(1)}(K)$. (we note that d) follows from Satz (61) p. 80 in [9].)

Theorem A.9. *Let $\mathscr{M}$ be a divisor of K and let H be a subgroup of $A_{\mathscr{M}}$ with $A_{\mathscr{M}} \supseteq H \supseteq S_{\mathscr{M}}$. Then there exists a unique abelian extension L/K with $\mathfrak{f}_{L/K}|\mathscr{M}$, such that $H = N_{L/K}(A_{\mathscr{M}}(L))S_{\mathscr{M}}(K)$ and*

$$A_{\mathscr{M}}(K)/H \simeq Gal(L/K).$$

Remark A.10. Let L/K be abelian. Let $\mathscr{M}$ be a divisor of K with $\mathfrak{f}_{L/K}|\mathscr{M}$. Let $\mathfrak{p}$ be a prime ideal in K prime to $\mathscr{M}$. Then there is a unique $\sigma \in Gal(L/K)$ with

$$\forall\ \alpha \in \mathcal{O}_L : \quad \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{p}\mathcal{O}_L}.$$

This σ is called the Artin symbol corresponding to $\mathfrak{p}$ and is denoted by $\left(\frac{L/K}{\mathfrak{p}}\right)$. By extending this symbol multiplicatively to all of $A_{\mathscr{M}}(K)$, we get a homomorphism: $A_{\mathscr{M}}(K) \to Gal(L/K)$ called the Artin map. The isomorphisms mentioned in theorems A.6 and A.9 are induced by the Artin map.

Theorem A.11. *Let L_1/K and L_2/K be abelian extensions, let $\mathscr{M}$ be a multiple of $\mathfrak{f}_{L_1/K}$ and $\mathfrak{f}_{L_2/K}$, and let (cf. theorem A.6) $H_1, H_2 \subseteq A_{\mathscr{M}}(K)$ be the corresponding ideal groups. Then*

$$H_1 \subseteq H_2 \Leftrightarrow L_1 \supseteq L_2.$$

Theorem A.12. *Let $\mathfrak{p} \nmid \mathscr{M}$ be a prime ideal in K, unramified in the abelian extension L/K and below the prime ideal $\mathfrak{P}$ in L; let (cf. theorem A.6) H be the ideal group in $A_{\mathscr{M}}(K)$ corresponding to L (where $\mathfrak{f}_{L/K}|\mathscr{M}$). Then the order of the Artin symbol, the inertial degree, and the order of $\mathfrak{p}H$ (in $A_{\mathscr{M}}/H$) are equal:*

$$ord\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right) = f_{\mathfrak{P}|\mathfrak{p}} = ord(\mathfrak{p}H).$$

In particular,

$$\mathfrak{p} \text{ splits totally in } L \;\Leftrightarrow\; \mathfrak{p} \in H.$$

Theorem A.13. *Let H be an ideal group (modulo $\mathscr{M}$). Then every coset of $A_{\mathscr{M}}/H$ contains infinitely many prime ideals.*

Definition A.14. For an ideal group H in K define the conductor of H: $\mathfrak{f}_H = \mathfrak{f}_{L/K}$ where L is the unique abelian extension in theorem A.9.

Let L/K be a finite abelian extension and let H be the corresponding ideal group (modulo $\mathscr{M}$) in K. Let $\chi_1, \ldots, \chi_n$ be the group characters of $A_{\mathscr{M}}/$H (of course, n is the order of $A_{\mathscr{M}}/H$). For each i, write $\ker\chi_i = H_{\chi_i}/H$ where H_{χ_i} is an ideal group (modulo $\mathscr{M}$) and let $\mathfrak{f}_i = \mathfrak{f}_{H_{\chi_i}}$.

Theorem A.15 (Conductor-Discriminant Formula). *The relative discriminant of the finite abelian extension L/K is given by*

$$\mathcal{D}_{L/K} = \prod_{1=1}^{n} \mathfrak{f}_i^{(0)}.$$

Bibliography

[1] T. Bülow: The Negative Pell Equation, C. R. Math. Rep. Acad. Sci. Canada Vol. 24 (2), 2002, 55-60.

[2] T. Bülow: Power Residue Criteria for Quadratic Units and the Negative Pell Equation, Canad. Math. Bull Vol. 46 (1), 2003, 39-53.

[3] T. Bülow: Relative Norms of Units and 4-rank of Class Groups (submitted).

[4] T. Bülow: 4-rank of the Class Group of Certain Biquadratic Number Fields of Dirichlet Type, preprint.

[5] P.G.L. Dirichlet: Einige neue Sätze über unbestimmte Gleichungen, Gesammelte Werke, Chelsea, New York, 219-236.

[6] Y. Furuta: Norm of Units of Quadratic Fields, J. Math. Soc. Japan, No. 2, 1959, 139-145.

[7] F. Halter-Koch: Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Anwendung auf biquadratisch-zyklische Körper, J. Number Theory 4, 1972, 144-156.

[8] F. Halter-Koch: Konstruktion von Klassenkörpern und Potenzrestkriterien für quadratische Einheiten, Manuscr. Math 54, 1986, 453-492.

[9] H. Hasse: Vorlesungen über Klassenkörpertheorie, Physica-Verlag, Würzburg, 1967.

[10] H. Hasse: Bericht über Neuere Untersuchungen und Probleme aus der Theorie der Algebraischen Zahlkörper, Teil II, Teubner, 1930.

[11] H. Hasse: Ûber die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \pmod{2^3}$, Aeq. Math, Vol. 3, 1969, 165-195.

[12] E. Hecke: Lectures on the Theory of Algebraic Numbers, Springer-Verlag, 1981.

[13] D. Hilbert: Über den Dirichletschen biquadratischen Zahlkörper, Mathematische Annalen, 45, 1894, 309-340.

[14] L. Holzer: Zahlentheorie, II, Leipzig, 1958-1959.

[15] Chr. U. Jensen: On the Solvability of a Certain Class of non-Pellian Equations, Math. Scand. 10, 1962, 71-84.

[16] Chr. U. Jensen: On the Diophantine Equation $\xi^2 - 2m^2\eta^2 = -1$, Math. Scand. 11, 1962, 58-62.

[17] T. Kubota: Über den bizyklischen biquadratischen Zahlkörper, Nagoya Math. J., 10, 1956, 65-85.

[18] S. Lang: Cyclotomic Fields II, Springer-Verlag, 1980.

[19] F. Lemmermeyer: Class Number Parity, unpublished.

[20] W. Narkiewicz: Elementary and Analytic Theory of Algebraic Numbers, 2nd edition, Springer-Verlag, 1989.

[21] O. Perron: Die Lehre von den Kettenbrüchen, Teubner, Leipzig, 1929.

[22] J. Perrot: Sur l'equation $t^2 - Dy^2 = -1$, J. Reine Angew. Math. 102, 1888, 185-223.

[23] L. Rédei: Bedingtes Artinsymbol mit Anwendungen in der Klassenkörpertheorie, Acta Math. Sci. Hung. 4, 1953, 1-29.

[24] L. Rédei: Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, Acta Math. Sci. Hung. 4, 1953, 31-87.

[25] L. Rédei, H. Reichardt: Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math. 170, 1934, 69-74.

[26] H. Reichardt: Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math. 170, 1934, 75-82.

[27] A. Scholz: Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, Math. Zeitschrift 39, 1935, 95-111.

[28] L.C Washington: Introduction to Cyclotomic Fields, 2.edition, Springer-Verlag, 1997.

[29] B. L. van der Waerden: Algebra, Zweiter Teil, Springer-Verlag, 1967.

[30] D. Zagier: Zetafunktionen und quadratische Körper, Springer-Verlag, 1981.