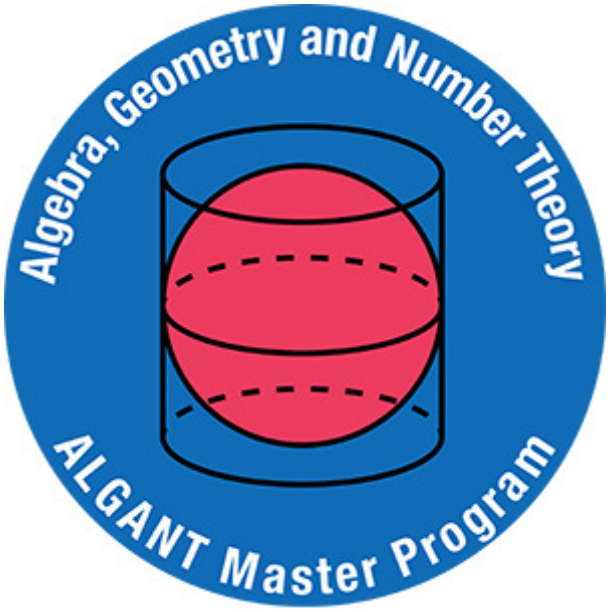


Angelo Iadarola

ON THE 8-RANK OF QUADRATIC CLASS GROUPS

Thesis advisor: Prof. Dr. Peter Stevenhagen

Universiteit Leiden

Academic Year 2016/2017

Acknowledgement

First of all I would like to thank my supervisor Prof. Dr. Peter Stevenhagen for being always available for clarifications, even when away from Leiden, and really involved in making both me and my thesis mathematically better by looking at my work with extreme precision.
Then I would like to thank Prof. Dr. S.J. Edixhoven, my Algant tutor in Leiden, who welcomed me warmly to the beautiful city of Leiden and the marvellous place known as Mathematisch Instituut and then helped me adapting to the Dutch academic system.
I would like to thank also Dr. Marco A. Garuti, the Algant coordinator in Padova, for being always available to answer my questions and help me out when in any kind of trouble.
I would like to thank the Algant consortium for giving me this unique academic opportunity to attend two very prestigious European universities and to boost my mathematical knowledge with the opportunity of working in a stimulating environment.
Vorrei ringraziare la mia famiglia per il fondamentale sostegno quotidiano che, anche da lontano, non mi ha mai fatto mancare in questi 5 anni intensi ma ricchi di soddisfazioni.
Last, but not least, I would like to thank all my friends from all over the world for both cheering my days and helping me out when in troubles according to what I was needing.

Contents

Chapter 1

Introduction

The focus of this thesis will be the study of the 2-part of the ideal class group of a quadratic number field.

A first definition of the class group dates back to 1801, even before a formal definition of ideals was given. It arose in the study of binary quadratic forms, polynomials of the type $ax^2 + bxy + cy^2$ with a, b, c integers, by Gauss in [7], who looked at the natural equivalence of forms under a change of variables (x, y) through linear transformations in $SL_2(\mathbb{Z})$. Gauss found a way to endow the set of equivalence classes of quadratic forms of given discriminant $D = b^2 - 4ac$ with a group structure. Only later, through the work of Dirichlet and Dedekind, it was realized that this group is the (narrow) ideal class group of the order $\mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$.

Around 1850, the class group arose also for higher degrees than quadratic, in Kummer's study of cyclotomic fields towards a proof of Fermat's Last Theorem, where he introduces "ideal numbers": in that case the problem was that the cyclotomic ring $\mathbb{Z}[\zeta_p]$ for p prime, is not always a principal ideal domain. Indeed, the finite size of its class group can be seen as a measure of how far the ring of integers of a number field is from being a principal ideal domain.

In the end, these appearances of the class group in, apparently, quite different contexts were unified and a formal definition of ideals was given by Dedekind [6]. Since then the study of the class group Cl_K of the ring of integers of the number field K has been central in algebraic number theory.

Another way of looking at the class group was provided by class field theory. The main information we get from class field theory is an isomorphism of finite abelian groups, the so-called Artin Map, between the class group of a number field and the Galois group $\mathrm{Gal}(H/K)$ of the Hilbert class field H of the number field over the number field K itself.

$$\mathrm{Cl}_K \xrightarrow[\sim]{\text{Artin Map}} \mathrm{Gal}(H/K)$$

Here the Hilbert class field is defined as the maximal abelian unramified extension of the number field.

Nowadays, much research about class groups concerns its average behaviour when looking at families of number fields. The first non-trivial case we can think of is quadratic fields.
Through modern software and other ad-hoc computational techniques, we have tools to study the class group of a quadratic number field and to provide evidence for its statistical behaviour when looking at families of quadratic number fields. Where the current difficulties lie mostly is in turning this computational evidence into actual mathematical statements with a complete theoretical proof. Indeed there are some statements dating back to Gauss which either were proven after many years or are still open problems.

A first example is provided by the Gauss class number problem in [7]: for given low class number (such as $1, 2, 3$) in 1801 Gauss gave a list of imaginary quadratic fields with the given

class number, conjecturing that such a list actually contained all the quadratic fields with that class number.
Gauss' lists were proven to be complete between the 1950's and 1980's for class number $1, 2, 3$ by Baker, Stark, Heegner, Oesterlé [8, 9, 12] and in 2004 for class number up to 100 by Watkins [21].

CONJECTURE 1.0.1 (Gauss 1801, [7]): *There are infinitely many real quadratic fields with class number* 1*.*

Although there is strong computational evidence in favour of this conjecture, it is still an open problem.

A way to approach the study of the average behaviour of quadratic class groups is understanding the average behaviour of their p-parts for p fixed.
For odd primes an important paper was published in 1984 by H. Cohen and H.W. Lenstra Jr. [2]; there the authors gathered most of the known computational evidence and proposed heuristics for the average behaviour of the odd primary parts. For instance, starting from the observation that, when $9||h_K$, for K imaginary quadratic, the rate of appearance of $C_3 \times C_3$ and C_9 as the 3-part of quadratic class groups is inversely proportional to the number of automorphisms of the two groups they formulated a more general conjecture for imaginary quadratic class groups.

CONJECTURE 1.0.2: *For every odd prime p and H abelian p-group, the probability*

$$\lim_{N\to\infty} \frac{1}{N} |\{-N < d < 0, d \text{ discriminant} : \mathrm{Cl}_K(\mathbb{Q}(\sqrt{d}))[p^\infty] \cong H\}|$$

exists, is positive and is inversely proportional to the number of automorphisms of H.

For the 2-part, which will be the focus of this thesis, there are more proven results than in the odd case. The oldest ones, concerning the 2-rank, date back to Gauss and others, concerning the 4-rank and 8-rank, to L. Rédei and H. Reichardt in the 1930's. These results gave the possibility to prove statements on the average behaviour of the 8-rank of quadratic class groups, at least in the case of some special families, like $\mathbb{Q}(\sqrt{-p})$ for p prime, which has cyclic 2-class group by genus theory.

By genus theory, calling $h(x)$ the class number of $\mathbb{Q}(\sqrt{x})$ for $x \in \mathbb{Z}$, we have

$$2|h(-4p) \Leftrightarrow p \equiv 1 \mod 4,$$

and Rédei's theorem implies that

$$4|h(-4p) \Leftrightarrow p \equiv 1 \mod 8.$$

P. Barrucand and H. Cohn found out that the 8-rank no longer depends on a congruence, but on the splitting in a non-abelian number field:

$$8|h(-4p) \Leftrightarrow p \text{ splits completely in } \mathbb{Q}\left(\zeta_8, \sqrt{1+\sqrt{2}}\right) \Leftrightarrow p = x^2 + 32y^2 \text{ for } x, y \in \mathbb{Z}. \quad (1.1)$$

This so-called Barrucand-Cohn theorem was proven in 1969 [1].

For the 2-rank and 4-rank it's clear that divisibility of $h(-4p)$ by 2 and 4 happens in $1/2$ and $1/4$ of the primes respectively. It follows from 1.1 that we have $8|h(-4p)$ is satisfied for $1/8$ of the primes. This is in line with the Cohen-Lenstra conjectures, which lead us to expect $2^k|h(-8p)$ for a fraction 2^{-k} of primes for all $k \geq 2$.

Based on the 8-rank result for $\mathbb{Q}(\sqrt{-p})$ and other fields like $\mathbb{Q}(\sqrt{\pm 2p})$ or $\mathbb{Q}(\sqrt{\pm pq})$ for p, q primes, in 1983 Cohn and J.C. Lagarias in [3] conjectured the following.

CONJECTURE 1.0.3 (Cohn-Lagarias conjecture): *Let $d, j \in \mathbb{Z}$. There exists a normal extension Ω_{2^j} over $\mathbb{Q}$ such that for primes $p_1, p_2 \nmid 2d$ with the same Frobenius symbol in $\Omega_{2^j}/\mathbb{Q}$, the groups $\mathrm{Cl}_K(\mathbb{Q}(\sqrt{dp_1}))$ and $\mathrm{Cl}_K(\mathbb{Q}(\sqrt{dp_2}))$ have the same 2^t-rank for $t \leq j$.*

If such a field exists, we call it Governing Field for the 2^j-rank.

The cases $j = 1, 2$ of this conjecture are obviously true from Gauss and Rédei's theory. For $j = 1$ we have $\Omega_2 = \mathbb{Q}(i)$; for $j = 2$ a governing field for the 4-rank exists and is contained in $\Omega_4(d) = \mathbb{Q}(i, \sqrt{2}, \{\sqrt{p} : p|d\})$. For $j = 3$ there was a lot of numerical evidence and some special cases had already been proven, supporting the fact that the conjecture may be true.

Indeed also for $j = 3$ the conjecture is true. The first complete proof was given by P. Stevenhagen in 1989 [20] and an alternative proof was provided by J. Corsman in 2007 [4] starting from Rédei's work. The aim of the thesis will be revising and correcting Corsman's proof trying to go through it with simpler tools than the ones used by him.

For $j = 4$ there is only negative evidence, provided mostly by D. Milovic in 2016 through analytical methods in [10], making it plausible that $j = 3$ is the only true and interesting instance of the conjecture.

1.1 Hilbert symbols

Before diving into the world of class groups, it's worth introducing a tool that will be largely used in the rest of this paper, the Hilbert symbols. We start defining it in the easiest setting, which is the rational numbers, then we will define it in the case of a general number field.

In the first case we give Serre's definition in [18, Chapter 3]. For each finite rational prime p, let $\mathbb{Q}_p$ be the p-adic completion, while for the infinite prime we let the real numbers $\mathbb{R}(= \text{“}\mathbb{Q}_\infty\text{”})$ be the usual completion for the euclidean norm.

DEFINITION 1.1.1 (Hilbert symbol): *Let $a, b \in \mathbb{Q}_p^*$ for p either finite or infinite. We define the Hilbert symbol*

$$(a,b)_p = \begin{cases} 1 & \text{if } x^2 - ay^2 - bz^2 = 0 \text{ has a non-trivial solution in } \mathbb{Q}_p^3 \\ -1 & \text{otherwise} \end{cases}.$$

Remark. As the value of the symbol doesn't change when multiplying a or b by a square, the Hilbert symbol defines a map $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \times \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \{\pm 1\}$.

PROPOSITION 1.1.2: *Let $a, b \in \mathbb{Q}_p^*$ for p either finite or infinite. Then we have*

$$(a,b)_p = 1 \Leftrightarrow a \in N(\mathbb{Q}_p(\sqrt{b})^*)$$

with $N : \mathbb{Q}_p(\sqrt{b})^* \to \mathbb{Q}_p^*$ the norm map.

For the infinite prime, $(a,b)_\infty = 1$ means just that a, b can't be both negative.
We have the following local-global property on the Hilbert symbols.

PROPOSITION 1.1.3: *Let $a, b \in \mathbb{Q}^*$. If $(a,b)_p = 1 \ \forall p \leq \infty$ prime, then the equation*

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

is non-trivially solvable in $\mathbb{Q}$, hence in $\mathbb{Z}$, and $a \in N(\mathbb{Q}(\sqrt{b})^*)$.

This is a classical result and a proof can be found in [18, p.42].
Now we go to the case when the setting isn't the rational numbers anymore, but a general

number field K.
In this case we will follow the presentation given by Neukirch [11, Chapter V §3], specializing it for the case $n = 2$, which is the one we will need.
Take a prime $\mathfrak{p}$ of K, either finite or infinite. Let $K_\mathfrak{p}$ be the completion of K at that prime. Let $L = K_\mathfrak{p}(\sqrt{K_\mathfrak{p}^*})$ be the maximal exponent 2 abelian extension of $K_\mathfrak{p}$. On the one hand, by class field theory we have the correspondence $\mathrm{Gal}(L/K_\mathfrak{p}) \simeq K_\mathfrak{p}^*/K_\mathfrak{p}^{*2}$ given by the Artin Map; on the other hand, by Kummer theory we have the isomorphism $\mathrm{Hom}(\mathrm{Gal}(L/K_\mathfrak{p}), \pm 1) \simeq K_\mathfrak{p}^*/K_\mathfrak{p}^{*2}$. Therefore the bilinear map

$$\begin{array}{rcl} \mathrm{Gal}(L/K_\mathfrak{p}) \times \mathrm{Hom}(\mathrm{Gal}(L/K_\mathfrak{p}), \pm 1) & \to & \pm 1 \\ (\sigma, \chi) & \mapsto & \chi(\sigma) \end{array}$$

gives rise to a perfect pairing

$$\begin{array}{rcl} K_\mathfrak{p}^*/K_\mathfrak{p}^{*2} \times K_\mathfrak{p}^*/K_\mathfrak{p}^{*2} & \to & \pm 1 \\ (a, b) & \mapsto & (a, b)_\mathfrak{p} \end{array}$$

called the Hilbert symbol of a, b at the ideal $\mathfrak{p}$.
We can give the explicit definition of the Hilbert symbol $(a, b)_\mathfrak{p}$ as

$$(a, b)_\mathfrak{p} = \frac{\sigma_a(\sqrt{b})}{\sqrt{b}},$$

where $\sigma_a \in \mathrm{Gal}(L/K_\mathfrak{p})$ is the element associated to a through the Artin Map.
In the case of $K = \mathbb{Q}$, this definition implies the one we gave before because the kernel of the local Artin map

$$K_\mathfrak{p}^* \to \mathrm{Gal}(K_\mathfrak{p}(\sqrt{b})/K_\mathfrak{p})$$

equals $N(K_\mathfrak{p}(\sqrt{b})^*)$.
From this definition some properties of the Hilbert symbols follow.

LEMMA 1.1.4: *Let $a, a', b \in K_\mathfrak{p}^*$. Then*

(i) $(a, b)_\mathfrak{p} = (b, a)_\mathfrak{p}$

(ii) $(aa', b)_\mathfrak{p} = (a, b)_p(a', b)_p$

(iii) For $\mathfrak{p}$ lying over an odd prime, $(a, b)_\mathfrak{p} = 1$ if a, b are units in $K_\mathfrak{p}^*$.

The definition of the Artin map implies that there is a link between Hilbert symbols and Legendre symbols: for $\mathfrak{p}||b$, but $\mathfrak{p} \nmid 2$ and $\mathrm{ord}_\mathfrak{p}\, a = 0$ we have

$$(a, b)_\mathfrak{p} = \left(\frac{a}{\mathfrak{p}}\right). \tag{1.2}$$

Class field theory implies the following

THEOREM 1.1.5 (Product Formula): *If $a, b \in K^*$, we have $(a, b)_\mathfrak{p} = 1$ for almost all $\mathfrak{p}$ and*

$$\prod_{\mathfrak{p}\ prime} (a, b)_\mathfrak{p} = 1.$$

In the case $K = \mathbb{Q}$, using (1.2), we see that the product formula implies the quadratic reciprocity law

$$\prod_{p \leq \infty} (p_1, p_2)_p = \left(\frac{p_1}{p_2}\right)\left(\frac{p_2}{p_1}\right)(p_1, p_2)_2 = 1.$$

In our case, we see that, for odd primes p_1, p_2, we have $(p_1, p_2)_2 = -1 \Leftrightarrow p_1 \equiv p_2 \equiv 3 \mod 4$, which implies the quadratic reciprocity law.
More generally, the symbol $(-,-)_2$ can be computed as follows.

PROPOSITION 1.1.6: $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \langle 2 \rangle \times \langle -1 \rangle \times \langle 5 \rangle$.

This proposition lets us build a table of the Hilbert symbols at 2 to compute the Hilbert symbol $(p_1, p_2)_2$.

$(-,-)_2$	2	-1	5
2	1	1	-1
-1	1	-1	1
5	-1	1	1

1.2 First theorems

Let $K = \mathbb{Q}(\sqrt{d})$ be the quadratic number field determined by the squarefree integer d. K has discriminant

$$D = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{otherwise} \end{cases}$$

In his work Gauss didn't encounter the usual class group, but the narrow class group, which is defined as follows

DEFINITION 1.2.1 (Narrow Class Group): *The narrow class group of K is*

$$\mathrm{Cl}_K = I_K / P_K^+,$$

where P_K^+ is the group of principal ideals generated by totally positive elements of K^*.

The 2-part of this group has nicer theorems and is easier to be dealt with. Moreover there is a surjection $\mathrm{Cl}_K \twoheadrightarrow \mathrm{Cl}_K^{ord}$ onto the "ordinary" class group $\mathrm{Cl}_K^{ord} = I_K/P_K$, whose kernel P_K/P_K^+, where P_K is the group of all the principal ideals of K, has order at most 2.
If $D < 0$ or $D > 0$ with $N(\varepsilon_D) = -1$ then $P_K = P_K^+$ so $\mathrm{Cl}_K = \mathrm{Cl}_K^{ord}$, while if $D > 0$ and $N(\varepsilon_D) = 1$, then $\#(P_K/P_K^+) = 2$ and we have the exact sequence

$$0 \to [(\sqrt{D})] \to \mathrm{Cl}_K \twoheadrightarrow \mathrm{Cl}_K^{ord} \to 0. \tag{1.3}$$

From now on we will omit "narrow", saying just class group and writing Cl_K.

Since we're going to deal with the $2, 4, 8$-rank of class groups it's worth recalling the general definition of 2^k-rank of a finite abelian group.

DEFINITION 1.2.2 (2^k-rank): *For a finite abelian group A, its 2^k-rank is defined as*

$$\begin{aligned} r_{2^k}(A) &= \dim_{\mathbb{F}_2}(2^{k-1}A/2^kA) \\ &= \dim_{\mathbb{F}_2} A[2^k]/A[2^{k-1}] \end{aligned}$$

Looking at the decomposition of the group A into cyclic groups as

$$A = \prod_i C_{n_i},$$

the 2^k-rank equals the number of n_i's divisible by 2^k.

1.2.1 2-rank

First of all we will look at the 2-torsion of the class group. As already said in the introduction, this result dates back to Gauss and his Genus Theory.

THEOREM 1.2.3: *Given a quadratic field K of discriminant D, the 2-rank of its class group is $r_2 = t - 1$, where t is the number of distinct prime divisors of D.*

This theorem is a classical result, so we're omitting a detailed proof [5, Theorem 6.1], giving only an outline of two possible proofs, since we're going to use them in the study of the 4-rank. The second definition of 2-rank we gave is $r_2 = \dim_{\mathbb{F}_2} \mathrm{Cl}_K[2]$. We have the following key statement which gives a complete description of $\mathrm{Cl}_K[2]$

PROPOSITION 1.2.4: *The set $\{\mathfrak{p}_i | D,\ \mathfrak{p}_i$ prime in $K\}$ of the prime ideals dividing the discriminant of K has cardinality t. The ideal classes $[\mathfrak{p}_i]$ have order dividing 2 and generate $\mathrm{Cl}_K[2]$ subject to a single relation*

$$\sum_{i=1}^{t} \varepsilon_i [\mathfrak{p}_i] = [0] \in \mathrm{Cl}_K \quad \text{for } \varepsilon_i \in \mathbb{F}_2 \text{ not all } 0.$$

Again, this is a classical result so we omit the proof, [5, Theorem 6.1].

Remark. The proposition guarantees that such a relation exists. As we mentioned after Definition 1.2.1, if $D < 0$ or $D > 0$ with $N(\varepsilon_D) = -1$ the narrow class group is equal to the ordinary class group, so we have the trivial relation

$$\sum_{i=1}^{t} \mathrm{ord}_{\mathfrak{p}_i}(\sqrt{D})[\mathfrak{p}_\mathrm{i}] = [(\varepsilon_D \sqrt{D})] = [0],$$

while when $D > 0$ and $N(\varepsilon_D) = 1$ we notice that $(1 + \varepsilon_D^{-1}) = \varepsilon_D^{-1}(1 + \varepsilon_D)$, so the ideal $(1 + \varepsilon_D)$ is self-conjugate, hence is a product of primes of the form $\mathfrak{p}_i$ times a rational integer:

$$\sum_{i \in I} [\mathfrak{p}_i] = [(1 + \varepsilon_D)] = [0].$$

This means that in the latter case finding this relation is linked to finding a fundamental unit in K, which may not be easy.

By the proposition it follows that we can build a surjective map of $\mathbb{F}_2$-vector spaces

$$\begin{aligned} \mathbb{F}_2^t &\to \mathrm{Cl}_K[2] \\ e_i &\mapsto [\mathfrak{p}_i] \end{aligned}$$

whose kernel has dimension 1. These $[\mathfrak{p}_i]$ were called ambiguous ideal classes by Gauss, because they are equal to their inverse. This implies that the dimension of $\mathrm{Cl}_K[2]$ as $\mathbb{F}_2$-vector space is actually $t - 1$.

The first definition of 2-rank we gave of 2-rank is $r_2(\mathrm{Cl}_K) = \dim_{\mathbb{F}_2}(\mathrm{Cl}_K/2\,\mathrm{Cl}_K)$.
In the introduction we've already seen the isomorphism of abelian groups, called Artin isomorphism

$$\mathrm{Cl}_K \xrightarrow[\sim]{\text{Artin}} \mathrm{Gal}(H/K)$$

realizing the (narrow) class group as the Galois group of the Hilbert (narrow) class field H over the base field K.
This means that the quotient $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$ of Cl_K corresponds by Galois theory to an intermediate extension between K and H. In order to understand which extension it is, we note that H is Galois over $\mathbb{Q}$ because K is fixed by any automorphism τ of $\overline{\mathbb{Q}}$, so $\tau(H)$ is again a maximal abelian unramified extension of K, so it must be H. Moreover, we have the exact sequence

$$1 \to \mathrm{Cl}_K \to \mathrm{Gal}(H/\mathbb{Q}) \to \langle\sigma\rangle \to 1$$

where $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$.
Take a ramifying prime p in $K/\mathbb{Q}$ and let $\mathfrak{P}$ be a prime in H over p. Since H/K is finitely unramified, the ramification index of $\mathfrak{P}$ in $H/\mathbb{Q}$ equals 2 and the ramification comes from $K/\mathbb{Q}$ so its inertia group is isomorphic to $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. This isomorphism gives an injection $\langle\sigma\rangle \hookrightarrow \mathrm{Gal}(H/\mathbb{Q})$ which implies that the previous exact sequence (right) splits, so we have

$$\mathrm{Gal}(H/\mathbb{Q}) = \mathrm{Cl}_K \rtimes \langle\sigma\rangle. \tag{1.4}$$

The Norm function $I_K \xrightarrow{N_{K/\mathbb{Q}}} I_{\mathbb{Q}}$ restricted to principal ideals P_K^+ has image inside the principal ideals $P_{\mathbb{Q}}^+ = I_{\mathbb{Q}}$, so it induces a Norm map on the class group

$$\mathrm{Cl}_K \xrightarrow{N} \mathrm{Cl}_{\mathbb{Q}} = [0].$$

Since $N([\mathfrak{a}]) = (1+\sigma)([\mathfrak{a}]) = [0]$, we have that the action of σ is given by the inversion, i.e. H is a dihedral extension of $\mathbb{Q}$.
We recall that for a dihedral group $G = A \rtimes \langle\sigma\rangle$ with A abelian, its commutator subgroup equals $[G,G] = A^2$, so $G^{ab} = A/A^2 \times \langle\sigma\rangle$. In our case, this implies that $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$ corresponds to the maximal (finitely) unramified abelian extension of K which is abelian also over $\mathbb{Q}$. We denote it by H_2 and call it the genus field of K.

Proposition 1.2.5: *Let $K = \mathbb{Q}(\sqrt{d})$ and $D = \mathrm{disc}(K)$. We have $H_2 = \mathbb{Q}(\{\sqrt{p_i^*} : p_i | D\})$, where p_i ranges over the prime divisors of D and $p_i^* = \pm p_i \equiv 1 \mod 4$ if p is odd, while*

$$2^* = \begin{cases} -4 & \text{if } d \equiv 3 \mod 4 \\ 8 & \text{if } d \equiv 2 \mod 8 \\ -8 & \text{if } d \equiv -2 \mod 8 \end{cases}.$$

Also the proof of this theorem can be found in [5, Theorem 6.1]. From this proposition we see that the degree of the extension H_2 over $\mathbb{Q}$ is 2^t, so the degree of the extension H_2/K is 2^{t-1}, implying that the 2-rank is indeed $t-1$.

1.2.2 4-rank

Now we can shift to the study of the 4-rank of the class group, following the theory developed by L. Rédei and H. Reichardt in [13, 14, 15].

The key idea from Rédei was considering the two groups $\mathrm{Cl}_K[2]$ and $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$ and linking them not with the non-canonical group isomorphism given by the definition of 2-rank, but with the natural map coming from the projection of Cl_K onto $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$:

$$\mathrm{Cl}_K[2] \xrightarrow{\varphi} \mathrm{Cl}_K/2\,\mathrm{Cl}_K\,.$$

From the exact sequence

$$1 \to \frac{\mathrm{Cl}_K[2] + 2\,\mathrm{Cl}_K}{2\,\mathrm{Cl}_K} \to \mathrm{Cl}_K/2\,\mathrm{Cl}_K \xrightarrow{\times 2} 2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K \to 0$$

we see that we have

$$\frac{\mathrm{Cl}_K}{\mathrm{Cl}_K[2] + 2\,\mathrm{Cl}_K} \simeq 2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K \tag{1.5}$$

so, in particular, they have the same cardinality 2^{r_4}. Looking at the left hand side, its cardinality is

$$\frac{h_K \cdot |\,\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K\,|}{|\,\mathrm{Cl}_K[2]||2\,\mathrm{Cl}_K\,|} = |\,\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K\,|$$

by Definition 1.2.2, so $|2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K\,| = |\,\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K\,| = |\ker\varphi| = 2^{r_4}$. This implies that, being $2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K$ and $\mathrm{Cl}_K[2]\cap 2\,\mathrm{Cl}_K$ vector spaces over $\mathbb{F}_2$ of the same dimension, $2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K$ and $\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K$ are non-canonically isomorphic and the 4-rank of Cl_K is $r_4 = \dim_{\mathbb{F}_2} \ker\varphi$.

Using Class Field Theory and the description of $\mathrm{Cl}_K[2]$ and $\mathrm{Cl}_K/2\,\mathrm{Cl}_K$ that we gave in the previous section we can build the following diagram:

$$\begin{array}{ccccc}
\mathrm{Cl}_K[2] & \xrightarrow{\varphi} & \mathrm{Cl}_K/2\,\mathrm{Cl}_K & \xrightarrow{\sim} & \mathrm{Gal}(H_2/K) \hookrightarrow \mathrm{Gal}(H_2/\mathbb{Q}) = \prod_{i=1}^{t} \mathrm{Gal}(\mathbb{Q}(\sqrt{d_i^*})/\mathbb{Q}) \\
\text{Prop 1.2.4}\uparrow & & & & \downarrow\sim \\
\mathbb{F}_2^t & & \xrightarrow{\qquad\qquad R_4 \qquad\qquad} & & \mathbb{F}_2^t
\end{array}$$

Therefore we have the following

THEOREM 1.2.6: $r_4 = t - 1 - \mathrm{rank}_{\mathbb{F}_2} R_4$.

Proof. The composition of maps $\mathrm{Cl}_K/2\,\mathrm{Cl}_K \to \mathbb{F}_2^t$ is injective, so the kernel of R_4 comes from $\ker\varphi$ and the first map, which, from Prop 1.2.4, has kernel of dimension 1. □

This theorem implies that computing the $\mathbb{F}_2$-linear map R_4 immediately yields r_4.

Let $R_4 = (c_{ij}) \in \mathrm{Mat}_{t\times t}(\mathbb{F}_2)$ be the matrix representation of $R_4 : \mathbb{F}_2^t \to \mathbb{F}_2^t$.
From the Artin Map we get that the ij-entry, $i \neq j$, describes the action of the Artin symbol of the i-th generator $\mathfrak{p}_i|p_i$ on the j-th element defining the Genus Field $\sqrt{p_j^*}$. Since we're dealing with quadratic extensions, this action can be written in terms of Legendre symbols, as

$$(-1)^{c_{ij}} \overset{(i\neq j)}{=} \left(\frac{p_j^*}{p_i}\right) \text{ for } p_i \text{ odd.}$$

If $\exists i$ s.t. $p_i = 2$, for $j \neq i$ we put $c_{ij} = 0$ if 2 splits in $\mathbb{Q}(\sqrt{p_j^*})$ and $c_{ij} = 1$ otherwise.
Moreover we know that the sum of the entries in every row has to be zero because all Artin symbols fix $\prod_{j=1}^{t} \sqrt{p_j^*} = \sqrt{D}$ so

$$c_{ii} = \sum_{\substack{j=1 \\ j\neq i}}^{t} c_{ij}.$$

1.3 8-rank of quadratic class groups

For the 8-rank Rédei developed an idea similar to the one for the 4-rank in [16, 17].
We saw in the previous section that there is a non-canonical isomorphism between $\ker\varphi =$

$\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K$ and $2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K$, but we can link them also with the natural map coming from the projection of $2\,\mathrm{Cl}_K$ onto $2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K$

$$\ker R_4 \twoheadrightarrow \ker\varphi = \mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K \xrightarrow{\psi} 2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K \overset{\text{Artin}}{\simeq} \mathrm{Gal}(H_4/H_2)$$

where H_4 is the 4-Hilbert class field, i.e. the unramified abelian subextension $H_4 \subset H$ of K such that $\mathrm{Gal}(H_4/K) = \mathrm{Cl}_K/4\,\mathrm{Cl}_K$.
In the same fashion as for the 4-rank we get that $r_8 = \dim_{\mathbb{F}_2} \ker\psi$.

Since $2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K \simeq (\mathbb{Z}/2\mathbb{Z})^{r_4}$ by definition of 4-rank, we get that H_4 can be obtained from H_2 by adjoining r_4 independent square roots of elements in H_2 which we denote by α_i for $i = 1, \dots, r_4$, so we can draw the following diagram, similar to the one for the 4-rank

$$\begin{array}{ccccc}
\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K & \xrightarrow{\psi} & 2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K & \xrightarrow[\sim]{\text{Artin}} & \mathrm{Gal}(H_4/H_2) = \prod_{i=1}^{r_4} \mathrm{Gal}(H_2(\sqrt{\alpha_i})/H_2) \\
\uparrow & & & & \downarrow \sim \\
\ker R_4 & & \xrightarrow{\qquad R_8 \qquad} & & \mathbb{F}_2^{r_4}
\end{array}$$

from which the theorem for the 8-rank follows immediately.

THEOREM 1.3.1: $r_8 = r_4 - \mathrm{rank}_{\mathbb{F}_2} R_8$.

Proof. The proof goes exactly as in Theorem 1.2.6: the composition $2\,\mathrm{Cl}_K/4\,\mathrm{Cl}_K \to \mathbb{F}_2^{r_4}$ is injective so the kernel of R_8 comes from the first two maps. □

Remark. The domain $\ker R_4$ has dimension $r_4 + 1$ instead of r_4, but this way of writing the map is more convenient because we avoid the problem of finding the fundamental unit to describe the kernel of Gauss' map as in Remark 1.2.1.

As for the 4-rank, we want to give an explicit description of R_8. Looking at the diagram we see that we need to find out how the Artin symbol of elements in $\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K$ acts on $\sqrt{\alpha_i}$: differently from the 4-rank where we had information on p_i^*, here we don't know much about α_i. Therefore, for the rest of the section our focus will be finding α_i and understanding this action.

We can choose α_i such that $\sqrt{\alpha_i}$ generates a normal extension $F \subset H$ over K, given by its splitting field, which is cyclic of degree 4 over K. Moreover $F \cap H_2$ is equal to a biquadratic extension $L = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2}) \subset H_2$ with $D_1 \cdot D_2 = D$ and $D_1 = \prod_{i \in I} p_i^*$ with $I \subset \{1, \dots, t\}$. Therefore we need to generate r_4 independent such F to describe R_8.
On the other side, call $\hat{L} \subset H_2$ the subfield corresponding to $\mathrm{Cl}_K/(\mathrm{Cl}_K[2] + 2\,\mathrm{Cl}_K)$. By (1.5) $\hat{L}$ is of degree 2^{r_4} over K.

LEMMA 1.3.2: *Let $L = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ be as above. Then the following are equivalent:*

(i) $\exists L \subset F$ *quadratic such that* $F \subset H_4$ *and* F *is cyclic of degree 4 over* K*;*

(ii) $\mathrm{Art}_{\mathfrak{p}_i, L/K} = id_L \quad \forall \mathfrak{p}_i | D$*;*

(iii) $L \subset \hat{L}$.

Proof. *(i)* ⇒ *(ii)* Look at the Artin symbol of $\mathfrak{p}_i$ inside F: since $[\mathfrak{p}_i]$ is of order at most 2 in Cl_K, by Artin isomorphism also its Artin symbol must be an element of order 2 in $\mathrm{Gal}(F/K)$. The latter fact implies that $\mathrm{Art}_{\mathfrak{p}_i, F/K}$ fixes L.
(ii) ⇒ *(iii)* $L \subset H_2$ implies that L is fixed by Artin symbols of classes in $2\,\mathrm{Cl}_K$. By (ii) L is

also fixed by Artin symbols of classes in $\mathrm{Cl}_K[2]$, so L is fixed by Artin symbols of classes in $\mathrm{Cl}_K[2] + 2\,\mathrm{Cl}_K$, i.e. $L \subset \hat{L}$.
$(iii) \Rightarrow (i)$ There exist r_4 "independent" fields F and $\hat{L}$ is of degree 2^{r_4} over K, so $\hat{L}$ is the composite of all the extensions L which can be extended to an F as in (i). □

In particular (ii) from the previous Lemma is equivalent to saying that $\forall i\ \mathfrak{p}_i$ splits in L/K. Therefore we want to find which sets $I \subset \{1, \ldots, r_4\}$ are such that $K(\sqrt{D_1})/K$ has this property. We're identifying the sets I and $\{1, \ldots, r_4\} \setminus I$ because they give rise to the same field.

Definition 1.3.3 (D-decomposition of the 2nd kind): *Given a discriminant D, we say that $D = D_1 D_2$ is a D-decomposition of the 2nd kind for D if*

(i) D_1, D_2 *are discriminants*

(ii) $(D_1, D_2)_p = 1\ \forall p \leq \infty$ *prime*

(iii) if $2|D_i \Rightarrow (D/D_i, 2)_2 = 1$.

We say that a D-decomposition is non-trivial if neither of the factors is 1.

These decompositions of the discriminant D are exactly the ones we're looking for because of the following lemma.

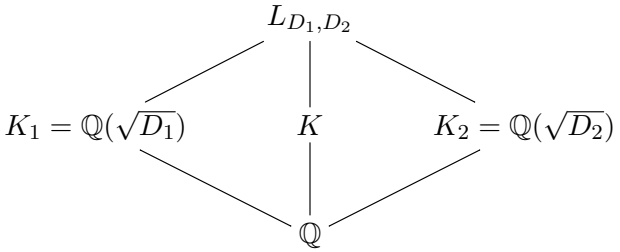
Lemma 1.3.4: *For discriminants D_1, D_2 such that $D = D_1 D_2$, the following are equivalent:*

(i) $D = D_1 D_2$ *is a D-decomposition of the 2nd kind*

(ii) $p|D_i \Rightarrow \left(\frac{D/D_i}{p}\right) = 1$

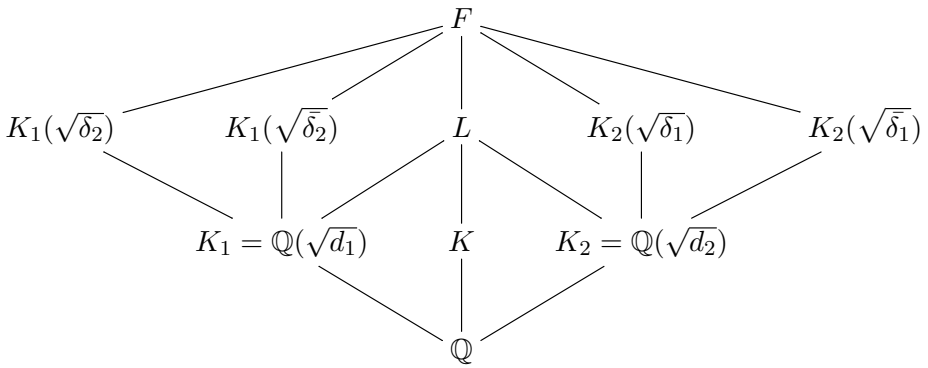
(iii) All primes $\mathfrak{p}|D$ in K split in $L_{D_1,D_2} = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})/K$.

Proof. $(i) \Leftrightarrow (ii)$ is trivial because of (1.2).
$(ii) \Leftrightarrow (iii)$ Look at the following diagram



(ii) implies that if a prime p ramifies in one of the side extensions, then it must split in the other side extension, hence ramify in $K/\mathbb{Q}$, so the primes $\mathfrak{p}$ lying over p must split in L/K. □

Since F is dihedral of degree 8 over $\mathbb{Q}$ we can draw the full diagram of subfields. We write d_1, d_2 for the largest squarefree divisors of D_1 and D_2



Now we're showing how we can construct δ_2, which is one of the α_i's which determine the map R_8 as in Theorem 1.3.1.
Condition (ii) in the definition of D-decomposition of the 2nd kind tells us, by Proposition 1.1.3 the equation

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

in non-trivially solvable over $\mathbb{Q}$ (or $\mathbb{Z}$), which implies that we can pick $\delta_2 = x + y\sqrt{d_1}$ such that F/L is unramified.
However, we have to be very careful, because Lemma 1.3.2 guarantees only the existence of such a field F, but it may not be unique. However, our interest about F is limited to how the Artin symbol of ideal classes in $\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K$ acts on $\sqrt{\delta_2}$, so it's enough to have the following.

LEMMA 1.3.5: *Let $[\mathfrak{m}] \in \mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K$. If F_1, F_2 are two different choices as cyclic extensions of degree 4 over K coming from the same D-decomposition of the 2nd kind, then*

$$F_1 H_2 = F_2 H_2.$$

Proof. Coming from the same D-decomposition of the 2nd kind, $F_1 \cap F_2 = L$, so they are not independent. □

By Lemma 1.3.2, prime ideals in K above primes ramifying in $K/\mathbb{Q}$ split in L/K, so, in particular, we have that the Artin symbol of $\mathfrak{m}$ actually lies in $\mathrm{Gal}(F/L)$.
Therefore we are now ready to define the Rédei symbol, as Rédei himself did in [17].

DEFINITION 1.3.6 (Rédei symbol): *Let D_1, D_2 be a D-decomposition of the 2nd kind. Let $m|D$ be a squarefree integer such that $[\mathfrak{m}] \in \mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K$ is represented by $\mathfrak{m}$ of norm m. Then we can define the Rédei symbol*

$$[d_1, d_2, m] = \mathrm{Art}_{\mathfrak{m}, F/K} \in \mathrm{Gal}(F/L) \simeq \mathbb{F}_2.$$

Two immediate properties of this symbol follow. It is trivially symmetric in the first two entries because L doesn't change when swapping d_1 and d_2. Moreover the symbol is additive in the third entry when taking the entries "modulo squares" because the Artin symbol is multiplicative in the ideal.

THEOREM 1.3.7 (8-rank of quadratic class groups): *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant D. Define the map of $\mathbb{F}_2$-vector spaces*

$$\ker R_4 \xrightarrow{R_8} \mathbb{F}_2^{r_4}$$

as in Theorem 1.3.1.
Let $(d_1^{(i)}, d_2^{(ii)})_{i=1}^{r_4}$ *be such that* $L_{d_1^{(i)},d_2^{(i)}} = \mathbb{Q}\left(\sqrt{d_1^{(i)}}, \sqrt{d_2^{(i)}}\right)$ *generate* $\hat{L}$.
Then R_8 *maps an ideal class* $[\mathfrak{m}]$*, with* $\mathfrak{m}$ *of norm* m*, to the* r_4*-tuple* $([d_1^{(i)}, d_2^{(i)}, m])_{i=1}^{r_4}$.

Proof. R_8 maps an ideal class $[\mathfrak{m}]$ to the action of the Artin symbol of $\mathfrak{m}$ on the elements α_i generating H_4 over H_2. By Theorem 1.3.2 the α_i's are in bijection with the D-decompositions of the 2nd kind of D, so, by definition of the Rédei symbol, the statement follows. □

Now we will give an example to show that these ranks can really be computed in concrete cases.

Example. Consider $K = \mathbb{Q}(\sqrt{-205})$. Its discriminant is $D = -4 \cdot 5 \cdot 41$, it has $t = 3$ distinct prime divisors, so from Theorem 1.2.3 $r_2 = 2$.
Computing all the Legendre symbols and using the "rule" for the diagonal, the matrix R_4 is

$$R_4 = \begin{pmatrix} & \sqrt{-1} & \sqrt{5} & \sqrt{41} \\ \mathfrak{p}_2 & 1 & 1 & 0 \\ \mathfrak{p}_5 & 0 & 0 & 0 \\ \mathfrak{p}_{41} & 0 & 0 & 0 \end{pmatrix}$$

The matrix has rank 1, so $r_4 = 2 - 1 = 1$.
It follows that $\mathrm{Cl}_K / 4\,\mathrm{Cl}_K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
In this case $\mathrm{Cl}_K[2]$ has basis $\mathfrak{p}_2, \mathfrak{p}_5$ because $\mathfrak{p}_5\mathfrak{p}_{41} = (\sqrt{-205})$, but, in general, especially in the case of real quadratic fields, we may want to keep all the generators.
Moreover, looking at the matrix we can deduce that $\mathrm{Cl}_K[2] \cap 2\,\mathrm{Cl}_K$ is generated by $\mathfrak{q}_5$ because its Artin symbol fixes $\sqrt{-1}, \sqrt{5}, \sqrt{41}$.
Always looking at the matrix, we notice that $\sqrt{-1} \cdot \sqrt{5}$ and $\sqrt{41}$ are the two elements which are fixed by the Artin symbol of all the three ideals, so $-5 \cdot 41$ is the only D-decomposition of the 2nd kind.
An element $\sqrt{\alpha}$ with $\alpha \in \mathbb{Q}(\sqrt{-5})$ generating an unramified extension F of $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-41})$ comes from a suitable solution of

$$x^2 + 5y^2 - 41z^2 = 0.$$

Picking $x = -7, y = 8, z = 3$ makes $\alpha = -7 + 8\sqrt{-5} \equiv 1 \mod 4$.
We can find the Artin symbol of $\mathfrak{p}_5$ in $\mathrm{Gal}(F/L)$ by checking whether the prime $\mathfrak{p}_5 = (\sqrt{-5})$ splits in $\mathbb{Q}(\sqrt{-5}) \subset \mathbb{Q}(\sqrt{-5}, \sqrt{\alpha})$. We find the Rédei symbol equals 1, as we have

$$\left(\frac{-7 + 8\sqrt{-5}}{\sqrt{5}}\right) = \left(\frac{-7}{5}\right) = -1.$$

This means that $r_8 = 0$.
In particular, also $r_{2^k} = 0$ for $k \geq 3$ so the 2-part is $\mathrm{Cl}_K^{(2)} K = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
Moreover, we have that $H_4 = \mathbb{Q}\left(i, \sqrt{5}, \sqrt{41}, \sqrt{-7 + 8\sqrt{-5}}\right)$.

Chapter 2

Cohn-Lagarias conjecture for the 8-rank

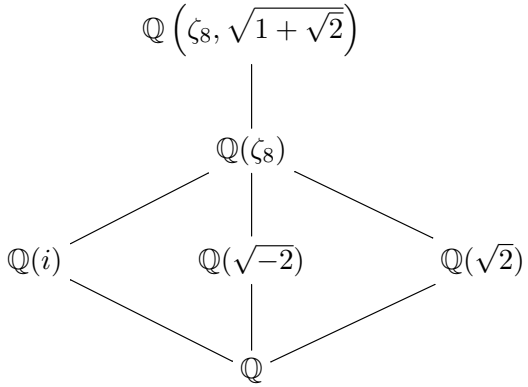
Now, using the classical results from the first chapter, we will address the main theorem.

THEOREM 2.0.1 (Cohn-Lagarias for the 8-rank): *Let $d \in \mathbb{Z}$ non-zero and not a square. There exists a normal extension Ω_8 over $\mathbb{Q}$ s.t. if p_1, p_2 are two odd rational primes not dividing d with the same Artin symbol in $\Omega_8/\mathbb{Q}$, then $\mathrm{Cl}_K(\mathbb{Q}(\sqrt{dp_1}))$ and $\mathrm{Cl}_K(\mathbb{Q}(\sqrt{dp_2}))$ have the same $2, 4, 8$-rank.*

We call such a field a Governing Field for the 8-rank. As we saw in the introduction the inspiration behind this theorem comes from one of the first examples of family of quadratic fields we can think of: $K = \mathbb{Q}(\sqrt{-p})$ with p a prime number. Barrucand and Cohn found out that

$$8|h(-4p) \Leftrightarrow p \text{ splits completely in } \mathbb{Q}\left(\zeta_8, \sqrt{1+\sqrt{2}}\right) \Leftrightarrow p = x^2 + 32y^2$$

Looking at K, we see that if $4|h(-4p)$ then $-4, p$ is a D-decomposition of the 2nd kind because $-4p$ has one non-trivial D-decomposition of the 2nd kind, being $p \equiv 1 \mod 8$, and $-4 \cdot p$ is the only candidate; the fact that $8|h(-4p)$ is equivalent to Cl_K having non-zero 8-rank, i.e. the only Rédei symbol defining the matrix for the 8-rank $[-1, p, 2] = 0$.
On the other side, the field $\mathbb{Q}\left(\zeta_8, \sqrt{1+\sqrt{2}}\right)$ is a D_4 extension of $\mathbb{Q}$, so we can build a (partial) diagram of subfields



From the diagram we see that p splitting in $\mathbb{Q}\left(\zeta_8, \sqrt{1+\sqrt{2}}\right)$ is equivalent to saying that the Artin symbol

$$\mathrm{Art}_{\mathfrak{p}, \mathbb{Q}\left(\zeta_8, \sqrt{1+\sqrt{2}}\right)/\mathbb{Q}(\sqrt{-2})} = 0$$

where $\mathfrak{p}$ is a prime ideal in $\mathbb{Q}(\sqrt{-2})$ lying over p.
Looking blindly at Definition 1.3.6 of Rédei symbol we would be naturally tempted to identify that Artin symbol with the Rédei symbol $[-1,2,p]$ because $\mathbb{Q}\left(\zeta_8, \sqrt{1+\sqrt{2}}\right)$ is dihedral of degree 8 over $\mathbb{Q}$ with $d=-2$ and $d_1=-1, d_2=2$. This is not possible according to our theory because not only $-4\cdot 8$ is far from being a D-decomposition of the 2nd kind for -8, but, even more, $\mathbb{Q}(\sqrt{-2})$ has class number 1, so we can't find any other candidate as D-decomposition of the 2nd kind because $\mathbb{Q}(\sqrt{-2})$ doesn't have any unramified extension of degree 4.
These remarks suggest two things:

1. The definition of Rédei symbol we gave may have too strong assumptions, failing in a natural example, and may be improved weakening the assumptions in order to catch a wider set of cases;

2. Looking carefully at what we said, we note that, assuming that 1. is achievable, Barrucand-Cohn statement may be rephrased as

$$[-1,p,2]=0 \Leftrightarrow 8|h(-4p) \Leftrightarrow [-1,2,p]=0$$

   We saw that the Rédei symbol is naturally symmetric in the first two entries, while in the third one it looks completely asymmetric. However this new formulation of Barrucand-Cohn makes us wonder whether, in a wider setting, there may be a symmetry also in third entry.

The answer to these 2 questions will be the subject of the next section, while in the last section we will present a proof of the main theorem.

2.1 Rédei symbol and Reciprocity Law

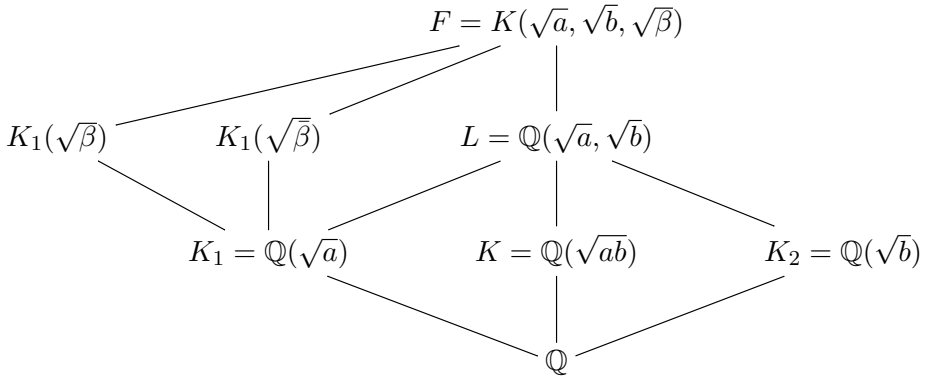
In the previous chapter we talked about D-decompositions of the 2nd kind, which let us build extensions of K which are unramified at all finite primes, which is a pivotal fact at that point because we need to work inside the Hilbert class field of K, and we considered only ideal classes in $\mathrm{Cl}_K[2]\cap 2\,\mathrm{Cl}_K$, but looking strictly at the symbols, what we need is, generally speaking, our topmost field F and an ideal in K of which we can define the Artin symbol, i.e. not divisible by primes ramifying in F/K, and force it to be in $\mathrm{Gal}(F/L)$: this is of course much less than asking for the extension to be unramified everywhere!
This is the general idea we want to pursue and that we will turn it into mathematics.

Let $\bar{a},\bar{b}\in(\mathbb{Q}^*/\mathbb{Q}^{*2})\setminus\{\bar{1}\}$ be two classes represented by two squarefree integers a,b. Assume that $(a,b)_p=1\ \forall p\leq\infty$ By Proposition 1.1.3, this implies that the equation

$$x^2-ay^2-bz^2=0 \tag{2.1}$$

is non-trivially solvable over $\mathbb{Q}$, so we can pick a non-trivial solution (x,y,z) and define $\beta=x+y\sqrt{a}$. As we saw in the previous chapter, for $a\neq b$, β generates a cyclic extension of degree 4 over K, dihedral of degree 8 over $\mathbb{Q}$, which we call $F=\mathbb{Q}(\sqrt{a},\sqrt{b},\sqrt{\beta})$. For $a=b$ the field F is cyclic of degree 4 over $K=\mathbb{Q}$.
For the rest of the section it's helpful to draw at least a partial diagram of $F/\mathbb{Q}$, also in order

to fix some notation.



Equation 2.1 has many different solutions and we are interested in studying the ramification in this diagram according to the choice of β, because our final purpose will be computing Artin symbols in this diagram.

LEMMA 2.1.1: *We can choose β such that $F/\mathbb{Q}$ is unramified outside $S(a) \cup S(b)$.*

Proof. Assume p odd. We claim that taking $\beta = x + y\sqrt{a}$ with $gcd(x, y) = 1$ implies that $p \nmid ab$ is unramified in $F/\mathbb{Q}$.
Non ramification in $L/\mathbb{Q}$ is guaranteed by the fact that p is unramified in both K_1 and K_2 by assumption. For ramification in F/L we can look at $K_1(\sqrt{\beta})/K_1$: from $p \nmid \beta$ in K_1 we see that at most one prime $\mathfrak{p}|p$ can divide β and that such $\mathfrak{p}$ is of norm p. From $N(\beta) \in b \cdot \mathbb{Q}^{*2}$ and $p \nmid b$ we see that $\mathrm{ord}_{\mathfrak{p}}(\beta)$ is even, hence $\mathfrak{p}$ is unramified in F/K.
Now consider the prime 2. Then $2 \notin S(a) \cup S(b)$ implies that $a \equiv b \equiv 1 \mod 4$. Look at the equation (2.1) $\mod 4$: we have $x^2 - y^2 - z^2 \equiv 0 \mod 4$, so 2 divides exactly one of y, z. Say $2|y$. Take x with sign such that $x - y \equiv 1 \mod 4$. Then

$$\beta = x + y\sqrt{a} = (x - y) + 2y\frac{1 + \sqrt{a}}{2} \in \mathcal{O}_{K_1}$$

so $\beta \equiv 1 \mod 4$ and $L(\sqrt{\beta})/L$ is unramified over 2. □

We are interested in computing Artin symbols over K instead of over $\mathbb{Q}$, so we have also to take into account primes which ramify in $K_i/\mathbb{Q}$ and see whether we can make F/K unramified at primes in K above them.

PROPOSITION 2.1.2: *Let p be an odd prime, $F = \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{\beta})$ with $\beta = x + y\sqrt{a}$ primitive element in $\mathcal{O}_K$.*

(i) $p|gcd(a, b) \Rightarrow p$ is unramified in $\mathbb{Q} \subset K$, totally ramified in $K \subset F$;

(ii) $p|ab, p \nmid gcd(a, b) \Rightarrow p$ is ramified in $\mathbb{Q} \subset K$, unramified in $K \subset F$.

If $2 \in S(a), b \equiv 1 \mod 8$ or $2 \in S(b), a \equiv 1 \mod 8 \Rightarrow 2$ is unramified in $K \subset F$ for a suitable choice of β.

Proof. Let p be an odd prime.

(i) Since $p|gcd(a, b)$, it follows that p ramifies in L/K. As F/K is cyclic, p ramifies also in F/L.

(ii) $p|ab, p \nmid gcd(a,b)$ implies that p ramifies in $K/\mathbb{Q}$ and is unramified in L/K.
Wlog, assume that $p|a, p \nmid b$. To study the ramification of p in F/L it's enough to look at $K_1(\sqrt{\beta})/K_1$. Since β is primitive, there can't exist p dividing x, y. Moreover, if $\mathfrak{p}$ above p in K_1 divides β, then $\mathfrak{p}^2 = p|\beta\bar{\beta} = N(\beta) = b$, which is a contradiction. So $\mathfrak{p}$ is unramified in F/K.

Now consider the prime 2. We have two possible cases, since one between a, b must be $\equiv 1 \mod 8$. Moreover note that, in general, $(a,b)_p = 1 \Rightarrow (4a,b)_p = 1$ for odd and infinite primes, so also for $p = 2$ by Theorem 1.1.5.
So we can focus on the equation $x^2 - d(a)y^2 - d(b)z^2 = 0$.
Case 1: assume $a \equiv 3 \mod 4$, then $b \equiv 1 \mod 8$. Look at the equation modulo 8: we have that $x^2 - 4y^2 - z^2 \equiv 0 \mod 8$ which implies that y must be even and $x \equiv 1 \mod 4$, so $\beta \equiv 1 \mod 4$.
Case 2: assume $a \equiv 2 \mod 4$ and $b \equiv 1 \mod 8$. Look at the equation modulo 16: we have that $x^2 - 8y^2 - bz^2 \equiv 0 \mod 16$; moreover $b \equiv 1, 9 \mod 16$. In the first case, if we can choose y even, then it is the same as before, while if we choose y odd we have that $x \equiv 3 \mod 4$ and $y \equiv 1 \mod 4$. □

Now let c be another squarefree integer. Assume that

$$S(a) \cap S(b) \cap S(c) = \emptyset \tag{2.2}$$

where, in general, $S(x) = \{p | p \text{ ramifies in } \mathbb{Q}(\sqrt{x})/\mathbb{Q}\}$, and

$$(a,b)_p = (a,c)_p = (b,c)_p = 1 \quad \forall p \leq \infty \text{ prime}. \tag{2.3}$$

These hypotheses imply that a dihedral field F as in Lemma 2.1.1 and Proposition 2.1.2 exists, and that for every prime $p|c$ we have that

- By (2.3), p splits or ramifies in $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$;
- By (2.2), p is not ramified in both $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$.

Moreover, for $2|c$ one of a or b is $1 \mod 4$ by (2.2) and therefore $1 \mod 8$ by the table at the end of Section 1.1.
Thus, by Proposition 2.1.2, we can always choose F in such a way that F/K is unramified above all $p|c$ and that the Artin symbol $\mathrm{Art}_{\mathfrak{p},F/K}$ for a prime $\mathfrak{p}|p$ is in $\mathrm{Gal}(F/L)$.
As $\mathrm{Gal}(F/L)$ is in the center of the group $\mathrm{Gal}(F/\mathbb{Q})$ (equal to it when dihedral, strictly contained when $a = b$), this implies that $\mathrm{Art}_{\mathfrak{p},F/K}$ is independent of the choice of a prime $\mathfrak{p}|p$ in K.

Similarly, in the case $a, b > 0$, the field $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ is totally real and for every infinite prime of K we have an element $\mathrm{Art}_{\infty,F/K} \in \mathrm{Gal}(F/L)$ that is non-trivial if and only if F is totally complex and independent of the choice of an infinite prime.

We have proved the following.

PROPOSITION 2.1.3: *Let a, b, c be squarefree integers $\neq 1$ satisfying (2.2) and (2.3). Let F be as in Lemma 2.1.1 and such that 2 is unramified in F/K for $2|c$.*
Then the element $\mathrm{Art}_{\mathfrak{c},F/K}$ for $\mathfrak{c}$ an integral ideal of norm $|c|$ of K is an element of $\mathrm{Gal}(F/L)$ that does not depend on the choice of $\mathfrak{c}$.

From now on we will say that an extension F cyclic of degree 4 over K and dihedral of degree 8 over $\mathbb{Q}$ is chosen *correctly* if F/K is unramified outside $S(a) \cup S(b)$ and at prime ideals dividing $\mathfrak{c}$.

DEFINITION 2.1.4 (Rédei symbol): *Let a, b, c be squarefree integers $\neq 1$ satisfying (2.2) and (2.3).*
Take $\mathfrak{c}$ an ideal in K of norm $|c|$.
If F is chosen correctly, we define the Rédei symbol $[a, b, c]_F$ as

$$[a,b,c]_F = \begin{cases} \mathrm{Art}_{\mathfrak{c},F/K} & \text{if } c > 0 \\ \mathrm{Art}_{\infty,F/K} \cdot [a,b,-c]_F & \text{if } c < 0 \end{cases} \in \mathrm{Gal}(F/L) \simeq \{\pm 1\}.$$

As final step in this definition we want to get rid of the dependency on F.

LEMMA 2.1.5: *Let a, b, c be as in Definition 2.1.4. Let F, F' be cyclic extensions of $K = \mathbb{Q}(\sqrt{ab})$ of degree 4 generated by $\alpha, \alpha' \in K_1$. If F and F' are both chosen correctly, then*

$$[a,b,c]_F = [a,b,c]_{F'}.$$

Proof. Through Artin isomorphism we can see the Rédei symbol $[a, b, \bullet]_F$ (resp. $[a, b, \bullet]_{F'}$) as a character $\chi_F : \mathrm{Cl}_K \to \mathbb{C}^*$ (resp. $\chi_{F'}$) with image isomorphic to $\mathbb{Z}/4\mathbb{Z}$. As $F \cap F' = \mathbb{Q}(\sqrt{ab})$ we have

$$\chi_F^2 = \chi_{F'}^2 = \chi_a : \mathrm{Cl}_K \to \pm 1 \tag{2.4}$$

with χ_a the quadratic character of L/K defined by the Jacobi symbol $\left(\frac{a}{\bullet}\right)_K$, which is defined outside primes dividing a. Note that if $\mathfrak{p}|a$, but $\mathfrak{p} \nmid b$, then we can define χ_a equivalently as $\left(\frac{b}{\mathfrak{p}}\right)_K$, being L/K quadratic and $ab = D_K$. If $\mathfrak{p}|gcd(a, b)$ we put $\chi_a(\mathfrak{p}) = 0$, but this is irrelevant in our case because of assumption (2.2).
Equality (2.4) implies that

$$\chi_F = \chi_{F'} \cdot \chi_x$$

for $x \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ and χ_x the quadratic character defined in the same way as χ_a. This implies that

$$F' = L(\sqrt{\beta} \cdot \sqrt{x}).$$

Since by assumption F and F' are chosen correctly, we have that $x|ab$, so $\chi_x(\mathfrak{c})$ is defined by assumption (2.2) and, even more, $\chi_x(\mathfrak{c}) = 1$ by assumption (2.3).
Therefore

$$[a,b,c]_F = \chi_F(\mathfrak{c}) = \chi_{F'}(\mathfrak{c}) = [a,b,c]_{F'}.$$

□

Remark. We see that, in Rédei's case, this definition is equivalent to Definition 1.3.6 because the condition on the Hilbert symbols and $S(d_1) \cap S(d_2) = \emptyset$ are satisfied by Definition 1.3.3, and m is always positive.

Now we can state the reciprocity law for Rédei symbols, which we are not proving.

THEOREM 2.1.6 (Rédei reciprocity law): *Let a, b, c be as in 2.1.4. Then*

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

Remark. In [17, p.20, Satz 4] Rédei provides a proof of this theorem using his definition of the symbol, which was different from Corsman's one because in Rédei's definition $[a, b, c] = [a, b, -c]$. This fact explains the presence of a "factor at infinity" when $c < 0$ or $b < 0$. Rédei's 1938 proof does not use ideles, cohomology or even Hilbert symbols, but it is the only correct one up to now.

In [4], Corsman has the correct intuition in the definition of the Rédei symbol, letting us stating the reciprocity law in a symmetric way. However, his proof incorrectly treats the ramification at 2 in Lemma 5.1.2.

A third statement of the reciprocity law was given by A. Smith in [19, Proposition 2.1], but it is incorrect.

Example. Consider the triple $37, -3, 73$. In our setting, this is a fairly simple triple because the three numbers are signed primes $\equiv 1 \mod 4$.
We can explicitly find the elements α_{-3}, α_{73} in $\mathbb{Q}(\sqrt{37})$ generating the appropriate dihedral extensions, and compute the two symbols.
$\alpha_{-3} = \frac{-5+\sqrt{37}}{2} \equiv \left(\frac{1+\sqrt{37}}{2}\right)^2$, so $[37, -3, 73] = 1$ as

$$\left(\frac{\alpha_{-3}}{\mathfrak{p}_{73}}\right) = \left(\frac{\frac{-5+\sqrt{37}}{2}}{73}\right) = \left(\frac{407}{73}\right) = -1$$

and $\mathrm{Art}_{\infty,F/K}$ is trivial, being K and F are both complex.
On the other hand, $\alpha_{73} = \frac{-25+3\sqrt{37}}{2} \equiv \left(\frac{1+3\sqrt{37}}{2}\right)^2$. With a computation similar to the previous one we have that $\left(\frac{\alpha_{73}}{\mathfrak{p}_3}\right) = 1$, but this time K is real, while α_{73} is totally negative, so F is complex which means that $\mathrm{Art}_{\infty,F/K}$ is non-trivial, so $[37, 73, -3] = 1$.

2.2 Proof of the main theorem

We're now ready to provide a proof of the Cohn-Lagarias conjecture for the 8-rank using the theory on Rédei symbols we developed in the previous sections and Theorem 1.3.7.
Let's start giving the following proposition which will provide us two key corollaries for the main proof.

PROPOSITION 2.2.1: *Let p_1, p_2 be two odd primes not dividing d such that $p_1 \equiv p_2 \mod 4d$. Writing $\mathrm{disc}(dp_i) = \prod_{i=1}^{t} d_i$ as a factorization of discriminants with $d_t = p_i^*$, the entries in the R_4 matrices of $\mathbb{Q}(\sqrt{dp_1})$ and $\mathbb{Q}(\sqrt{dp_2})$ are equal.*

Proof. Recall the definition of R_4 from Theorem 1.2.6: we need to compute the Legendre symbols $\left(\frac{d_j}{q_j}\right)$, with q_j the positive prime dividing d_j.
For $i \neq j$ and $1 \leq i, j \leq t-1$, p doesn't appear in the symbols so they are obviously the same. For either $i = t$ or $j = t$ the equality follows by assumption that $p_1 \equiv p_2 \mod 4d$, so also the diagonal follows, being c_{ii} the sum of the elements in the i-th row. □

COROLLARY 2.2.2: *(i) If $\mathrm{disc}(\mathbb{Q}(\sqrt{dp_1})) = Dp_1^* = D_1 D_2$ is a D-decomposition of the 2nd kind, with $p_1 | D_2$, then $\mathrm{disc}(\mathbb{Q}(\sqrt{dp_2})) = Dp_2^* = D_1 \left(\frac{D_2}{p_1^*} p_2^*\right)$ is a d-decomposition of the 2nd kind.*

(ii) Let m be a divisor of D such that $[mp_1^\varepsilon] \in 2\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{dp_1})}$ for some $\varepsilon \in 0, 1$. Then $[mp_2^\varepsilon] \in 2\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{dp_2})}$

Proof. (i) D-decompositions of the 2nd kind are the generators of $\ker R_4^T$, so the statement follows.

(ii) If $[mp_i^\varepsilon] \in 2\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{dp_i})}$, then it is in $\ker R_4 = \mathrm{Cl}_{\mathbb{Q}(\sqrt{dp_i})}[2] \cap 2\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{dp_i})}$. Since the R_4 matrix is equal, the statement follows.

□

One last ingredient we need for the proof is a rather easy lemma, which gives the value of the symbol for a particular triple. Moreover we give this immediate relation, which will be useful later.

LEMMA 2.2.3: *Let D_1, D_2 be a D-decomposition of the 2nd kind for D. Then $[d_1, d_2, -D] = 0$, where d_1, d_2 are the squarefree integers such that $D_i = \mathrm{disc}(\mathbb{Q}(\sqrt{d_i}))$ for $i = 1, 2$.*

Proof. Recall from Chapter 1 (1.3):

$$0 \to [(\sqrt{D})] \to \mathrm{Cl}_K \twoheadrightarrow \mathrm{Cl}_K^{ord} \to 0$$

We need to divide this result into two cases.
Case 1: $D < 0$. Then $-D > 0$, so $\mathrm{Cl}_K = \mathrm{Cl}_K^{ord}$, so $[(\sqrt{D})]$ is the trivial class, which implies that $\mathrm{Art}_{(\sqrt{D}),F/K}$ is trivial.
Case 2: $D > 0$. The narrow Hilbert class field H is defined as the maximal abelian extension unramified at all finite primes, while the ordinary one H^{ord} is defined as the maximal abelian extension unramified at all finite and infinite primes, so we have an exact sequence

$$1 \to Art_\infty \to H \to H^{ord} \to 1.$$

This exact sequence, together with the one we recalled and Artin isomorphism, yields that

$$\mathrm{Art}_{(\sqrt{D}),H/K} = \mathrm{Art}_{\infty,H/K},$$

so their restrictions to F are equal. This implies that $[d_1, d_2, -D] = \mathrm{Art}^2_{(\sqrt{D}),F/K}$ is trivial. □

We will now state a theorem which will easily imply the Cohn-Lagarias result that we want to prove.
Let Dp^* be the discriminant of $\mathbb{Q}(\sqrt{dp})$. We can find D-decompositions of the 2nd kind D_1, D_2 of Dp^*: by symmetry we can always assume that p^* is contained in D_2. Therefore when we consider the Rédei symbols $[d_1, d_2, m]$ defining the map R_8 as in Theorem 1.3.7 we can always assume that $p|d_2$ and $p \nmid d_1$, i.e. d_1 does not depend on p.

THEOREM 2.2.4: *Let d be a squarefree integer. For all $d_1|d$ with $D_1 = \mathrm{disc}(\mathbb{Q}(\sqrt{d_1}))$ and m a positive integer, there exists a field $\Omega_8(d_1, m)$ such that the following holds.*
Given an odd prime $p \nmid d$, let $Dp^* = \mathrm{disc}(\mathbb{Q}(\sqrt{dp}))$ and $D_2 = \frac{Dp^*}{D_1}$ so that d_2 is the squarefree integer such that $D_2 = \mathrm{disc}(\mathbb{Q}(\sqrt{d_2}))$. If D_1, D_2 is a D-decomposition of the 2nd kind for Dp^* and there is an ideal $\mathfrak{m}$ of $\mathbb{Q}(\sqrt{dp})$ of norm m such that $[\mathfrak{m}] \in \mathrm{Cl}_{\mathbb{Q}(\sqrt{dp})}[2] \cap 2\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{dp})}$, then $[d_1, d_2, m]$ depends only on the splitting behaviour of p in $\Omega_8(d_1, m)$.

Whenever the assumptions of the theorem are satisfied, we say that $\Omega_8(d_1, m)$ governs the symbol $[d_1, d_2, m]$.

Proof. Consider $[d_1, d_2, m]$ for d_1, d_2 providing a D-decomposition of the 2nd kind for Dp^*.
If $p|m$ then we can multiply by the symbol from Lemma 2.2.3 so that, by additivity on the third entry, $[d_1, d_2, m] = [d_1, d_2, m']$, where m' is the biggest squarefree divisor of $-Dm$, so that $p \nmid m'$. Now only one between d_1, d_2 is divisible by p. Assume that it is d_2.
Now we can apply the Reciprocity Law to have that $[d_1, d_2, m'] = [d_1, m', d_2]$ so that now p is isolated in third entry, which means that we can study how the symbol behaves when p varies, since the first two entries, which define the diagram of field in which we're working, are fixed.
Call α_m the element defining the topmost field F. Looking at the definition of the Rédei symbol, by multiplicativity of the Artin symbol, the only factor depending on p is

$$\mathrm{Art}_{\mathfrak{p},\mathbb{Q}(\sqrt{d_1},\sqrt{\alpha_m},\sqrt{\bar{\alpha_m}})/\mathbb{Q}(\sqrt{d_1})}\,.$$

This Artin symbol is trivial if $\mathfrak{p}$ totally splits in $\mathbb{Q}(\sqrt{d_1}, \sqrt{\alpha_m}, \sqrt{\bar{\alpha_m}})$, while non-trivial otherwise, so $\Omega_8(d_1, m) = \mathbb{Q}(\sqrt{d_1}, \sqrt{\alpha_m}, \sqrt{\bar{\alpha_m}})$. □

The Cohn-Lagarias Theorem for the 8-rank is now only a corollary.
Using Corollary 2.2.2, we can compare 8-rank matrices for p with same residue class $\bmod 4d$. The corollary says that if p_1, p_2 are in the same residue class then the Rédei symbols for $\mathbb{Q}(\sqrt{dp_1})$ and $\mathbb{Q}(\sqrt{dp_2})$ are governed by the same field. So the splitting of all the primes in the same residue class is governed by the composite of $\Omega_8(d_1, m)$ over d_1 ranging among the D-decompositions of the 2nd kind and $\mathfrak{m}$ among a basis of $\mathrm{Cl}_{\mathbb{Q}(\sqrt{dp})}[2] \cap 2\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{dp})}$.
Taking the composite over all the residue classes yields the governing field for the 8-rank.
This fact gives also information about $\mathrm{Gal}(\Omega_8/\mathbb{Q})$. Since Ω_8 is obtained first by adjoining $\sqrt{p_i}$ for $p_i|2d$ prime divisor and $\sqrt{-1}$ and then by adjoining all the $\sqrt{\alpha_m}$ for each D-decomposition of the 2nd kind, each ideal $\mathfrak{m}$ and each residue class $\bmod 4d$, the result is that $\mathrm{Gal}(\Omega_8/\mathbb{Q})$ is a 2-group.

Bibliography

[1] P. Barrucand; H. Cohn. *Note on primes of type $x^2 + 32y^2$, class number, and residuacity.* Journal für die reine und angewandte Mathematik, **238**, pp. 67-70, 1969.

[2] H. Cohen; H. W. Lenstra Jr. *Heuristics on class groups of number fields.* Lecture Notes in Math., **1068**, Springer, Berlin, pp. 33-62, 1984.

[3] H. Cohn; J.C. Lagarias. *On the Existence of Fields Governing the 2-Invariants of the Classgroup of $Q(\sqrt{dp})$ as p Varies.* Mathematics of Computation, **41**(164), pp. 711-730, 1983.

[4] J. Corsman. *Rédei symbols and governing fields.* PhD Thesis, McMaster University, 2007.

[5] D.A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* 2nd edition, Wiley, 2013.

[6] R. Dedekind. *Vorlesungen über Zahlentheorie.* 1894.

[7] C.F. Gauss. *Disquisitiones Arithmeticae.* 1801.

[8] K. Heegner. *Diophantische Analysis und Modulfunktionen.* Mathematische Zeitschrift, **56**(3): 227-253, 1952.

[9] K. Ireland; M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, New York, pp. 358-361, 1993.

[10] D. Milovic. *On the 16-rank of class groups of quadratic number fields.* PhD Thesis, Universiteit Leiden, Université Paris-Sud, 2016.

[11] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, Berlin Heidelberg, 1999.

[12] J. Oesterlé. *Nombres de classes de corps quadratiques imaginaire.* Sem. Bourbaki, **631**, 1983-84.

[13] L. Rédei; H. Reichardt. *Die durch vier teilbaren Invarianten der Klassengruppe des quadratischen Zahlkörpers.* Journal für die reine und angewandte Mathematik, (170), pp.69-74, 1933.

[14] L. Rédei. *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper.* Journal für die reine und angewandte Mathematik, (171), pp.55-60, 1934.

[15] L. Rédei. *Eine obere Schranke der Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper.* Journal für die reine und angewandte Mathematik, (171), pp.61-64, 1934.

[16] L. Rédei; *Über die Grundeinheit und die durch acht teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*. Journal für die reine und angewandte Mathematik, (171), pp. 131-148, 1934.

[17] L. Rédei. *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper*. Journal für die reine und angewandte Mathematik, (180), pp. 1-43, 1938.

[18] J.P. Serre. *A Course in Arithmetic*. Springer-Verlag, New York, 1973.

[19] A. Smith. *Governing fields and statistics for 4-Selmer groups and 8-class groups*. https://arxiv.org/abs/1607.07860v1, 2016.

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

[21] M. Watkins. *Class numbers of imaginary quadratic fields*. Mathematics of Computation, **73**, pp. 907-938, 2004.