On the Second Class Group of Real Quadratic Number Fields

Maximilian Boy

Vom Fachbereich Mathematik
der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor der Naturwissenschaften
(Doctor rerum naturalium, Dr. rer. nat.)
genehmigte Dissertation

1. Gutachter: Prof. Dr. Gunter Malle
2. Gutachter: Prof. Dr. Jürgen Klüners
Datum der Disputation: 22.2.2012

D 386

Contents

1 Introduction

To every algebraic number field K a finite abelian group - the class group - can be associated. This group helps to describe the isomorphism classes of finitely generated modules over the ring of integers of K and if it is trivial one can multiply in these integers as in the rational integers. These are just two examples why class groups are interesting. But only few is known about the distribution of the class groups for a given sequence of number fields. The Cohen-Lenstra heuristic [C-L] is an about 30 years old conjecture which tries to describe those distributions. For a deterministic sequence of number fields it defines good primes (all but finitely many) and gives a probability distribution on the set of isomorphism classes of finite abelian groups of order just divisible by good primes such that the distribution of the good part (maximal subgroup of order just divisible by good primes) of the class groups of the fields of this sequence corresponds to the probability distribution. The idea behind this procedure is the following. The probability distribution on the groups should be most natural and a prime p should be good if there is no structural property which prevents the p-parts of the class groups to be distributed in the most natural random way. Only little parts of the Cohen-Lenstra heuristic are proven (see [D-H] or [F-K] for example), but one believes this heuristic to be correct, because being most natural is a good argument and because the numerical data suits very well to the heuristic.

For a number field K class field theory gives a number field K_1 - the Hilbert class field - such that K_1/K is a Galois extension with group isomorphic to the class group. The Galois group of the Hilbert class field K_2 of K_1 over K is isomorphic to an extension of the class group of K_1 by the class group of K. This group is called second class group of K and it is a finite meta abelian group.

The aim of this thesis is to do the same for the second class groups of real quadratic number fields as Cohen-Lenstra did for the class groups. Therefore the mathematical standard procedure: do some lemmas, give a theorem and then prove it, is replaced by: do some lemmas, give a conjecture and then some numerical data which fits to the conjecture.

The structure of the thesis is as follows: Chapter 2 recalls some basic facts about the part of mathematics which is needed here. Chapter 3 defines the good part of second class groups for real quadratic number fields and gives properties of these good parts which are necessary for concrete calculations. So far all statements are proven. But in chapter 4 this is not the case any more. Chapter 4.1 explains the Cohen-Lenstra heuristic and chapter 4.2 gives a conjecture about the distribution of the good parts of the second class groups of real quadratic number fields. Finally chapter 5 compares the prediction from 4.2 with the numerical data, describes how the data have been calculated and it contains information about a number field database program which has been made to present some of the numerical data of second class groups on the internet. This program can also be used to create and present other number field databases.

My own contributions are the definition of the good part of second class groups, the conjecture how second class groups of real quadratic number fields could be distributed, the calculation of second class groups for a lot of fields and a number field database program which allows to present different number field tables on the internet.

I thank Prof. Malle for his excellent guidance and useful advices and Prof. Eick and Johannes Lengler for helpful conversations. I am also thankful for the financial support of the Lotto-Stiftung Rheinland-Pfalz and the Stipendienstiftung der Universität Kaiserslautern.

2 Notations and Background

In this chapter very basic facts about algebra, which are used more than once in the following, are explained. Mainly this has notational purpose, and should give an impression, which part of mathematics is used. A lot of statements, which are on the same level as those mentioned here, are used without reference in the following.

2.1 Finite Groups

This chapter gives some notations related to a finite group G. The characteristic subgroup $G' := \langle g \cdot h \cdot g^{-1} \cdot h^{-1} \mid g, h \in G \rangle$ of G has the property that G/G' is abelian and that it is contained in every normal subgroup $N \leq G$ with G/N is abelian. It is called the **derived subgroup** of G. Another important characteristic subgroup is the **Frattini subgroup** $F(G)$ of G. It is defined as intersection of all maximal subgroups of G, and if G is a p-group, then $G/F(G)$ is elementary abelian and a set of elements of G forms a minimal system of generators of G, if and only if the set of their images in $G/F(G)$ is a basis over $\mathbb{F}_p$.

If G is abelian, then $\mathbb{D}_G$ **denotes** a group isomorphic to $C_2 \ltimes_{inv} G$, where the generator of C_2 acts by inversion on every element of G. G is identified as normal subgroup of $\mathbb{D}_G$. Every subgroup of G is therefore a normal subgroup of $\mathbb{D}_G$. If G is of odd order, then every proper normal subgroup of $\mathbb{D}_G$ is contained in G and all complements of G in $\mathbb{D}_G$ are conjugate.

The number of elements of a finite set S is denoted by $|S|$, and for a prime p the p-part of $|S|$ is denoted by $|S|_p$. For a finite abelian group A and a prime p, if nothing else is specified, the notion A_p denotes the p-Sylow subgroup of A, and for an integer n, one defines $A_{\neq n} := \bigoplus_{p \nmid n} A_p$ and $A_n := \bigoplus_{p \mid n} A_p$.

2.2 G-modules

This chapter recalls some basic facts for finite G-modules. They are either adaptations of more general theorems or modifications of theorems about modules over a finite dimensional algebra over a field, where the proofs carry over word for word.

Every ring which will appear here is associative with 1. For a commutative ring R and a group G the **group ring** RG is the free R-module on the elements of G, where the multiplication on RG is induced by the multiplication of G. A **G-module** A is a right module over the ring $\mathbb{Z}G$ (if it shall be a left module, then this is mentioned explicitly). A G-module can be defined by a homomorphism: $G \to \mathrm{Aut}(A)$, where A is an abelian group. In the following G **is always a finite group**, and A always a finitely generated G-module. The main objects of interest are finite G-modules and the G-modules are written **multiplicatively** here in general. Let A be a G-module. If A is finite, then it is also a module over $S^{-1}\mathbb{Z}G$, where $S^{-1}\mathbb{Z}$ is the localization of $\mathbb{Z}$ at all integers coprime to $|A|$ and if p is a prime and A a p-group of exponent e, then A is a $\mathbb{Z}/p^e\mathbb{Z}$-module, too. An **irreducible** G-module is a non trivial G-module with no non trivial proper submodules. The G-endomorphisms of such modules are described by the **lemma of Schur**:

Lemma 1. *Let A be an irreducible G-module. Then $\mathrm{End}_G(A)$ is a skew field.*

Proof. [Su] chapter 2.5 □

A non trivial G-module, which is not the direct sum of two of its non trivial submodules is called **indecomposable**. Since only finite G and A are used, the **theorem of Krull-Remak** holds (in general one needs much weaker finiteness conditions on A; see [Su] chapters 2.3, 2.4):

Lemma 2. *Let A be a finite G-module. Then A is the direct product of a finite number of indecomposable submodules. If $A = A_1 \oplus \cdots \oplus A_n = B_1 \oplus \cdots \oplus B_m$ with $A_i, B_j \leq A$ indecomposable, then $n = m$ and after a suitable reordering of the B_i one has $A_i \cong B_i$ as G-modules for all $i = 1, ..., n$.*

Proof. This is a consequence of [Su] theorem 2.4.8, because a finite G-module possesses a composition series. □

The symbol $\oplus$ is used as **notation** for internal direct sums with $=$ and for external direct sums with $\cong$. The **Fitting lemma** is the analogue to the lemma of Schur and describes the G-endomorphisms of indecomposable G-modules:

Lemma 3. *Let A be a finite and indecomposable G-module, and φ be a G-endomorphism of A. Then φ is bijective or nilpotent.*

Proof. [Be] lemma 1.4.4. □

Let R be a commutative ring, G a finite group and H a subgroup of G. A finitely generated RG-module A is called **relatively projective to** H, if whenever there are finitely generated RG-modules B, C, an RG-homomorphism $g : A \to C$, a surjective RG-homomorphism $f : B \to C$ and an RH-homomorphism $h : A \to B$ such that $f \circ h = g$, then there exists an RG-homomorphism $\hat{h} : A \to B$ with $f \circ \hat{h} = g$ ([Be] definition 3.6.1). The notion relatively projective means relatively projective to $H = \{1\}$. If A, B are RG-modules, then the map

$$Tr_H^G : \mathrm{Hom}_{RH}(A, B) \to \mathrm{Hom}_{RG}(A, B) : f \mapsto (x \mapsto \prod_{g \in L} (f(x^g))^{g^{-1}})$$

is called **trace map** ([Be] definition 3.6.2). L is a left transversal of H in G. Some criteria for an RG module to be relatively projective to H are given by the following lemmas:

Lemma 4. *Let G be a finite group, $H \leq G$ a subgroup, R a commutative ring and A a finitely generated RG module, which is relatively projective to H. Then the following hold:*

(a) If $I \leq \mathrm{Ann}_R(A)$ is an ideal of R, then the $(R/I)G$-module A is relatively projective to H, too.

(b) If A is projective as RH-module, then A is projective as RG-module.

Proof. This is obvious. □

Lemma 5. *([Be] proposition 3.6.4) Let G be a finite group, $H \leq G$ a subgroup, R a commutative ring and A a finitely generated RG module. Then the following are equivalent:*

(a) A is relatively projective to H.

(b) *If $i : A \to M$ is an RG-monomorphism into any RG-module M such that $i(A)$ has an RH-complement, then $i(A)$ has an RG-complement in M.*

(c) *There is an RH-endomorphism f of A such that $id_A = Tr_H^G(f)$.*

Proof. This is a selection of the statements of [Be] proposition 3.6.4. □

This lemma will be called **theorem of Maschke** here, because $(c \Rightarrow b)$ with $f = \frac{1}{(G:H)}$ results in the following corollary:

Corollary. *Let G be a finite group with subgroup H. Let A be a finite G-module such that $(G : H)$ and $|A|$ are coprime. If $A = B \oplus C$ as H-modules and if B is a G-module, then there exists a G-module D such that $A = B \oplus D$.*

Let A be a finitely generated G-module of a finite group G and

$$X = \cdots \xrightarrow{d_3} X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} X_{-1} \xrightarrow{d_{-1}} X_{-2} \xrightarrow{d_{-2}} \cdots$$

be an exact sequence of projective G-modules such that there is an injective G-homomorphism $\mu : \mathbb{Z} \to X_{-1}$ and a surjective G-homomorphism $\epsilon : X_0 \to \mathbb{Z}$ with $d_0 = \mu \circ \epsilon$ (here G acts trivially on the G-module $\mathbb{Z}$). The n-th cohomology group of the complex $\mathrm{Hom}_G(X, A)$ is called n-th **Tate cohomology** group of the G-module A and one writes $\hat{H}^n(G, A)$ for it $(n \in \mathbb{Z})$. They exist, are well defined and they are finite abelian groups, which are unique up to isomorphism (see [Ne1] for this definition and the immediate consequences). The Tate cohomology is comparable with the ordinary (co-)homology, know from homological algebra: $\hat{H}^n(G, A) \cong \mathrm{Ext}^n_{\mathbb{Z}G}(A, \mathbb{Z})$ for $n > 0$ and $\hat{H}^n(G, A) \cong \mathrm{Tor}^{-n-1}_{\mathbb{Z}G}(\mathbb{Z}, A)$ for the integers $n < -1$. The next lemma gives properties of the Tate cohomology groups, like the **inf-res-sequence**:

Lemma 6. *Let G be a finite group and A, B be finitely generated G-modules. Then the following hold:*

(a) *$\hat{H}^n(G, A \oplus B) \cong \hat{H}^n(G, A) \oplus \hat{H}^n(G, B)$ for all $n \in \mathbb{Z}$, in particular $\hat{H}^n(G, A) = \{1\}$, if $A = \{1\}$.*

(b) *$|G| \cdot \hat{H}^n(G, A) = \{1\}$ for all $n \in \mathbb{Z}$, in particular $\hat{H}^n(G, A) = \{1\}$, if A is finite and $|G|$ and $|A|$ are coprime.*

(c) *If N is a normal subgroup of G, n a positive integer and $\hat{H}^r(N, A) = \{1\}$ for all $r = 1, ..., n-1$, then there are homomorphisms of abelian groups* inf, res *such that the following sequence (the so called inf-res sequence) is exact:*

$$\{1\} \to \hat{H}^n(G/N, A^N) \xrightarrow{\mathrm{inf}} \hat{H}^n(G, A) \xrightarrow{\mathrm{res}} \hat{H}^n(N, A).$$

Proof. Statement (a), (b) and (c) are theorem 3.7, 3.16 and 4.7 from [Ne1] chapter 1. □

Let G be a finite group and A a finite G-module. An exact sequence of groups (and group homomorphisms) $\{1\} \to A \xrightarrow{f} H \xrightarrow{g} G \to \{1\}$ is called an **extension** of the G-module A by G, if the action of G on A induced by the conjugation of a transversal of G under g in H coincides with the G-module structure. In the literature the definition of an extension is a bit more general (see [Su] chapter 7). If the sequence splits, the extension is called **split**. In this case, H is isomorphic to the semidirect product $G \ltimes A$, where the action

comes from the module structure. Properties of extensions of abelian groups are related to the cohomology groups. In particular, on has the following lemma, which is a version of the **Schur-Zassenhaus theorem**:

Lemma 7. *Let G be a finite group, A a finite G-module and $\{1\} \to A \to H \to G \to \{1\}$ be an extension of A by G. Then the following hold:*

(a) If $\hat{H}^2(G, A) = \{1\}$, then the extension is split.

(b) If the extension is split and $\hat{H}^1(G, A) = \{1\}$, then all complements of A in H are conjugate.

Proof. Statement (a) is explained in [Su] chapter 2.7 and statement (b) is [Su] theorem 2.8.8. □

With the help of the standard resolution (see [Ne2] chapter 1.2), one can calculate the cohomology groups. The results are not very nice, but in low degrees or for cyclic G one gets easy formulas. Define $A^G := \{a \in A \mid a^g = a \, \forall g \in G\}$ to be the **submodule of A of all fixed points** and $I_G A := \left\{a^{g-1} \mid a \in A, g \in G\right\}$ the **augmentation submodule** of A (the notation a^{g-1} means $a^g \cdot a^{-1}$). For a finite cyclic group of order m, the notation C_m is used.

Lemma 8. *Let G be a finite group, A be a G-module and $n_G : A \to A : a \mapsto \prod_{g \in G} a^g$ be the norm map of G. Then $\hat{H}^0(G, A) \cong A^G / \mathrm{Im}(n_G)$ and $\hat{H}^{-1}(G, A) \cong \mathrm{Ker}(n_G)/I_G A$.*

Proof. [Ne1] chapter 1.2, page 25. □

Lemma 9. *Let A be a C_m-module and $\varphi \in \mathrm{Aut}(A)$ the action of a generator of C_m. Then*

$$\hat{H}^n(C_m, A) \cong \begin{cases} \mathrm{Ker}(\varphi - 1)/\mathrm{Im}(1 + \varphi + \cdots + \varphi^{m-1}), \, n \in \mathbb{Z} \, even \\ \mathrm{Ker}(1 + \varphi + \cdots + \varphi^{m-1})/\mathrm{Im}(\varphi - 1), \, n \in \mathbb{Z} \, odd. \end{cases}$$

If in addition A is finite, then $\hat{H}^0(C_m, A) \cong \hat{H}^{-1}(C_m, A)$.

Proof. [Ne1] chapter 1.6. □

In general it is difficult to construct direct summands of G-modules, therefore the following lemma which uses this description of $\hat{H}^{-1}$ and $\hat{H}^0$ is helpful. It is a special case of a decomposition induced by idempotents.

Lemma 10. *([Su] 2.5.17) Let A be a finite G-module over a finite group G and $N \leq G$ be a normal subgroup such that $|N|$ and $|A|$ are coprime. Then the following hold:*

(a) $A = A^N \oplus I_N A$ is a direct decomposition into G-modules.

(b) If $K \leq A$ is a G-submodule with $A = A^N \oplus K$, then $K = I_N A$.

(c) If $T \leq A$ is a G-submodule with $A = I_N A \oplus T$, then $T = A^N$.

(d) If $M \leq A$ is a G-submodule with $A = A^N \cdot M$, then $I_N A \subseteq M$.

(e) If $S \leq A$ is a G-submodule with $A = I_N A \cdot S$, then $A^N \subseteq S$.

Proof. Since $|A|$ and $|N|$ are coprime the normalized norm map of N

$$n_N : A \to A : a \mapsto \frac{1}{|N|} \sum_{g \in N} a^g$$

is an idempotent N-homomorphism and even G-homomorphism, because N is normal in G. Therefore one has the decomposition $A = \mathrm{Ker}(n_N) \oplus \mathrm{Im}(n_N)$ of G-modules. Because of lemma 8 and 6 (b) one can replace $\mathrm{Ker}(n_N)$ by $I_N A$ and $\mathrm{Im}(n_N)$ by A^N. This shows statement (a). The remaining parts are a consequence of the following obvious fact: If $B \leq A$ is a G-submodule, then $B^N \leq A^N$ and $I_N B \leq I_N A$. Hence $K^N \leq A^N \cap K = \{1\}$ and by (a) one has $K = I_N K \leq I_N A$. But $|I_N A| = |K|$ and (b) follows. Statement (c) is proven in the same way. The assumption $A = M \cdot A^N$ implies $A = A^N \cdot M^N \cdot I_N M$, hence $A = A^N \cdot I_N M$ and therefore $I_N A = I_N M \leq M$. This is a proof for (d), and (e) is proven analogously. □

Let G be a finite group. Two G-modules A, B are called **conjugate**, if and only if there is an automorphism $\phi \in \mathrm{Aut}(G)$ such that $B \cong {}^{\phi}A$ as G-module. The module ${}^{\phi}A$ has the same underlying group as A and $g \in G$ acts on ${}^{\phi}A$ by $a \mapsto a^{\phi^{-1}(g)}$. Some obvious properties of conjugate modules are listed in the following lemma:

Lemma 11. *Let G be a finite group, A and B be G-modules and $\phi \in \mathrm{Aut}(G)$. Then the following hold:*

(a) $A \cong B$ *if and only if* ${}^{\phi}A \cong {}^{\phi}B$

(b) ${}^{\phi}(A \oplus B) \cong {}^{\phi}A \oplus {}^{\phi}B$

(c) If N is the kernel of the action of G on A, then $\phi(N)$ is the kernel of its action on ${}^{\phi}A$.

(d) A is irreducible (respectively indecomposable, resp. faithful), if and only if ${}^{\phi}A$ *is irreducible (resp. indecomposable, resp. faithful).*

(e) If $\phi \in \mathrm{Inn}(G)$, then ${}^{\phi}A \cong A$.

(f) $\mathrm{Out}(G)$ *acts from the left on the set of isomorphism classes of G-modules by* $\overline{\psi}.A := {}^{\psi}A$ *for any representative ψ.*

(g) Conjugacy of G-modules is an equivalence relation and the equivalence classes regarding conjugacy are the orbits of the action from (f).

Proof. If ϕ is the left conjugation with some $h \in G$, then the map $A \to {}^{\phi}A : a \mapsto a^h$ is an isomorphism of G-modules. This shows (e). The other statements are obvious. □

For a set S of isomorphism classes of G-modules, which the theorem of Krull-Remak holds for and which is closed under direct sums, indecomposable direct summands and conjugacy, one can build the **representation module**. It is an $\mathrm{Out}(G)$-module, where the group is the free $\mathbb{Z}$-module over all isomorphism classes of indecomposable G-modules from this set S and the action is described in lemma 11. To express the representation module in terms of the representation modules of faithful modules, the following notation is needed:

Let G be a finite group. Two normal subgroups N, M are called **Kronecker equivalent**, if and only if there is an automorphism $\phi \in \mathrm{Out}(G)$ such that $\phi(N) = M$. Define

$U_N := \{\phi \in \mathrm{Out}(G) \mid \phi(N) = N\}$. The group U_N is the stabilizer of N and the Kronecker equivalence class is the orbit of N under the action of $\mathrm{Out}(G)$ on the set of normal subgroups of G. So Kronecker equivalence is an equivalence relation on the normal subgroups of G, the size of the class of N is $(\mathrm{Out}(G) : U_N)$ and U_N is a subgroup of $\mathrm{Out}(G)$.

Lemma 12. *Let G be a finite group and S be a set of isomorphism classes of finite G-modules, which is closed under direct sums, indecomposable direct summands and conjugacy. Let R be the representation module corresponding to S and let for a normal subgroup $N \leq G$ the group R_N be the free $\mathbb{Z}$-module over all classes of indecomposable modules A from S such that the kernel of the action of G on A equals N and let $U_N := \{\phi \in \mathrm{Out}(G) \mid \phi(N) = N\}$. Then the following is true:*

(a) For any normal subgroup $N \leq G$, the group R_N is a U_N-submodule of R.

(b) $R \cong \bigoplus_{N \in L} R_N \uparrow_{U_N}^{\mathrm{Out}(G)}$ as $\mathrm{Out}(G)$-module, where L is any system of representatives for Kronecker equivalence.

Proof. As sum of abelian groups one has $R = \bigoplus_{N \trianglelefteq G} R_N$. If $\phi \in \mathrm{Out}(G)$, then one has $R_{\phi(N)} = \phi(R_N)$ by lemma 11. This shows (a). If $\tilde{R}_N$ is the direct sum of all R_M, where M runs through the Kronecker equivalence class of N, then $\tilde{R}_N$ is an $\mathrm{Out}(G)$-module and $R = \bigoplus_{N \in L} \tilde{R}_N$ as $\mathrm{Out}(G)$-modules, where L is a system of representatives for Kronecker equivalence. Let N be any element of L and let $\phi_1, ..., \phi_r$ be a left transversal of U_N in $\mathrm{Out}(G)$. Then the Kronecker equivalence class $[N]$ of N equals $[N] = \{\phi_1(N), ..., \phi_r(N)\}$. If $\{A_\lambda \mid \lambda \in \Lambda\}$ is the set of isomorphism classes of indecomposable G-modules with kernel N, then $\left\{ {}^{\phi_i}A_\lambda \mid \lambda \in \Lambda \right\}$ is the set of indecomposable G-modules with kernel $\phi_i(N)$. Hence

$$\tilde{R}_N = \bigoplus_{i=1}^{r} \bigoplus_{\lambda \in \Lambda} \mathbb{Z}({}^{\phi_i}A_\lambda),$$

where $\mathrm{Out}(G)$ acts by left multiplication. This shows $\tilde{R}_N \cong R_N \uparrow_{U_N}^{\mathrm{Out}(G)}$ by definition of induced action. □

Here the following **convention** is used: If an abelian normal subgroup N of a group G is viewed as G-module or G/N-module without further information about the module structure, then this module structure is always one of these which are induced by conjugation on the right.

2.3 Algebraic Number Theory and Class Field Theory

Most of the following statements can be found in the first three chapters of [Ne2].

A **number field** K is a finite field extension of $\mathbb{Q}$. In the following an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ is fixed and all number fields are considered to be subfields of $\overline{\mathbb{Q}}$. An embedding of K is one of the $(K : \mathbb{Q})$ different injective homomorphisms of fields from K to $\mathbb{C}$ and it is called real, if its image is contained in $\mathbb{R}$. A number field is called totally real, if all of its embeddings are real. Fields of the type $\mathbb{Q}(\sqrt{d})$, where the positive integer d is not a square are called **real quadratic number fields** for example. The elements of K, which are integral over $\mathbb{Z}$ form a Dedekind domain, called $\mathcal{O}_K$. The ring $\mathcal{O}_K$ and all of its ideals $A \neq 0$ are free $\mathbb{Z}$-modules of rank $(K : \mathbb{Q})$. The fractional ideals of $\mathcal{O}_K$ form an abelian

group I_K, which contains the subgroup H_K of principal fractional ideals. The quotient of these groups $\mathrm{Cl}(K)$, which is a finite abelian group, is called **class group** and its order h_K is called class number of K.

If L is another number field containing K, one can define transfer mappings from structures belonging to K to structures belonging to L and norm mappings in the other direction. For example one calls the group homomorphism $j : I_K \to I_L : A \mapsto A \cdot \mathcal{O}_L$ transfer and the group homomorphism $N_{L/K} : I_L \to I_K$, which is defined by mapping a prime ideal $Q \neq 0$ to $(Q \cap \mathcal{O}_K)^{(\mathcal{O}_L/Q:\mathcal{O}_K/(\mathcal{O}_K \cap Q))}$, is called norm. Since principal ideals are mapped to principal ideals and p-groups to p-groups, these homomorphisms induce for every prime p group homomorphisms $N : \mathrm{Cl}_p(L) \to \mathrm{Cl}_p(K)$ and $j : \mathrm{Cl}_p(K) \to \mathrm{Cl}_p(L)$. The extension L/K of number fields is called **unramified** if and only if every embedding of L, which coincides under restriction to K with a real embedding of K is real and if every prime ideal $P \neq 0$ of $\mathcal{O}_K$ is unramified in the extension L/K. A prime ideal P of K is called ramified in the extension L/K, if and only if there is a prime ideal Q of $\mathcal{O}_L$ such that $P \subseteq Q^2$.

If L/K is an extension of number fields, then the trace $T : L \times L \to K : (x, y) \mapsto \mathrm{Tr}(x \cdot y)$ defines a non degenerate bilinear map. The ideal generated by the determinants of the Gram-matrices of any K-basis of L from $\mathcal{O}_L$ is called **discriminant** $d_{L/K}$ of L/K. If $K = \mathbb{Q}$, then the determinant of the Gram-matrix of a $\mathbb{Z}$-basis of $\mathcal{O}_L$ is called absolute discriminant d_L (this basis exists; see before). The prime ideals of $\mathcal{O}_K$, which ramify in the extension L/K are exactly the prime divisors of $d_{L/K}$.

For a number field K one defines the **Dedekind zeta function** by

$$\zeta_K : \{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\} \to \mathbb{C} : s \mapsto \sum_I \frac{1}{N(I)^s},$$

where N is the absolute norm and I runs through all non zero integral ideals of $\mathcal{O}_K$. It is a holomorphic function and for s with $\mathrm{Re}(s) > 1$ one has the Euler product

$$\zeta_K(s) = \prod_p \frac{1}{1 - N(p)^{-s}},$$

where p runs through all prime ideals of $\mathcal{O}_K$ ([Ne2] chapter VII.5).

If K is a number field, then a number field $K_1 \leq \overline{\mathbb{Q}}$, which is unramified and abelian over K and contains all other subfields of $\overline{\mathbb{Q}}$ with these properties, is called the **Hilbert class field** of K. The following lemma is an important result from class field theory:

Lemma 13. *Let K be a number field. Then the Hilbert class field K_1 of K exists and* $\mathrm{Gal}(K_1/K) \cong \mathrm{Cl}(K)$.

Proof. [Ne2] Satz VI.6.9. □

The Hilbert class field K_2 of the Hilbert class field of a number field K is called the **second Hilbert class field**. It is a finite meta abelian extension of K and if K/F is a Galois extension of number fields, then K_i/F is Galois for $i \in \{1, 2\}$. For a Galois extension L/K of number fields, the maximal unramified extension M of L such that M/L is Galois and $\mathrm{Gal}(M/L)$ is contained in the center of $\mathrm{Gal}(M/K)$ is called **central class field** of L over

K. The central class field is well defined, it is an intermediate field between L and L_1 and if $K = L$, then $M = K_1$.

If L/K is a Galois extension of number fields, the Galois group $\mathrm{Gal}(L/K)$ acts naturally on $\mathrm{Cl}_p(L)$ for all primes p. Since $\mathrm{Cl}_p(L)$ is abelian it becomes a $\mathrm{Gal}(L/K)$-module. The action is defined as follows: Let c be an ideal class in $\mathrm{Cl}_p(L)$ and $A \trianglelefteq \mathcal{O}_L$ a representative. $\mathrm{Gal}(L/K)$ may be identified with a subgroup of $\mathrm{Aut}(L)$, so set c^σ to be the class of $\sigma(A)$ for each $\sigma \in \mathrm{Gal}(L/K)$. This is well defined since σ maps (principal) ideals to (principal) ideals and endomorphisms of finite abelian groups decompose to all prime parts. One can choose an identification $\mathrm{Gal}(L_1/L) \cong \mathrm{Cl}(L)$ according to lemma 13 such that this action corresponds to the conjugation from the left in $\mathrm{Gal}(L_1/K)$ (see [Ne1] chapter 2 theorem 1.11).

For a number field K the **notation** $\hat{K}$ is used for the Galois closure of K over $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}$.

3 The Group $\mathrm{Gal}(K_2/\mathbb{Q})$

This chapter describes properties of the group $\mathrm{Gal}(K_2/\mathbb{Q})$, where K is a quadratic number field and K_2 is the second Hilbert class field of K that is the Hilbert class field of the Hilbert class field of K. But not this general situation is of main interest here, but only a special situation. Instead of the number field tower $\mathbb{Q} \subseteq K \subseteq K_1 \subseteq K_2$, one considers the tower $\mathbb{Q} \subseteq K \subseteq K_{1,f} \subseteq K_{2,f}$. The fields $K_{1,f}$ and $K_{2,f}$ are called first and second non central coprime Hilbert class field of K in the following and they are Galois extensions of $\mathbb{Q}$, which are unramified over K. These class fields are just chosen in a way such that consecutive steps in the class field tower have coprime degrees, and that the non coprime part does not occur later. For the definition see chapter 3.5. The group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ coincides with $\mathrm{Gal}(K_2/\mathbb{Q})$, if $\mathrm{Cl}(K)$ is cyclic of odd prime power degree, and it is a proper factor group of it, if $\mathrm{Cl}(K)$ is of even order or non cyclic (see chapter 3.5).

The philosophy of Cohen-Lenstra distinguishes between good and bad primes (see chapter 4), and these factor groups shall be a generalization of the good part of class groups to the second class groups of real quadratic number fields. Not everything what is known about the group $\mathrm{Gal}(K_2/\mathbb{Q})$ in the bad case is given here. See for example [No] or [BP]. The group theoretic statements given in this chapter also hold true for imaginary quadratic number fields, but one gets additional problems, when trying to describe the distribution of their second class groups (see chapter 4).

This chapter has two aims. At first it gives information how to calculate the group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ for concrete real quadratic number fields. This is done by the propositions 2 and 8 and prepared by chapter 3.1. Second it gives information about the structure of the group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$. This is done by pure group theoretic argumentation in the chapters 3.3 and 3.4 and summarized by proposition 7 in terms of number fields.

The group $\mathrm{Gal}(K_{2,f}/K_{1,f})$ is a finite $G := \mathbb{D}_{\mathrm{Gal}(K_{1,f}/K)}$-module, which behaves as if $|G|$ and $|\mathrm{Gal}(K_{2,f}/K_{1,f})|$ would be coprime and the group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ is the corresponding semidirect product (see proposition 7). It does not matter if one studies the group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ or the group $\mathrm{Gal}(K_{2,f}/K)$ because they uniquely determine each other (see proposition 7).

3.1 Class Group Relations

Calculating class groups of polynomials of high degree is a difficult task for a computer and waiting for the result is a difficult task for a human. The following formulas may be used to reduce these calculations to fields of smaller degree and they are also useful for the description of the group $\mathrm{Gal}(K_2/\mathbb{Q})$. There are a lot of very similar formulas in the literature (see [Lem1] chapter 1, [Lem2] chapter 5, [Ho], [C-M] chapter 7 or [C-R1] for example). In this chapter, a class group relation for a Galois extension L/K of number fields is a formula, which expresses a connection between the p class groups of the intermediate fields of L/K for all primes $p \nmid (L:K)$. That means, in the following just the "coprime case" is considered (with some exceptions). In this case class group relations correspond to certain relations of fixed points (see lemma 1). The class number formula of Brauer [Br] gives a connection between the vanishing of products of class numbers of intermediate fields of L/K times some factors depending on their units on one hand and sums of the characters of $\mathrm{Gal}(L/K)$, which are induced by the principal characters of $\mathrm{Gal}(L/M)$, where M runs through the intermediate fields of L/K, on the other hand. In the coprime case the unit

factors disappear and Brauers formulas demonstrate the reduction to the orders in a class group relation (see [Wa]). All formulas given in this chapter correspond to relations on the induced principal characters and Honda mentions this connection for his formula in [Ho].

The following Lemma gives a link between the modules of fixed points and the class groups. It is Lemma 3 in [C-R1] and explains the name "class group relation" for the following relations on fixed points, but other versions which concentrate on the group $\mathrm{Gal}(K_2/\mathbb{Q})$ and which include some not coprime cases will be given later.

Lemma 1. *([C-R1]) Let L/K be a Galois extension of number fields with group G of order n, p a prime not dividing n and $j : \mathrm{Cl}_p(K) \to \mathrm{Cl}_p(L)$ the transfer of ideal classes. Then j is injective and $\mathrm{Im}(j) = \mathrm{Cl}_p(L)^G$, where $G \leq \mathrm{Aut}(\mathcal{O}_L)$ acts in the natural way on $\mathrm{Cl}_p(L)$.*

Proof. (see [Lem1] chapter 1) If $N : \mathrm{Cl}_p(L) \to \mathrm{Cl}_p(K)$ is the norm and I is a representative of an ideal class of $\mathrm{Cl}_p(K)$ then $(N \circ j)(I) = I^n$, hence $N \circ j$ is an isomorphism by the assumption on p, j is injective and N is surjective. Therefore $\mathrm{Im}(j) = \mathrm{Im}(j \circ N)$. But $j \circ N = \sum_{g \in G} g \in \mathrm{End}(\mathrm{Cl}_p(L))$ and $\mathrm{Im}(\sum_{g \in G} g) = \mathrm{Cl}_p(L)^G$ by lemma 2.8, because $\hat{H}^0(G, \mathrm{Cl}_p(L)) = \{1\}$ by the assumption on p. □

Lemma 2. *([Wa] theorem 1.2) Let G be a finite group, A a finite G-module of order coprime to $|G|$ and let $a_U \in \mathbb{Z}$ such that there is a relation $\sum_{U \leq G} a_U \cdot 1_U^G = 0$ on the induced principal characters. Then:*

$$\bigoplus_{U \leq G} (A^U)^{a_U} \cong \{1\}\,.$$

Remark: This statement is well defined because of the theorem of Krull-Remak. Walter [Wa] shows a more general statement. His proof reduces the problem to the following fact from integral representation theory: If G is a finite group and M and N are $\mathbb{Z}G$-modules which are finitely generated and free $\mathbb{Z}$-modules such that $\mathbb{Q} \otimes_{\mathbb{Z}} N \cong \mathbb{Q} \otimes_{\mathbb{Z}} M$ as $\mathbb{Q}G$-modules, then $R \otimes_{\mathbb{Z}} N \cong R \otimes_{\mathbb{Z}} M$ as RG-modules, where $\mathbb{Z} \leq R \leq \mathbb{Q}$ is a ring, which contains $|G|^{-1}$. In the special case here, this reduction is just the Frobenius reciprocity: for a finite G-module A and non negative integers a_U for every subgroup $U \leq G$ one has:

$$\bigoplus_{U \leq G} (A^U)^{a_U} \cong \bigoplus_{U \leq G} (\mathrm{Hom}_U(\mathbb{Z}, A))^{a_U} \cong \bigoplus_{U \leq G} (\mathrm{Hom}_G(\mathbb{Z} \uparrow_U^G, A))^{a_U} \cong \mathrm{Hom}_G(\bigoplus_{U \leq G} (\mathbb{Z} \uparrow_U^G)^{a_U}, A).$$

Lemma 3. *Let A be a $\mathbb{D}_G$-module, where A and G are finite abelian groups of coprime order. Then there is a decomposition*

$$A = \bigoplus_{N \leq G} A_N$$

of $\mathbb{D}_G$-modules such that N acts trivial on A_N and every element of $G \setminus N$ acts fixed point freely on A_N. The A_N are unique up to isomorphism and have the properties:

(a) $A^M = \bigoplus_{M \leq N \leq G} A_N$ for every subgroup M of G.

(b) $A_N = \{1\}$, if G/N is not cyclic.

(c) *If $G/N \neq \{1\}$ is cyclic of prime power order and M is the minimal subgroup in G/N, then $A_N \cong A^N/A^M$ and $A^N \cong A^N/A^M \oplus A^M$.*

(d) *$A_G = A^G$.*

Proof. Since for every $g \in G$ the subgroup $\langle g \rangle$ is a normal subgroup of $\mathbb{D}_G$, the decomposition $A = I_{\langle g \rangle} A \oplus A^{\langle g \rangle}$ of lemma 2.10 is a decomposition of $\mathbb{D}_G$-modules. Let $A = A_1 \oplus \cdots \oplus A_r$ be the decomposition of A into indecomposable $\mathbb{D}_G$-modules. Then each $g \in G$ acts trivially or fixed point freely on each of these summands. The set of all elements of G which act trivially on a fixed indecomposable A_i form a subgroup N_i of G. Now set A_N to be the sum of all indecomposable A_i where $N_i = N$. Then A_N is unique up to isomorphism by the theorem of Krull-Remak. For a subgroup M of G one has $A^M = \bigoplus_{N \leq G} (A_N)^M$. If $M \subseteq N$, then every element of A_N is fixed by every element of M and $(A_N)^M = A_N$ follows. In the other case there is an $m \in M \setminus N$, which acts fixed point freely on A_N and $(A_N)^M = \{1\}$. Hence it suffices to consider the subgroups containing M: $A^M = \bigoplus_{M \leq N \leq G} A_N$. This shows property (a) which implies also the properties (d) and (c), because cyclic p-groups have unique minimal subgroups. If $B \neq \{1\}$ is an irreducible G/N-submodule of A_N, then B and A_N are faithful modules of the finite abelian group G/N, because every element of $G \setminus N$ acts fixed point freely on A_N and therefore it can not fix a subgroup B of A_N. By the lemma of Schur G/N is isomorphic to a finite abelian subgroup of the unit group of a skew-field and hence cyclic (see [Su] 2.5.21), so the property (b) follows. □

Remark: This lemma is a generalization of [Su] 2.5.23 and [C-R1] proposition 4 and the proof is similar to the one in [C-R1]. The lemma is used for reductions to the cyclic case, and for most of the questions in the following, such a decomposition is fine enough (one does often not need indecomposables). The conclusion of the lemma holds true if one replaces $\mathbb{D}_G$ by a finite group H such that $G \leq H$ and every subgroup of G is a normal subgroup of H, for example $H = G$ or $G = Z(H)$.

Lemma 4. *Let A be a C_p^n-module such that $|A| < \infty$, p a prime and $p \nmid |A|$. Let $U_1, U_2, ..., U_m$ with $m = \frac{p^n - 1}{p-1}$ be the subgroups of C_p^n of index p.*
Then $(A^{C_p^n})^{m-1} \oplus A \cong A^{U_1} \oplus ... \oplus A^{U_m}$ as C_p^n-modules.

Proof. By lemma 3 there are isomorphisms of C_p^n-modules

$$A \cong A^{U_1}/A^{C_p^n} \oplus \cdots \oplus A^{U_m}/A^{C_p^n} \oplus \ A^{C_p^n}$$

and $A^{U_i}/A^{C_p^n} \oplus A^{C_p^n} \cong A^{U_i}$ for every $i \in \{1, ..., m\}$. The group $A^{C_p^n}$ can be added $m-1$ times on both sides and one gets the lemma. □

Lemma 5. *Let G be a finite abelian group of odd order and A be a $\mathbb{D}_G$-module such that $|A| < \infty$ and $|G|$ and $|A|$ are coprime. Let $\varphi \in \mathbb{D}_G$ be an arbitrary involution.*
Then $A^{\mathbb{D}_G} \oplus A^{\mathbb{D}_G} \oplus A \cong A^{\langle \varphi \rangle} \oplus A^{\langle \varphi \rangle} \oplus A^G$ as groups.

Proof. Case 1: (see [Ho] theorem 4) $G = \langle \sigma \rangle$ is cyclic: Because $|A|$ and $|G|$ are coprime lemma 2.10 shows that there is a decomposition $A = A^G \oplus I_G A$ of $\mathbb{D}_G$-modules. So assume $A = I_G A$ and $A^G = \{1\}$ (the case $A = A^G$ is obvious). This gives the possibility to identify $\mathbb{D}_G$ with a subgroup of $\mathrm{Aut}(A)$ (if A is not faithful, there is no problem). Since G

is cyclic, $A^G = \{1\}$ and A is abelian, the endomorphism $\sigma - 1 \in \mathrm{End}(A)$ is bijective and a calculation shows that $1 - \varphi$ and $\varphi + 1$ are conjugate as elements of $\mathrm{End}(A)$:

$$\varphi \ - \ 1 \ = \ - \ (\varphi \ + \ 1)^{\sigma^{\frac{n-1}{2}}(\sigma-1)},$$

where $n = |G|$. Hence $\mathrm{Ker}(\varphi - 1) \cong \mathrm{Ker}(\varphi + 1)$. For $\tau \in G$ one has $A^{\langle\varphi^\tau\rangle} = (A^{\langle\varphi\rangle})^\tau$ and φ and $\varphi \cdot \tau$ are conjugate in $\mathbb{D}_G$. Therefore

$$A^{\langle\varphi\rangle} \cap A^{\langle\varphi\sigma\rangle} = A^{\mathbb{D}_G} \leq A^G = \{1\}$$

so

$$|A| \geq |A^{\langle\varphi\rangle}| \cdot |A^{\langle\varphi\sigma\rangle}| = |A^{\langle\varphi\rangle}|^2.$$

On the other hand

$$|A| = |\mathrm{Ker}(\varphi - 1)| \cdot |\mathrm{Im}(\varphi - 1)| \leq |\mathrm{Ker}(\varphi - 1)| \cdot |\mathrm{Ker}(\varphi + 1)| = |\mathrm{Ker}(\varphi - 1)|^2 = |A^{\langle\varphi\rangle}|^2.$$

So $A = A^{\langle\varphi\rangle} \oplus A^{\langle\varphi\cdot\sigma\rangle} \cong A^{\langle\varphi\rangle} \oplus A^{\langle\varphi\rangle}$ as groups.
Case 2: Reduction to the cyclic case: By lemma 3 the $\mathbb{D}_G$-module A has a decomposition of $\mathbb{D}_G$-modules such that $\mathbb{D}_G$ acts as dihedral group on every summand. Since taking fixed points commutes with direct sums, the general case reduces to the cyclic case. □

Remark: If G is cyclic the condition $|G|$ coprime to $|A|$ of the lemma can be replaced by $A \ \cong \ A^G \ \oplus \ I_G A$.

Lemma 6. *Let G be a finite abelian group of odd order and $\varphi \in \mathbb{D}_G$ be an involution. Let 1_U^H denote the induced principal $\mathbb{C}$-character of a subgroup $U \leq H$ in a group H.*
Then

$$1_{\{1\}}^{\mathbb{D}_G} + 2 \cdot 1_{\mathbb{D}_G}^{\mathbb{D}_G} = 2 \cdot 1_{\langle\varphi\rangle}^{\mathbb{D}_G} + 1_G^{\mathbb{D}_G}.$$

Proof. Let $1, a_1, \ldots, a_{\frac{|G|-1}{2}}$ denote representatives of the conjugacy classes of $\mathbb{D}_G$ contained in G. Use the definition $1_U^H(x) \ = \ \frac{1}{|U|} \cdot |\left\{g \in H \mid g^{-1}xg \in U\right\}|$ for all $x \in H$ to calculate the following table of character values:

	1	φ	a_1	...	$a_{\frac{\lvert G\rvert-1}{2}}$
$1_{\{1\}}^{\mathbb{D}_G}$	$2 \cdot \lvert G\rvert$	0	0	...	0
$1_{\mathbb{D}_G}^{\mathbb{D}_G}$	1	1	1	...	1
$1_{\langle\varphi\rangle}^{\mathbb{D}_G}$	$\lvert G\rvert$	1	0	...	0
$1_G^{\mathbb{D}_G}$	2	0	2	...	2

The formula follows by inspection. □

Lemma 7. *Let G be a finite abelian group with n subgroups. Denote a basis of $\mathbb{Q}^n$ by $(e_M)_M$, where M ranges over the subgroups of G. Let f denote the linear map of $\mathbb{Q}^n$, which is represented by the matrix $((G : M) \cdot \chi_{\{N \subseteq M\}} \cdot \chi_{\{N \, cyclic\}})_{N,M}$ in this basis and define $K := \mathrm{Ker}(f)$. Here χ is the characteristic function. Then the following is true:*

(a) If $(a_M)_{M \leq G} \in \mathbb{Q}^n$, then $\sum_{M \leq G} a_M \cdot 1_M^G = 0$ if and only if $(a_M) \in K$.

(b) Let $H_1, ..., H_r$ be the subgroups of G for which G/H_i is not cyclic and let $V_1, ..., V_r$ be any subgroups of G such that there are primes p_i with $V_i/H_i \cong C_{p_i} \times C_{p_i}$. Let $M_{i,1}, ..., M_{i,p_i+1}$ be the subgroups of G between H_i and V_i. Define the vectors $v^1, ..., v^r \in \mathbb{Q}^n$ by $v^i_{V_i} = -p_i$, $v^i_{H_i} = -1$, $v^i_{M_{i,j}} = 1$ for all $j = 1, ..., p_i + 1$ and $v^i_M = 0$ for all other subgroups $M \leq G$. Then $v^1, ..., v^r$ is a basis of K.

(c) If G is not cyclic, then K contains an element $(a_M)_M$ with $a_{\{1\}} \neq 0$ and $a_N = 0$ for all $\{1\} \neq N \leq G$ with G/N not cyclic.

Proof. Since G is abelian $1^G_M(x) = \frac{1}{|M|} \cdot |\{g \in G \mid x^g \in M\}| = (G : M) \cdot \chi_{\{x \in M\}}$ for all $x \in G$, where χ is the characteristic function. So for $(a_M)_{M \leq G} \in \mathbb{Q}^n$ one has the equivalence: $\sum_{M \leq G} a_M \cdot 1^G_M = 0$ if and only if $\sum_{M \leq G} a_M \cdot (G : M) \cdot \chi_{\{x \in M\}} = 0$ for all $x \in G$, if and only if $(a_M)_M \in K$. This implies (a). Let $M_1, ..., M_n$ be the subgroups of G and let these groups and $H_1, ..., H_r$ be ordered in a way that $i < j$ implies $H_j \not\subseteq H_i$ and $M_j \not\subseteq M_i$, then the matrix representation of f in the basis $(e_{M_i})_i$ is an upper triangular matrix with $n - r$ non zero entries on the diagonal. Hence $\dim_{\mathbb{Q}}(K) \leq r$. Because $v^i_{H_i} \neq 0$ and $v^i_{H_j} = 0$ for all $j < i$ the vectors $v^1, ..., v^r$ are linear independent. If a cyclic subgroup $N \leq G$ is contained in V_i but not in H_i, then there is exactly one j such that $N \leq M_{i,j}$. Therefore for a cyclic subgroup $N \leq G$ the sum $\sum_{M \leq G} v^i_M \cdot (G : M) \cdot \chi_{\{N \leq M\}}$ can take the three values 0, if $N \not\subseteq V_i$,

$$(G : V_i) \cdot (-(V_i : H_i) + (p_i + 1)(V_i : M_{i,1}) - p_i) = (G : V_i) \cdot (-p_i^2 + (p_i + 1)p_i - p_i) = 0$$

if N is contained in H_i or $(G : V_i) \cdot ((V_i : M_{i,1}) - p_i) = 0$. This shows that $v^i \in K$ and implies statement (b). The vectors $v^2, ..., v^r$ can be used to cancel out every component of v^1 corresponding to a subgroup H different from $H_1 = \{1\}$ with G/H not cyclic. This shows (c). □

Remark: This lemma gives the well known description of the relations on the induced principal characters for an abelian group G. By duality of abelian groups (see [Bae]) one can calculate that the kernel of the linear map of $\mathbb{Q}^n$ which is described by the matrix $(\chi_{\{M \subseteq N\}} \cdot \chi_{\{G/N \, cyclic\}})_{N \leq G, M \leq G}$ also equals K. Together with lemma 3 this gives a proof of lemma 2 in the case of abelian G.

Corollary. *Let L/K be an abelian extension of degree n of number fields and p be a prime not dividing n. Then there is always a class group relation which reduces the calculation of $\mathrm{Cl}_p(L)$ to the calculation of $\mathrm{Cl}_p(M)$ for all the number fields M with $K \leq M \leq L$ and cyclic Galois group $\mathrm{Gal}(M/K)$.*

Proof. Let $G := \mathrm{Gal}(L/K)$ and let $U_1, ..., U_r$ be the subgroups of G such that G/U_i is cyclic. If G is cyclic the statement is empty, so assume G to be non cyclic, therefore $U_i \neq \{1\}$ for all i. By lemma 7 c there are $a, a_1, ..., a_r \in \mathbb{Q}$ such that $a \cdot 1^G_{\{1\}} = \sum_i a_i \cdot 1^G_{U_i}$ with $a \neq 0$. By taking the common denominator one may assume $a, a_1, ..., a_r$ to be integers. Lemma 2 shows that

$$\mathrm{Cl}_p(L)^a \cong \bigoplus_i (\mathrm{Cl}_p(L)^{U_i})^{a_i}.$$

Because of lemma 1, one has $\mathrm{Cl}_p(L)^{U_i} \cong \mathrm{Cl}_p(L^{U_i})$. Since $a \neq 0$, this implies the corollary. □

3.2 The Group $\mathrm{Gal}(K_1/\mathbb{Q})$

This chapter summarizes well known facts about the Galois group $\mathrm{Gal}(K_1/\mathbb{Q})$ of the Hilbert class field K_1 of a real quadratic field K.

Proposition 1. *Let K_1 be the Hilbert class field of a quadratic number field K. Then $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathbb{D}_{\mathrm{Cl}(K)}$.*

Proof. By definition K_1 is the maximal unramified and abelian field extension of K, so each conjugate of K_1 over $\mathbb{Q}$ is also an abelian and unramified extension of K, hence contained in K_1 and so $K_1/\mathbb{Q}$ is Galois. By a theorem of Minkowski (see [Ne1] chapter III) $\mathbb{Q}$ has no extension which is unramified at all finite primes, hence $\mathbb{Q}$ must coincide with its extension L which is unramified at all finite primes and maximal in K_1 with respect to this property. By Hilberts ramification theory (see [Ne1] chapter I) $\mathrm{Gal}(K_1/\mathbb{Q}) = \mathrm{Gal}(K_1/L)$ is generated by the inertia subgroups of the finite primes in $K_1/\mathbb{Q}$. But these groups have order 2 at most and can not be contained in $\mathrm{Gal}(K_1/K)$ since K_1/K is unramified. Furthermore $\mathrm{Gal}(K_1/K) \cong \mathrm{Cl}(K)$ by class field theory. So $\mathrm{Gal}(K_1/\mathbb{Q}) \cong C_2 \ltimes \mathrm{Cl}(K)$ and is generated by involutions outside $\mathrm{Cl}(K)$. If φ is the generator of a complement of $\mathrm{Cl}(K)$ and if $\{\varphi \cdot x_i\}$ with $x_i \in \mathrm{Cl}(K)$ are these involutions, then $1 = \varphi x_i \cdot \varphi x_i = x_i^{\varphi} \cdot x_i$. Every element of $\mathrm{Gal}(K_1/\mathbb{Q})$ is of the form $\prod_i y_i$ or $\varphi \cdot \prod_i y_i$ where $y_i \in \left\{x_i, x_i^{-1}\right\}$ satisfies $y_i^{\varphi} = y_i^{-1}$. Hence φ inverts every element of $\mathrm{Cl}(K)$ and $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathbb{D}_{\mathrm{Cl}(K)}$. □

Corollary 1. *The group $\mathrm{Gal}(K_1/\mathbb{Q})$ is uniquely determined by the group $\mathrm{Gal}(K_1/K)$.*

Corollary 2. *If K is a quadratic number field with odd class number, then $\mathrm{Gal}(K_1/\mathbb{Q})' = \mathrm{Gal}(K_1/K)$.*

Remark: If K is a quadratic number field and L/K an unramified extension of number fields with $L/\mathbb{Q}$ Galois, then the same argumentation as in the proof of the Lemma shows $\mathrm{Gal}(L/\mathbb{Q}) \cong C_2 \ltimes \mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/\mathbb{Q})$ is generated by involutions outside $\mathrm{Gal}(L/K)$.

Since Hasse [Ha] a lot of authors (like Kondo [Ko] for example) proved theorems of the following type: If G is a finite group, U a fixed subgroup of G, N a fixed normal subgroup of G and L a number field with Galois closure $\hat{L}$ such that $\mathrm{Gal}(\hat{L}/\mathbb{Q}) \cong G$ and $\hat{L}^U = L$. Then $\hat{L}/\hat{L}^N$ is unramified if and only if d_L is minimal in a certain sense depending on G, N and U.

The following proposition is such a theorem for the group $\mathbb{D}_G$ and for the proof this lemma about Artin representation is needed:

Lemma 8. *([Se]) Let L/K be a Galois extension of totally real number fields with group $G := \mathrm{Gal}(L/K)$. Let $\sum_{U \leq G} a_U 1_U^G = 0$ with $a_U \in \mathbb{Z}$ be a relation on the induced principal characters. Then $\prod_{U \leq G} (\bar{d}_{L^U})^{a_U} = 1$.*

Proof. Proposition 6 and Corollary 1 of [Se] on page 104 show the equation

$$\prod_{U \leq G} (d_{L^U/K})^{a_U} = 1.$$

In the totally real case, one does not have to distinguish, between $d_{K/\mathbb{Q}}$ and d_K. So taking the norm yields

$$\prod_{U\leq G}(d_{L^U})^{a_U} = \prod_{U\leq G}(d_K)^{a_U\cdot(L^U:K)} = d_K^{\sum_{U\leq G} a_U\cdot(G:U)} = 1,$$

because $\deg(1_U^G) = \dim_{\mathbb{C}}(\mathbb{C}G\otimes_{\mathbb{C}U}\mathbb{C}) = (G:U)$. □

Proposition 2. *Let G be a finite abelian group of odd order and N a totally real number field of degree $|G|$ such that $\mathrm{Gal}(\hat{N}/\mathbb{Q})\cong\mathbb{D}_G$. Let K denote the unique quadratic subfield of $\hat{N}$. Then $\hat{N}/K$ is unramified if and only if $d_N = d_K^{\frac{|G|-1}{2}}$.*

Proof. Lemma 8 shows that a relation on the induced principal characters of the subgroups of the Galois group of a Galois extension gives the same relation among the discriminants of their fixed fields. Hence using lemma 6 one has $d_{\hat{N}}\cdot d_{\mathbb{Q}}^2 = d_N^2\cdot d_K$. Since all occurring fields are totally real and $d_{\mathbb{Q}} = 1$, one has the following equivalences:

$$\hat{N}/K \text{ is unramified } \iff d_{\hat{N}} = d_K^{|G|} \iff d_N^2\cdot d_K = d_K^{|G|} \iff d_N = d_K^{\frac{|G|-1}{2}}.$$

□

3.3 Coprime Modules

Let $\mathbb{M}$ denote the countable infinite set of isomorphism classes of all $\mathbb{D}_G$-modules A with the following properties:

- G and A are finite abelian groups.
- $|G|$ is odd, and $|G|$ and $|A|$ are coprime.
- $A^G = \{1\}$.

The **notation** $(G,A)\in\mathbb{M}$ is used for a $\mathbb{D}_G$-module A from $\mathbb{M}$. By proposition 1 the Galois group $\mathrm{Gal}(K_2/K_1)$ for a quadratic number field K is a $\mathbb{D}_{\mathrm{Cl}(K)}$-module. But as mentioned in the introduction to chapter 3 in stead of K_1 and K_2 certain fields $K_{1,f}$ and $K_{2,f}$ are of interest. They will be defined at the beginning of chapter 3.5. The group $\mathrm{Gal}(K_{2,f}/K_{1,f})$ is a $\mathrm{Gal}(K_{1,f}/\mathbb{Q})$-module from $\mathbb{M}$ (see proposition 7) therefore this chapter deals with properties of modules from $\mathbb{M}$. This connection of modules from $\mathbb{M}$ and $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ will be explained in chapter 3.5.

Lemma 9. *Let $(G,A),(G,B)\in\mathbb{M}$ and let C be a $\mathbb{D}_G$-submodule of A.*
Then $(G,C),(G,A/C),(G,A\oplus B)\in\mathbb{M}$.

Proof. It has to be shown that $(A/C)^G = \{1\}$. By lemma 2.6 b the G-modules A and A/C have trivial Tate cohomology and hence by lemma 2.8 one has $A^G = n_G(A)$ and therefore $(A/C)^G = n_G(A/C) = (n_G(A)\cdot C)/C$, where n_G are the norm maps (the G-homomorphisms induced by the action of $\sum_{g\in G} g\in\mathbb{Z}G$ on the corresponding G-modules). The assumption on the G-module A implies $A^G = \{1\}$ and therefore $n_G(A) = \{1\}$ and $(A/C)^G = \{1\}$. □

Lemma 10. *Let G be a finite group, A a finite G-module and B a finite $\mathbb{D}_G$-module such that G is cyclic or $|G|$ is coprime to $|A|$ and $|B|$. Then the following hold:*

(a) $A^G = \{1\}$ *if and only if* $I_G A = A$.

(b) If $A^G = \{1\}$, *then* $\hat{H}^i(G, A) = \{1\}$ *for every positive integer* i.

(c) If $B^G = \{1\}$, *then* $\hat{H}^i(\mathbb{D}_G, B) = \{1\}$ *for every positive integer* i.

Proof. Assume first G to be cyclic. Let x denote a generator of G and let σ denote the automorphism of A induced by x. One has $A^G = \mathrm{Ker}(\sigma - 1)$ and $I_G A = \mathrm{Im}(\sigma - 1)$. This shows statement (a). Statement (b) follows by lemma 2.9. The inf res sequence from cohomology (see lemma 2.6) shows that there is an exact sequence of abelian groups

$$\hat{H}^i(\mathbb{D}_G/G, B^G) \to \hat{H}^i(\mathbb{D}_G, B) \to \hat{H}^i(G, A)$$

for all integers $i > 0$. By assumption $B^G = \{1\}$, which implies (c). If $|G|$ and $|A|$ are coprime, by lemma 2.10 one has $A = A^G \oplus I_G A$ and by lemma 2.6 one has $\hat{H}^i(G, A) = \{1\}$, for all integers i. This shows (a) and (b). The proof of statement (c) is the same as in the cyclic case. □

Corollary. *Let* $(G, A) \in \mathbb{M}$. *Then* $I_G A = A$, $\hat{H}^1(\mathbb{D}_G, A) = \{1\}$ *and* $\hat{H}^2(\mathbb{D}_G, A) = \{1\}$.

Lemma 11. *Let* $(G, A) \in \mathbb{M}$ *and let* $\varphi \in \mathbb{D}_G \setminus G$ *be any involution. Then:*

(a) $A = A^{\langle\varphi\rangle} \oplus K$ *as group, where* $K \cong A^{\langle\varphi\rangle}$ *as subgroup of* A.

(b) If τ, σ *are elements of* $\mathbb{D}_G$ *such that* $\langle \tau \cdot \sigma^{-1} \rangle = G$, *then* $A = (A^{\langle\varphi\rangle})^\tau \oplus (A^{\langle\varphi\rangle})^\sigma$.

(c) If $G = \langle\sigma\rangle$ *is cyclic,* B *the external direct sum of two copies of* $A^{\langle\varphi\rangle}$, $f : A \to B$ *the group isomorphism which maps* $a \cdot b^\sigma$ *to* (a, b) $\forall\, a, b \in A^{\langle\sigma\rangle}$, $\Phi = \begin{pmatrix} \mathbb{1} & \sigma + \sigma^{-1} \\ 0 & -\mathbb{1} \end{pmatrix}$ *and* $\Sigma = \begin{pmatrix} 0 & -\mathbb{1} \\ \mathbb{1} & \sigma + \sigma^{-1} \end{pmatrix}$, *then the following diagrams are commutative:*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\Phi} \\ A & \xrightarrow{f} & B \end{array} \qquad\qquad \begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\Sigma} \\ A & \xrightarrow{f} & B \end{array}$$

Proof. This is a corollary to the proof of lemma 5. □

Remark: This lemma still holds true, if A is a finite $\mathbb{D}_G$-module, where G is a finite cyclic group of odd order such that $A^G = \{1\}$ (see remark after lemma 5).

For every $(G, A) \in \mathbb{M}$, the C_2-module structure of complements of G in $\mathbb{D}_G$ on A is unique and independent of the G-module structure of A. It is described by the next lemma. It always corresponds to the representation $\begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}$ respectively to the module $(A^{C_2})\uparrow_{\{1\}}^{C_2}$.

Lemma 12. *Let* A *be a finite* C_2*-module such that* $A \cong A^{C_2} \oplus A^{C_2}$ *as groups and* A^{C_2} *is a (group theoretic) direct summand of* A. *Let* $\varphi \in \mathrm{Aut}(A)$ *denote the action of the generator of* C_2. *Then* A *has trivial Tate cohomology and there is a subgroup* $M \leq A$ *such that* $A = M \oplus M^\varphi$ *and* $M \cong A^{C_2}$ *as group. In particular the module structure is unique.*

Proof. The module A decomposes as C_2-module into components of prime power order and cohomology is compatible with direct sums. This allows the restriction to the following two cases:
Case 1: $2 \nmid |A|$: Because $|C_2|$ and $|A|$ are coprime, A has trivial Tate cohomology as C_2-module and one has $A = A^{C_2} \oplus I_{C_2}A$ (see lemma 2.10). The automorphism φ of A is trivial on the first summand and inverts every element of the second summand. By the assumption $A \cong A^{C_2} \oplus A^{C_2}$ the theorem of Krull-Remak implies that there is an isomorphism of groups $f : A^{C_2} \to I_{C_2}A$. Set $M := \langle a \cdot f(a) | a \in A^{C_2} \rangle$. Since $2 \nmid |A|$ any element of A is a square $a^2 \cdot f(b^2)$ with $a, b \in A^{C_2}$. One has $a \cdot f(a) \cdot (a \cdot f(a))^{\varphi} = a^2$ and $b \cdot f(b) \cdot (b^{-1} \cdot f(b^{-1}))^{\varphi} = f(b^2)$ and therefor $A = M \cdot M^{\varphi}$. Since $|A| = |A^{C_2}|^2 = |M| \cdot |M^{\varphi}|$ one has $A = M \oplus M^{\varphi}$.
Case 2: A is a 2 group: By assumption A^{C_2} has a group theoretical complement $M \leq A$ which is isomorphic to A^{C_2} by the theorem of Krull-Remak. Let $x \in M \cap M^{\varphi}$ and suppose $x \neq 1$. Let 2^n denote the order of x. Then $n > 0$ and $y := x^{(2^{n-1})}$ is an element of order 2 such that $y^{\varphi} \cdot y^{-1}$ is contained in M. But because the order of y is 2 this is also an element of A^{C_2} and so $y^{\varphi} = y$. Since $y \in M$, $y = 1$ follows. This is a contradiction. Because $|A| = |M| \cdot |\varphi(M)|$, one has $A = M \oplus M^{\varphi}$. Since A is finite and $\mathrm{Im}(\varphi + 1) \leq \mathrm{Ker}(\varphi - 1)$, by lemma 2.9, it remains to show that $|\mathrm{Ker}(\varphi - 1)| \leq |\mathrm{Im}(\varphi + 1)|$ to prove the Tate cohomology to be trivial. But $A = M \cdot M^{\varphi} = M \cdot M^{\varphi+1} = M \cdot \mathrm{Im}(\varphi + 1)$ implies $|\mathrm{Im}(\varphi + 1)| \geq \frac{|A|}{|M|} = |\mathrm{Ker}(\varphi - 1)|$. □

Lemma 13. *Let $(G, A) \in \mathbb{M}$. Then A is relatively projective (to $\{1\}$) as $\mathbb{D}_G$-module.*

Proof. Let φ be the generator of a complement of G in $\mathbb{D}_G$. By lemma 5 the assumptions of lemma 12 are fulfilled and there is a subgroup $M \leq A$ such that $A = M \oplus M^{\varphi}$ as group. Let $f : A \to A$ be the projection on the first summand. Because of lemma 2.5, it suffices to show: $Tr_{\{1\}}^{\mathbb{D}_G}(\frac{1}{|G|} \cdot f) = id_A$ (since $(G, A) \in \mathbb{M}$, the orders $|A|$ and $|G|$ are coprime and multiplication with $\frac{1}{|G|}$ is a well defined isomorphism). For this let $x \in A$. Then one has:

$$\begin{aligned} Tr_{\{1\}}^{\mathbb{D}_G}(\frac{1}{|G|} \cdot f)(x) &= (\prod_{g \in \mathbb{D}_G} f(x^g)^{g^{-1}})^{\frac{1}{|G|}} \\ &= (\prod_{g \in G} (f(x^g) \cdot f(x^{g\varphi})^{\varphi})^{g^{-1}})^{\frac{1}{|G|}} \\ &= (\prod_{g \in G} x)^{\frac{1}{|G|}} \\ &= x. \end{aligned}$$

□

In the following the modules from $\mathbb{M}$ will be classified. This is not difficult, because these modules behave like principal indecomposable modules, known from rings with minimal condition.

Let R be a ring and G be a finite group. A finitely generated RG-module is called **relatively hereditary** if and only if every module M, which arises from A by taking submodules or quotients iteratively, is relative projective. A finite $\mathbb{D}_G$-module A has this property, if $(G, A) \in \mathbb{M}$ or if $2 \cdot |G|$ and $|A|$ are coprime for example. In the first case this is an obvious consequence of the lemmas 9 and 13 and in the coprime case this statement is implied by lemma 2.5.

The next lemma is an adaptation of standard methods from representation theory (like "idempotent refinement") to the special case which is of interest here. The proofs of statements (c) and (e) of lemma 14 and of proposition 3 (c) are almost word for word the same as in [Bau], Sätze 3.6, 3.8, 3.9, although these theorems show different statements.

Lemma 14. *Let G be a finite group and A be an indecomposable finite relatively hereditary G-module. Then the following hold:*

(a) There is a prime p and integers e and r such that $A \cong (C_{p^e})^r$ as group.

(b) A is projective as $(\mathbb{Z}/p^e\mathbb{Z})G$-module.

(c) For any submodule F of A the G-module A/F is indecomposable.

(d) If F is the Frattini-subgroup of A, then A/F is an irreducible and projective $\mathbb{F}_pG$-module.

(e) If B is another indecomposable finite relatively hereditary G-module with Frattini-subgroup E such that $|B|=|A|$ and $B/E \cong A/F$, then $A \cong B$.

Proof. (see [Bau], [Go]) Statement (a) can be proved as lemma 5.2.1 and theorem 5.2.2 in [Go] which uses the assumption that $|G|$ has to be coprime to $|A|$. But the assumptions of this lemma are sufficient by lemma 2.5, because Gorenstein [Go] uses the coprimeness assumption just to ensure that submodules with group theoretic complement also have module theoretic complements. The underlying group $(C_{p^e})^r$ of A is a free $\mathbb{Z}/p^e\mathbb{Z}$-module, so statement (b) follows by lemma 2.4. Assume that A/F is not indecomposable. Therefore there exist submodules $M, N \leq A$ with $F \subsetneq N$ and $F \subsetneq M$ such that $A/F = M/F \oplus N/F$. Define the surjective R-homomorphism $\tau : A \to A/M \cong (A/F)/(M/F) \cong N/F$ where $R := \mathbb{Z}/p^e\mathbb{Z}G$, the first map is the residue-map and the last two maps are any R-isomorphisms. If $i : N \to A$ is the inclusion, then $\tau \circ i : N \to N/F$ is a surjective R-homomorphism. By (b) there exists an R-homomorphism $\varphi : A \to N$ such that $\tau \circ i \circ \varphi = \tau$. Since $\tau \neq 0$ the Fitting lemma (lemma 2.3) shows that $i \circ \varphi$ is an automorphism of A. This is a contradiction to $|N| < |A|$ and shows (c). If F is the Frattini-subgroup of A, then F is a G-submodule of A and A/F is an $\mathbb{F}_p$-vector space and G-module. By the assumption on A, the abelian group A/F is relatively projective as G-module and obviously it is projective as $\mathbb{F}_p$-vector space. Therefore A/F is projective as $\mathbb{F}_pG$-module by lemma 2.4. By (c) A/F is an indecomposable $\mathbb{F}_pG$-module. Since A/F is elementary abelian, a non trivial proper submodule of A/F would have a group theoretic complement and therefore (by the assumption on A) a module theoretic complement. This shows that A/F is irreducible and statement (d) follows. By (a) one has $B \cong A \cong (C_{p^e})^{\dim_p(A/F)}$ as groups and A, B are projective R-modules by (b). Let $\pi_A : A \to A/F$ and $\pi_B : B \to A/F$ be surjective R-homomorphisms. Then there exist R-homomorphisms $f_A : A \to B$ and $f_B : B \to A$ such that $\pi_A = \pi_B \circ f_A$ and $\pi_B = \pi_A \circ f_B$. Therefore $\pi_A \circ f_B \circ f_A = \pi_A$ and $\pi_B \circ f_A \circ f_B = \pi_B$. Because $\pi_A, \pi_B \neq 0$, the Fitting lemma shows that $f_A \circ f_B$ and $f_B \circ f_A$ are isomorphisms and hence $A \cong B$ as G-modules. This implies statement (e). □

Remark: The assumption that A is a projective indecomposable $\mathbb{Z}/p^e\mathbb{Z}G$-module is sufficient for statement (c).

Proposition 3. *Let G be a finite abelian group of odd order.*

(a) Let $(G, A) \in \mathbb{M}$. Then A is a finite direct sum of indecomposable $\mathbb{D}_G$-modules A_i, with $(G, A_i) \in \mathbb{M}$. The $\mathbb{D}_G$-modules A_i are (after reordering) unique up to isomorphism.

(b) *Let $(G, A) \in \mathbb{M}$ such that A is an indecomposable $\mathbb{D}_G$-module. Then there is a prime p not dividing $|G|$ and integers e and r such that $A \cong (C_{p^e})^r$ as group. If F is the Frattini-subgroup of A, then A/F is an irreducible and projective $\mathbb{F}_p\mathbb{D}_G$-module with $(A/F)^G = \{1\}$.*

(c) *If p is a prime not dividing $|G|$, e an integer and M an irreducible and finite $\mathbb{F}_p\mathbb{D}_G$-module with $M^G = \{1\}$, then there is (up to isomorphism) exactly one indecomposable $\mathbb{D}_G$-module A with $(G, A) \in \mathbb{M}$, $|A| = |M|^e$ and $A/F \cong M$, where F is the Frattini-subgroup of A.*

Proof. (see [Bau]) Statement (a) is a consequence of the theorem of Krull-Remak and of lemma 9, and (b) and the uniqueness-part of (c) are implied by lemma 14, because if $(G, A) \in \mathbb{M}$, then the $\mathbb{D}_G$-module A is relative hereditary by lemma 13 and lemma 9.
It remains to show the existence part of (c): Set $R := (\mathbb{Z}/p^e\mathbb{Z})G$ and let be $0 \neq m \in M$. The R-homomorphism $f : R \to M : x \mapsto m \cdot x$ is surjective. If $R = A_1 \oplus \cdots \oplus A_n$ is a decomposition of R into indecomposable R modules, then there is a summand (without loss of generality) $A_1 =: A$ such that the restriction of f to A is surjective (because surjective means non zero since M is irreducible). Because $M^G = \{1\}$ and because of lemma 2.10, one has $A^G = \{1\}$ and hence $(G, A) \in \mathbb{M}$. Let F be the Frattini-subgroup of A. Because M is an elementary abelian group $F \leq \mathrm{Ker}(f|_A)$ and because A/F is irreducible by (b), one has $F = \mathrm{Ker}(f|_A)$, which shows the existence part of (c). □

This proposition reduces the classification of indecomposable modules from $\mathbb{M}$ to the classification of the irreducible $\mathbb{F}_p\mathbb{D}_G$-modules A with $A^G = \{1\}$, where p is a prime and G is a finite abelian group such that $2 \cdot p \nmid |G|$. This classification is well known (see [I] chapters 6, 9) and will be done by the next two lemmas. The methods are similar to those in [Lem1], where Lemmermeyer gives a generalization to the p-rank theorem.

Let χ_1, χ_2 be two characters of irreducible representations of a finite group G over the algebraic closure $\overline{K}$ of a field K. The characters χ_1 and χ_2 are called **Galois conjugate** over K if and only if there is a K-automorphism σ of $\overline{K}$ such that $\chi_1(g)^\sigma = \chi_2(g)$ for all $g \in G$. Galois conjugacy is an equivalence relation on a set of representatives of irreducible $\overline{K}G$-representations.

Lemma 15. *Let p be a prime and $n > 1$ an integer such that $2, p \nmid n$. Let*

$$\mathbb{D}_n = \langle x, y \mid x^2 = y^n = 1, y^x = y^{-1} \rangle$$

be a dihedral group and let $\xi_0 = 1, \xi_1, ..., \xi_{n-1} \in \overline{\mathbb{F}}_p$, with $r = \frac{n-1}{2}$ and $\xi_i^{-1} = \xi_{i+r}$ for $i = 1, ..., r$, be the n-th roots of 1. Let a_p be an integer and let $Y_1, ..., Y_{a_p}$ be a system of representatives of the irreducible faithful $\mathbb{D}_n$-representations over $\mathbb{F}_p$. Then the following hold:

(a) *If $p = 2$, then $\mathbb{1}_{\overline{\mathbb{F}}_p}$ and $X_i = (x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, y \mapsto \begin{pmatrix} \xi_i & 0 \\ 0 & \xi_i^{-1} \end{pmatrix})$ for $i \in \{1, ..., r\}$ form a system of representatives of all irreducible $\mathbb{D}_n$-representations over $\overline{\mathbb{F}}_p$. If $p \neq 2$, then there is in addition the irreducible representation $(x \mapsto -1, y \mapsto 1)$. The X_i with ξ_i primitive are the irreducible faithful representations.*

(b) *The 1-dimensional irreducible representations from (a) are their own Galois conjugacy class, and two representations X_i and X_j are Galois conjugate, if and only if*

there is an integer k such that $\xi_i^{p^k} = \xi_j^{\pm 1}$. Over $\overline{\mathbb{F}}_p$ every Y_i is the sum of the representations in a Galois conjugacy class. Every Galois conjugacy class with a faithful representative occurs in that way, different Y_i belongs to different conjugacy classes and a Y_i is faithful, if and only if every $\overline{\mathbb{F}}_pG$-representation of the conjugacy class belonging to Y_i is faithful, if and only if one $\overline{\mathbb{F}}_pG$-representation of the conjugacy class belonging to Y_i is faithful.

(c) *Let $f_p := \min_k(p^k \equiv 1(n), k > 0)$ be the order of p mod n. If -1 is a power of p mod n, set $d_p := f_p$, else define $d_p := 2 \cdot f_p$. Then the a_p non similar irreducible faithful $\mathbb{D}_n$-representations over $\mathbb{F}_p$ all have degree d_p.*

Proof. a: The polynomial $x^n - 1$ is separable over $\mathbb{F}_p$ and $\xi_i + \xi_i^{-1} = \xi_j + \xi_j^{-1}$ if and only $\xi_i = \xi_j^{\pm 1}$. All given representations have different characters and are non-equivalent therefore. The irreducible representations of the normal subgroup $\langle y \rangle \leq \mathbb{D}_n$ over $\overline{\mathbb{F}}_p$ are given by $x \mapsto (\xi_i)$ for $i = 0, ..., n-1$. If X is an irreducible $\mathbb{D}_n$-representation over $\overline{\mathbb{F}}_p$, then by the theorem of Clifford ([I] theorem 6.5) there is a basis such that the restriction to $\langle y \rangle$ is $X(y) = \begin{pmatrix} \xi_i & 0 \\ 0 & \xi_i^{-1} \end{pmatrix}$ for a suitable $i \in \{1, ..., n-1\}$ or $X(y) = 1$. With the Ansatz $X(x) = (a)$ or $X(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, using $X(x)^2 = \mathbb{1}$ and $X(x) \cdot X(y) \cdot X(x) = X(y)^{-1}$, one can calculate the possible values for $X(x)$. For the one dimensional case, this is $X(x) = 1$ and if $p \nmid 2$ in addition $X(x) = -1$. In the two dimensional case the result is $X(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $X(x) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. Both representations are similar via $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.
b: By [I] corollary 9.22 non-similar irreducible representations have different characters, therefore all representations in a Galois conjugacy class have the same kernel. Because of [I] theorem 9.14 and theorem 9.21, it just has to be shown that the two representations X_i and X_j are Galois conjugate, if and only if there is an integer k such that $\xi_i^{p^k} = \xi_j^{\pm 1}$. But this is a consequence of the fact that $\xi_i + \xi_i^{-1} = \xi_j + \xi_j^{-1}$ if and only $\xi_i = \xi_j^{\pm 1}$ and that all Galois groups of finite extensions of $\mathbb{F}_p$ are generated by the Frobenius automorphism.
c: The size l_i of the Galois conjugacy class of the faithful irreducible representation X_i is the smallest integer $k > 0$ such that $\xi_i^{p^k} + \xi_i^{-p^k} = \xi_i + \xi_i^{-1}$. By the previous l_i is the smallest $k > 0$ such that $\xi^{p^k} = \xi^{\pm 1}$. Therefore $l_i = \frac{f_p}{2}$ if -1 is a power of p mod n and $l_i = f_p$ in the other case. Since all the faithful irreducible $\mathbb{D}_n$-representations are two dimensional by (a), statement (c) follows. □

Lemma 16. *Let $G \neq \{1\}$ be a finite abelian group and p be a prime such that $2, p \nmid |G|$. Let A be an irreducible $\mathbb{F}_p\mathbb{D}_G$-module with $A^G = \{1\}$ and let $N \leq \mathbb{D}_G$ be the kernel of the action of $\mathbb{F}_p\mathbb{D}_G$ on A. Then the following hold:*

(a) *N is a proper subgroup of G and G/N is cyclic.*

(b) *If $n = (G : N)$, then A is a finite, faithful and irreducible $\mathbb{D}_n$-module.*

(c) *If $1 < m$ is an odd integer coprime to p and B is a finite, faithful, irreducible $\mathbb{F}_p\mathbb{D}_m$-module, then for every subgroup M of G such that $G/M \cong C_m$, there is an (up to isomorphism) unique $\mathbb{F}_p\mathbb{D}_G$-module A with $A^G = \{1\}$ and kernel M. One has $A \cong B$ as $\mathbb{F}_p\mathbb{D}_m$-module via $G/M \cong C_m$ and different choices of M lead to non isomorphic $\mathbb{F}_p\mathbb{D}_G$-modules.*

Proof. Statement (a) is a consequence of lemma 3 and implies (b). Part (c) is obvious. □

So the **classification** of modules from $\mathbb{M}$ for a fixed finite abelian group G of odd order works as follows. Two modules from $\mathbb{M}$ are isomorphic if and only if their indecomposable $\mathbb{D}_G$-module summands are isomorphic (after reordering). The indecomposable summands are also from $\mathbb{M}$ and every indecomposable module $(G, A) \in \mathbb{M}$ can be constructed by the following steps. Different choices in one of the steps lead to non isomorphic modules:

1.) Choose a subgroup $N \leq G$ such that $C_n \cong G/N$ is cyclic.

2.) Choose a prime p with $p \nmid |G|$.

3.) Let ϕ_n be the n-th cyclotomic polynomial over $\mathbb{Q}$. Choose an irreducible factor of ϕ_n mod p modulo the following equivalence relation on the factors of ϕ_n: $f \equiv g$ if and only if there is a primitive n-th root $\xi \in \overline{\mathbb{F}}_p$ of 1 such that $f(\xi) = 0$ and either $g(\xi) = 0$ or $g(\xi^{-1}) = 0$.

4.) Choose a positive integer e.

Then there is a unique irreducible faithful $\mathbb{F}_p\mathbb{D}_n$-module C belonging to step 3.) according to lemma 15. The choice in step 1.) gives by lemma 16 a unique irreducible $\mathbb{F}_p\mathbb{D}_G$-module B with $B^G = \{1\}$ belonging to C and step 4.) gives a unique indecomposable $\mathbb{D}_G$-module A with $(G, A) \in \mathbb{M}$, $|A| = |B|^e$ and $A/F(A) \cong B$, because of proposition 3.

Corollary 1. *Let $(G, A) \in \mathbb{M}$ and let A denote also* ***the abelian group underlying*** *the module A. If $n := |G| = 1$, just $A = \{1\}$ is possible. Otherwise A is any finite direct sum of the groups $(C_{p^e})^r$, where p is any prime not dividing n, e any positive integer (independent from all other choices) and r is any of the integers $\mathrm{lcm}(2, f_{p,q})$, where $f_{p,q} := \min_k(p^k \equiv 1(q), k > 0)$ and q goes through the prime divisors of n.*

Proof. Denote $f_{p,n} := \min_k(p^k \equiv 1(n), k > 0)$, where p is a prime and n an integer with $p \nmid n$. If q is another prime and divides n, then $f_{p,q}$ divides $f_{p,n}$. The unit group of $\mathbb{Z}/q\mathbb{Z}$ is cyclic. Therefore there is an m such that $p^m \equiv -1\,(q)$, if and only if $f_{p,q}$ is even. Lemma 15 c implies that the degrees of the faithful irreducible $\mathbb{D}_q$-representations over $\mathbb{F}_p$ are exactly the sums of the $\mathrm{lcm}(2, f_{p,q})$, where q is a prime dividing n. Hence the statement is a consequence of the classification. □

Remark: The similar question, which class numbers of number fields with certain Galois group can (possibly) occur, is treated in [K-N], and [Lem1] also answers similar questions about the ranks of class groups with certain Galois-modules structures.

Let $G \neq \{1\}$ be a finite abelian group of odd order. On page 10 two $\mathbb{D}_G$-modules A, B have been called conjugate, if and only if there is an automorphism $\phi \in \mathrm{Aut}(\mathbb{D}_G)$ such that $B \cong {}^{\phi}A$ as $\mathbb{D}_G$-module. Lemma 2.11 defines an action of $\mathrm{Out}(G)$ on the set of isomorphism classes of G-modules. The set of isomorphism classes of $\mathbb{D}_G$-modules from $\mathbb{M}$ is closed under this action. Since G is a characteristic subgroup of $\mathbb{D}_G$ and all complements of G in $\mathbb{D}_G$ are conjugate, one has $\mathrm{Aut}(\mathbb{D}_G) = \mathrm{Inn}(\mathbb{D}_G) \cdot U$ and $U \cap \mathrm{Inn}(\mathbb{D}_G) = \langle \mathrm{inv} \rangle$, where $U \cong \mathrm{Aut}(G)$ is the subgroup of $\mathrm{Aut}(\mathbb{D}_G)$ which fixes one complement of G in $\mathbb{D}_G$, and inv is the automorphism which inverts every element. Therefore $\mathrm{Out}(\mathbb{D}_G) \cong \mathrm{Aut}(G)/\langle \mathrm{inv} \rangle$ and after choosing a complement of G in $\mathbb{D}_G$, one gets a left action of $\mathrm{Aut}(G)/\langle \mathrm{inv} \rangle$ on the isomorphism classes of $\mathbb{D}_G$-modules from $\mathbb{M}$. Hence the representation module R (see page 10) of $\mathbb{D}_G$-modules from $\mathbb{M}$ is an $\mathrm{Aut}(G)/\langle \mathrm{inv} \rangle$-module.

Corollary 2. *Let $G \neq \{1\}$ be a finite abelian group of odd order and R be the representation module of $\mathbb{D}_G$-modules from $\mathbb{M}$. Let S be the set of primes not dividing $|G|$, L be a system of representatives of Kronecker equivalence for proper normal subgroups N of G such that G/N is cyclic, let $U_N := \{\phi \in \mathrm{Aut}(G)/\langle \mathrm{inv}\rangle \mid \phi(N) = N\}$. Define an $\mathrm{Aut}(G)/\langle \mathrm{inv}\rangle$-module $\tilde{R}$ by $\tilde{R} := \bigoplus_{e\geq 1}\bigoplus_{p\in S}\bigoplus_{N\in L}(\mathbb{Z}(\mathrm{Aut}(G/N)/\langle \mathrm{inv}, x \mapsto x^p\rangle)) \uparrow_{U_N}^{\mathrm{Aut}(G)/\langle \mathrm{inv}\rangle}$, where U_N acts on $\mathrm{Aut}(G/N)/\langle \mathrm{inv}, x \mapsto x^p\rangle$ in the natural way by left multiplication and e runs through all positive integers. Then $R \cong \tilde{R}$ as left $\mathrm{Aut}(G)/\langle \mathrm{inv}\rangle$-modules.*

Proof. By lemma 14 and by lemma 2.11 the representation module R equals $R = \bigoplus_{e\geq 1}\bigoplus_{p\in S} R_{e,p}$, where $R_{e,p}$ is the representation module of the $\mathbb{D}_G$-modules from $\mathbb{M}$, which as groups are homocyclic p-groups of exponent e. By proposition 3 one has $R_{e,p} \cong R_{1,p}$ for all $p \in S$ and for all integers $e \geq 1$. Because of lemma 2.12 one has $R_{1,p} \cong \bigoplus_{N\in L} R_{1,p,N} \uparrow_{U_N}^{\mathrm{Aut}(G)/\langle \mathrm{inv}\rangle}$, where $R_{1,p,N}$ is the free $\mathbb{Z}$-module over all isomorphism classes of irreducible $\mathbb{F}_p\mathbb{D}_G$-modules from $\mathbb{M}$ with kernel N. By definition of $\mathbb{M}$, N has to be a proper subgroup of G and by lemma 3 the factor group G/N has to be cyclic. If for an integer n the module $T_{p,n}$ is the representation module of the faithful irreducible $\mathbb{F}_p\mathbb{D}_n$-modules, then after any identification of $C_{(G:N)}$ with G/N, $T_{p,(G:N)}$ is also an U_N-module in the natural way and as such it is isomorphic to $R_{1,p,N}$. Because of lemma 15, the group $\mathrm{Aut}(G/N)/\langle \mathrm{inv}\rangle$ acts transitively on $T_{p,(G:N)}$ and each fixed group equals $\langle inv, x \mapsto x^p\rangle/\langle \mathrm{inv}\rangle$. Therefore $R_{1,p,N} \cong T_{p,(G:N)} \cong \mathbb{Z}(\mathrm{Aut}(G/N)/\langle \mathrm{inv}, x \mapsto x^p\rangle)$ as U_N-modules. □

Example: This example shows how these corollaries allow to calculate the number of $\mathbb{D}_{C_9\times C_3}$-module structures from $\mathbb{M}$ on C_2^6: The group $G := C_9 \times C_3$ has three Kronecker equivalent subgroups N_1, N_2, N_3 with $G/N_i \cong C_9$ and two Kronecker equivalence classes M_0 and $\{M_1, M_2, M_3\}$ of subgroups such that $G/M_i \cong C_3$. One has the isomorphisms $\mathrm{Aut}(C_3)/\langle inv, x \mapsto x^2\rangle \cong \mathrm{Aut}(C_9)/\langle inv, x \mapsto x^2\rangle \cong \{1\}$ since 2 is a primitive root mod 3 and mod 9, and there is one irreducible faithful $\mathbb{F}_2\mathbb{D}_3$-module and it has degree 2 and one irreducible faithful $\mathbb{F}_2\mathbb{D}_9$-module and it has degree 6. With the notation of the proof of corollary 2, one has $R_{1,2} \cong \mathbb{Z} \oplus \mathbb{Z} \uparrow_{U_{M_1}}^{\mathrm{Aut}(G)/\langle inv\rangle} \oplus \mathbb{Z} \uparrow_{U_{N_1}}^{\mathrm{Aut}(G)/\langle inv\rangle}$. The last two summands are free $\mathbb{Z}$-modules of rank three, which are permuted by $\mathrm{Aut}(G)/\langle inv\rangle$ as by $\mathbb{S}_3$. By the second corollary to the classification every $\mathbb{D}_{C_9\times C_3}$-module structure on C_2^6 corresponds to an element of $R_{1,2} \cong \mathbb{Z}^7$ (as group) where all components are non negative integers and where the sum of the dimensions of the corresponding modules adds to 6. The following table shows the 23 module structures from $\mathbb{M}$ of $\mathbb{D}_{C_9\times C_3}$ on C_2^6. Each row represents one module-structure. The first 4 columns count how many of its indecomposable summands are isomorphic to the two dimensional faithful indecomposable $\mathbb{F}_2\mathbb{D}_3$-module with kernel M_0, M_1, M_2 and M_3 and the last three columns do the same for the faithful $\mathbb{F}_2\mathbb{D}_9$-module of dimension 6 with kernel N_1, N_2 and N_3. By horizontal lines the module structures are grouped into 8 sections of conjugate modules:

3	0	0	0	0	0	0
2	1	0	0	0	0	0
2	0	1	0	0	0	0
2	0	0	1	0	0	0
1	2	0	0	0	0	0
1	0	2	0	0	0	0
1	0	0	2	0	0	0

1	1	1	0	0	0	0
1	1	0	1	0	0	0
1	0	1	1	0	0	0
0	1	1	1	0	0	0
0	3	0	0	0	0	0
0	0	3	0	0	0	0
0	0	0	3	0	0	0
0	2	1	0	0	0	0
0	2	0	1	0	0	0
0	1	2	0	0	0	0
0	0	2	1	0	0	0
0	1	0	2	0	0	0
0	0	1	2	0	0	0
0	0	0	0	1	0	0
0	0	0	0	0	1	0
0	0	0	0	0	0	1

Example: The same as in the previous example can be done for the $\mathbb{D}_{C_5}$-module structures from $\mathbb{M}$ on $C_{11}^4 \times C_{121}^2$. All these modules are faithful $\mathbb{D}_{C_5}$-modules and one has $\mathrm{Aut}(C_5)/\langle inv, x \mapsto x^{11}\rangle = \mathrm{Aut}(C_5)/\langle inv\rangle \cong C_2$. Hence there are two non isomorphic irreducible faithful $\mathbb{F}_{11}\mathbb{D}_{C_5}$-modules, both of degree 2. Therefore (with notation of the proof of corollary 2) $R_{1,11} \oplus R_{2,11} \cong \mathbb{Z}C_2 \oplus \mathbb{Z}C_2$, where $\mathrm{Aut}(C_5)/\langle inv\rangle$ acts as C_2. So one has the following six $\mathbb{D}_{C_5}$-module structures from $\mathbb{M}$ on $C_{11}^4 \times C_{121}^2$, which are grouped into three conjugacy classes by horizontal lines again. The rows and columns of this table have analogous meaning as in the previous example.

2	0	1	0
0	2	0	1
2	0	0	1
0	2	1	0
1	1	1	0
1	1	0	1

If G is a finite abelian group of odd order and A a finite G-module such that $A^G = \{1\}$ and $(|A|, |G|) = 1$, then $(G, A) \notin \mathbb{M}$ in general. But if it does, then the $\mathbb{D}_G$-module structure is uniquely determined by the G-module structure (see [Bos] for similar questions):

Lemma 17. *Let $(G, A_1), (G, A_2) \in \mathbb{M}$. Then A_1 and A_2 are isomorphic as $\mathbb{D}_G$-modules if and only if they are isomorphic as G-modules.*

Proof. Assume that A_1 and A_2 are isomorphic as G-modules. Let A be the underlying group of A_1 and A_2 and let $\rho, \tau \in \mathrm{Hom}(\mathbb{D}_G, \mathrm{Aut}(A))$ be the homomorphisms which define the $\mathbb{D}_G$-module structure on A corresponding to A_1 and A_2. Without lost of generality $\rho|_G = \tau|_G$. Let φ and $\tilde{\varphi}$ denote the image of a complement of G in $\mathbb{D}_G$ under ρ and τ. It will be shown that there is an $h \in C_{\mathrm{Aut}(A)}(\rho(G))$ such that $h \circ \varphi = \tilde{\varphi} \circ h$.
1. Case: $G = \langle g\rangle$ is cyclic: $\sigma := \rho(g)$. By lemma 11 one has $A = A^{\langle\varphi\rangle} \oplus (A^{\langle\varphi\rangle})^\sigma$. This is a decomposition into $\sigma + \sigma^{-1} \in \mathrm{End}(A)$ invariant subgroups which are $\sigma + \sigma^{-1}$ isomorphic. The same holds true for $\tilde{\varphi}$. By the theorem of Krull-Remak there is a $\sigma + \sigma^{-1}$ isomorphism

$f : A^{\langle\varphi\rangle} \to A^{\langle\tilde{\varphi}\rangle}$. Define $\hat{f} : A \to A$ by $\hat{f}(a \cdot b) = f(a) \cdot (f(b^{\sigma^{-1}}))^{\sigma}$ for $a \in A^{\langle\varphi\rangle}$ and $b \in \sigma(A^{\langle\varphi\rangle})$. $\hat{f}$ is a $\sigma + \sigma^{-1}$ automorphism of A. If $a, b \in A^{\langle\varphi\rangle}$, then

$$\begin{aligned}
\hat{f}((a \cdot b^{\sigma})^{\sigma}) &= \hat{f}(a^{\sigma} \cdot b^{(\sigma+\sigma^{-1})\cdot\sigma-1}) \\
&= \hat{f}(b^{-1} \cdot (a \cdot b^{\sigma+\sigma^{-1}})^{\sigma}) \\
&= f(b^{-1}) \cdot f(a \cdot b^{\sigma+\sigma^{-1}})^{\sigma} \\
&= f(a)^{\sigma} \cdot f(b)^{-1} \cdot f(b)^{\sigma^2+1} \\
&= (f(a) \cdot f(b)^{\sigma})^{\sigma} \\
&= (\hat{f}(a \cdot b^{\sigma}))^{\sigma}
\end{aligned}$$

$$\begin{aligned}
\hat{f}((a \cdot b^{\sigma})^{\varphi}) &= \hat{f}(a \cdot b^{\sigma^{-1}}) \\
&= \hat{f}(a \cdot b^{\sigma+\sigma^{-1}} \cdot b^{-\sigma}) \\
&= f(a) \cdot f(b)^{\sigma+\sigma^{-1}} \cdot f(b)^{-\sigma} \\
&= f(a)^{\tilde{\varphi}} \cdot f(b)^{\sigma\cdot\tilde{\varphi}} \\
&= (\hat{f}(a \cdot b^{\sigma}))^{\tilde{\varphi}}
\end{aligned}$$

So $h := \hat{f}$ is an automorphism of A with commutes with each element of $\rho(G)$ and fulfills $h \circ \varphi = \tilde{\varphi} \circ h$.
2. Case: Reduction to cyclic case: The $\langle\rho(G), \varphi, \tilde{\varphi}\rangle$-module A satisfies the assumptions of lemma 3 (see the remark after that lemma). So one can apply case 1 to every summand in the decomposition described in lemma 3. □

3.4 Factor Groups

Let $\mathbb{G}$ denote the countable infinite set of isomorphism classes of all groups G with the following properties:

- $|G| < \infty$
- $G/G' \cong C_2$
- $G''' = \{1\}$
- $|G'/G''|$ and $|G''|$ are coprime or G'/G'' is cyclic.

This chapter derives properties of these groups. It studies at first G', then the C_2-extension of G'' contained in there and puts both together at the end. The groups from $\mathbb{G}$ occur as factor groups of $\mathrm{Gal}(K_2/\mathbb{Q})$ of a real quadratic number field K, because $\mathrm{Gal}(K_{2,f}/\mathbb{Q}) \in \mathbb{G}$ (see proposition 7; the field $K_{2,f}$ will be defined at the beginning of chapter 7). In the case that $|G'/G''|$ and $|G'''|$ are coprime, these groups are just the extensions of A by H for a $(H, A) \in \mathbb{M}$. This case is enough to cover the groups $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$, but the other case is described by the same group theory and obviously $\mathrm{Gal}(K_2/\mathbb{Q}) \in \mathbb{G}$ for a real quadratic number field K with odd cyclic class group.

Lemma 18. *(see [C-R2]) Let G be a finite group with an abelian normal subgroup N such that G/N is abelian. Assume that G/N is cyclic or that $(G : N)$ and $|N|$ are coprime. The group N can be interpreted as a G-module and G as an extension of N by G/N. The following hold:*

(a) $I_G N = G'$.

(b) $N = G'$ *if and only if* $I_G N = N$ *if and only if* $N^G = \{1\}$.

(c) If $N = G'$, *then* $\hat{H}^i(G/N, N) = \{1\}$ *for every* $i \in \mathbb{Z}$, *the extension splits and all complements of* N *in* G *are conjugate.*

Proof. a: Assume at first G/N to be cyclic. Let $m+1$ be the order of G/N, 1, x, ... , x^m be a system of representatives of G/N in G such that the class of x generates G/N and let $a, b \in N$. Then every commutator of G is of the form

$$x^i a x^j b a^{-1} x^{-i} b^{-1} x^{-j} = a^{x^{-i}\cdot(1-x^{-j})} b^{x^{-j}\cdot(x^{-i}-1)}$$

where $i, j \in \{1, ..., m\}$. Hence $G' = \langle a^{x^i-1} | a \in N, 1 \leq i \leq m \rangle = I_G N$. Now suppose $|G/N|$ and $|N|$ to be coprime, so the extension has trivial cohomology, is split and all complements are conjugate (see lemma 2.7 and lemma 2.6). It remains to show $I_G N = G'$, which is a similar calculation as in the cyclic case if one chooses a complement of G' as system of representatives of G/G' in G (see remark after this lemma).
b: This follows from (a) by lemma 10.
c: This is a consequence of (a), lemma 10 and the theorem of Zassenhaus (lemma 2.7). □

Remark: If (in the situation of the lemma) G/G' is cyclic a calculation with the commutators shows that $I_{G/G'} G' = G'$. One does not need to assume that the G/G' extension of G' splits. But in general one can not use a system of representatives of G/G' that vanishes in the commutators and therefore has to assume that this extension splits in order to have $I_{G/G'} G' = G'$.

With the orbit stabilizer theorem the following corollaries can be deduced from the previous lemma. The second one is called Theorem of Taussky:

Corollary 1. *Let* G *be a finite group such that* $G'' = \{1\}$ *and* G/G' *is a* p*-group. Then* $|G'|_q \equiv 1(p)$ *for every prime* $q \neq p$.

Corollary 2. *Let* G *be a finite group such that* $G'' = \{1\}$ *and* G/G' *is a cyclic* p*-group. Then* $p \nmid |G'|$.

The following lemma recalls some basic facts from group theory, which are needed in lemma 20 (see [C-R2] and [Su]).

Lemma 19. *Let* G *be a group and* N *a normal subgroup. Then the following hold:*

(a) $(G/N)' = (G' \cdot N)/N$.

(b) If H *is a normal subgroup of* G *containing* N *and* $\{1\} \to H \to G \to G/H \to \{1\}$ *is split, then* $\{1\} \to H/N \to G/N \to G/H \to \{1\}$ *is split.*

(c) Let G *be a finite* p*-group and* $N \neq \{1\}$. *Then* G *has a normal subgroup* $U \subsetneq N$ *such that* $N/U \subseteq \mathrm{Z}(G/U)$.

(d) Let G *be a finite* p*-group such that* $G'' = \{1\}$. *Then the natural exact sequence* $\{1\} \to G' \to G \to G/G' \to \{1\}$ *is split if and only if* $G' = \{1\}$.

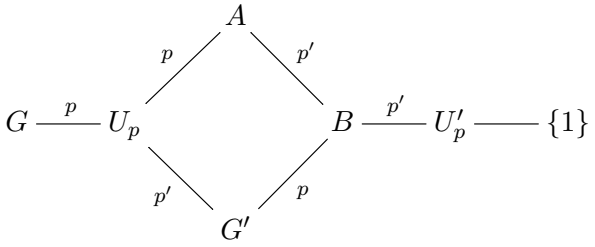
Proof. a: A calculation with the definition shows the equation:

$$(G/N)' = \langle gNhNg^{-1}Nh^{-1}N | g, h \in G \rangle = \langle ghg^{-1}h^{-1}N | g, h \in G \rangle = (G'N)/N.$$

b: If U is a complement of H in G then $(U \cdot N)/N$ is a complement of H/N in G/N since $U \cdot N \cap H \subseteq N$.
c: The Frattini subgroup F of N is a normal subgroup of G. There is an integer $n > 0$ such that $N/F \cong C_p^n$ and G acts by conjugation on the set of $\frac{p^n-1}{p-1} \equiv 1(p)$ maximal subgroups of N/F and hence has a fixed point U, which is a normal subgroup of G and a proper normal subgroup of N of index $(N : U) = p$. Because G/U is a p-group $\mathrm{Z}(G/U) \cap N/U \neq \{1\}$, hence $N/U \leq \mathrm{Z}(G/U)$.
d: Suppose the sequence is split and $G' \neq \{1\}$. By (c) G' contains a normal subgroup U of G with $(G' : U) > 1$ such that G acts trivially on G'/U. By (b) the exact sequence $\{1\} \to G'/U \to G/U \to G/G' \to \{1\}$ also splits. As both G'/U and G/G' are abelian, this implies G/U is abelian; contradiction to $(G' : U) > 1$. □

Lemma 20. *(see [C-R2]) Let G be a finite abelian group with the properties $G'' = \{1\}$ and $G \cong G/G' \ltimes G'$. Then $p \nmid |G'/U_p'|$ for all primes p, where $G' \leq U_p \leq G$ are subgroups such that $G/U_p \cong \mathrm{Syl}_p(G/G')$.*

Proof. Suppose $p \mid |G'/U_p'|$ for some prime p. U_p' is a characteristic subgroup of a normal subgroup of G and hence a normal subgroup of G. Let A respectively B denote the subgroups of U_p respectively G' containing U_p' such that $U_p/A \cong \mathrm{Syl}_p(U_p/U_p')$ respectively $G'/B \cong \mathrm{Syl}_p(G'/U_p')$. For the same reason as for U_p' they are normal subgroups of G and $B \leq A$.



By assumption $(G' : B) > 1$ and by lemma 19

$$\{1\} \to G'/B \to G/B \to G/G' \to \{1\}$$

is split, so without loss of generality $B = \{1\}$. Let $H \leq G$ be any complement of G'. Then

$$|A|_{p'} = |G|_{p'} \geq |H \cdot A|_{p'} = \frac{|H|_{p'} \cdot |A|_{p'}}{|A \cap H|_{p'}} = \frac{|A|_{p'}^2}{|A \cap H|_{p'}}$$

and H contains A. Because $U_p = G' \oplus A$ lemma 19 shows $(G/A)' = U_p/A \cong G' \neq \{1\}$. G/A is a p group and a split extension of $(G/A)'$ by G/U_p, because H/A is a complement of $(G/A)'$. This contradicts lemma 19. □

Lemma 21. *Let G be a C_2-extension of a finite abelian group A with the module structure described in lemma 12. Let x denote an involution outside A and $M \leq A$ a subgroup corresponding to x as described in lemma 12 (that means $A = M \oplus M^x$). Then the following hold:*

(a) $G \cong C_2 \ltimes A$ and all involutions of G outside A are conjugate.

(b) $G \cong M \wr C_2$.

(c) $G' = \left\{m^{-1} \cdot m^x \mid m \in M\right\} \cong A^{\langle x \rangle}$ *as group.*

(d) $G/G' \cong C_2 \times A^{\langle x \rangle}$ *as group.*

(e) $H := \langle G', x \rangle \cong \mathbb{D}_{A^{\langle x \rangle}}$ *as group and* $H = \langle y \mid y \sim x \rangle$.

(f) H *is a normal subgroup of* G *and* $G/H \cong A^{\langle x \rangle}$ *as group.*

(g) $1^G_{\{1\}} + 2 \cdot 1^G_H = 2 \cdot 1^G_{\langle x \rangle} + 1^G_{G'}$

Proof. By lemma 12 the Tate cohomology of the C_2-module A is trivial, in particular $\hat{H}^2(C_2, A) \cong \hat{H}^1(C_2, A) \cong \{1\}$. This shows (a), and (b) follows from the definition of wreath products. Properties (c), (d), (e) and (f) can be calculated from (b), and if one observes that $\{1\}$, H and G' are normal subgroups of G and the conjugacy class of x in G is xG', then (g) is a consequence of the definition $1^V_U(x) = \frac{1}{|U|} \cdot |\left\{g \in V | g^{-1}xg \in U\right\}|$. □

Lemma 22. *Let* G *be a group from* $\mathbb{G}$ *and* $x \in G \setminus G'$ *a generator of* G/G'. *Then:*

(a) $|G'/G''|$ *is odd,* $G/G'' \cong \mathbb{D}_{G'/G''}$ *and* $G''^{G'/G''} = \{1\}$.

(b) If $((G' : G''), |G''|) = 1$, *then* $(G'/G'', G'') \in \mathbb{M}$.

(c) $G \cong \mathbb{D}_{G'/G''} \ltimes G''$, *all complements of* G'' *are conjugate.*

(d) $G \cong C_2 \ltimes G'$ *and all involutions from* $G \setminus G'$ *are conjugate.*

(e) There is a subgroup $M \leq G''$ *such that* $G'' = M \oplus M^x$. *As group:* $M \cong G''^{\langle x \rangle}$ *and* $G''^{\langle x \rangle}$ *is a direct summand of* G''.

Proof. a: Let $\varphi \in \mathrm{Aut}(G'/G'')$ be the automorphism induced by x. By lemma 18 one has $G''^{G'/G''} = \{1\}$, $(G'/G'')^{G/G'} = \{1\}$, $\mathrm{Im}(\varphi - 1) = G'/G''$ and $\hat{H}^i(G/G', G'/G'') = \{1\}$, so $G/G'' \cong G/G' \ltimes G'/G''$ by the theorem of Zassenhaus. Because of the second corollary to lemma 18 the index $(G' : G'')$ is odd and lemma 2.9 implies $G'/G'' = \mathrm{Ker}(\varphi+1)$. Therefore $G/G'' \cong \mathbb{D}_{G'/G''}$.
b: This is the definition.
c: This is a consequence of (a), lemma 10 and the theorem of Zassenhaus.
d: This follows with (a) and (c), because all involutions in $\mathbb{D}_{G'/G''}$ are conjugate.
e: This is implied by (a), lemma 11 (see remark after it) and lemma 12. □

To calculate with concrete groups from $\mathbb{G}$ in [GAP] one could use the classification of the modules from $\mathbb{M}$, but the description in the following lemma is more useful. One can search the SmallGroupLibrary or calculate semidirect products according to this lemma.

Lemma 23. *Let* G *be a finite abelian group and* A *be a finite* $\mathbb{D}_G$*-module such that* G *is cyclic or* $|G|$ *and* $|A|$ *are coprime. Let* $U = \mathbb{D}_G \ltimes_\rho A$ *be the split extension of* A *by* $\mathbb{D}_G$ *corresponding to this module structure. Then the following are equivalent:*

(a) $U \in \mathbb{G}$.

(b) $A^G = \{1\}$ *and* $|G|$ *is odd.*

(c) $I_G A = A$ *and* $|G|$ *is odd.*

(d) $U' = G \ltimes_\rho A$ *and* $U'' = A$.

Proof. Statement (d) implies (a) by definition and (a) implies (b) and (d) by lemma 22. The statements (b) and (c) are equivalent because of lemma 10. It remains to show (c) $\Rightarrow$ (d): For $g \in G$ and $a \in A$ as a commutator one has $g^{-1}aga^{-1} = a^{g-1}$ and since G is abelian $(G \ltimes A)' = A$. If $x \in \mathbb{D}_G$ is an involution and $g \in G$ then $xgxg^{-1} = g^{-2}$. Because $|G|$ is odd the remaining part follows. □

Lemma 24. *Let $G \in \mathbb{G}$, let U be a complement of G'' in G, let $K \leq G$ be the subgroup of all elements of G acting trivial on G'' and let be $M := \bigcap_{n \in G''} U^n$. Then $M = Z(G')$ is the largest subgroup of U which is normal in G, one has $K = M \oplus G''$ and M is contained in U'. The center of G is trivial.*

Proof. By definition M is the largest subgroup of U which is normal in G. Therefore M is normal in U and contained in U' because $U \cong \mathbb{D}_H$ for some finite abelian H of odd order by lemma 23. A subgroup of U is normalized by G'' if and only if it is centralized by G'', hence $K = M \oplus G''$. Since $M \leq U'$, one has $K \leq G'$. Because $G''^{G'} = \{1\}$ and $U'^{U} = \{1\}$ by lemma 18, one has $C_G(G') = M$ and that implies $Z(G') = M$ and $Z(G) = \{1\}$. □

Some class number formulas hold true in the non "coprime case". The class group relations from before can be extended such that the connection to the fixed point relations remains for the 2-part of a $\mathbb{D}_H$-module A, where H and A are finite abelian groups of coprime order and $|H|$ is odd ([C-M] theorem 7.8). In this chapter some relations on the commutator factor group of subgroups of groups from $\mathbb{G}$ are considered and the connection to class groups (analogous to lemma 1) is given in chapter 3.5. This motivates the following notation, which is well defined by lemma 22 d:

Notation: *Let G be a group from $\mathbb{G}$ and $U \leq G$ be a subgroup. Then define*

$$C(U) := U/\langle U', T \cap U \mid T \text{ complement of } G' \text{ in } G\rangle.$$

Lemma 25. *Let G be a group from $\mathbb{G}$, U a subgroup of G with $G'' \leq U \leq G'$ and x a involution of $G \setminus G'$. Then*

(a) $C(U) \cong U/G'' \oplus G''^{U}$,

(b) $C(\langle U, x\rangle) \cong G''^{\langle U,x\rangle}$,

(c) $G''^{U} \cong G''^{\langle U,x\rangle} \oplus G''^{\langle U,x\rangle}$.

Proof. The extension $\{1\} \leq G'' \leq G'$ is split by lemma 22 and since $U' \leq G''$ the extension $\{1\} \leq G''/U' \leq U/U'$ is also split. Therefore $C(U) \cong U/U' \cong U/G'' \oplus G''/U'$, because every complement of G' in G has trivial intersection with U. A calculation as in lemma 18 shows $U' = I_U G''$ and using lemma 2.10 one has $G'' = I_U G'' \oplus G''^{U}$. This proves statement (a).
The extension $\{1\} \leq G'' \leq \langle U, x\rangle$ is split, so without loss of generality there is an abelian subgroup $V \leq U$ such that $\langle x, V\rangle \cong \mathbb{D}_V$ is a complement of G'' in $\langle U, x\rangle$ (otherwise change x to one of its conjugates). By the previous $\langle U, x\rangle = \langle V, x\rangle \ltimes (G''^{U} \oplus U')$. The involutions of $\langle U, x\rangle \setminus G'$ are the elements $x \cdot u \cdot g \cdot a$ with $u \in V, g \in G''^{U}, a \in U'$ and $1 = xugaxuga = g^{x+1} \cdot a^{xu+1}$. If A is the subgroup of $\langle U, x\rangle$ generated by U' and all these involutions, then $A = \langle V, x\rangle \ltimes (M \oplus U')$, with $M := \left\{g \in G''^{U} \mid g^{x+1} = 1\right\}$. Therefore $C(\langle U, x\rangle) \cong G''^{U}/M \cong G''^{\langle U,x\rangle}$ by lemma 21 and statement (b) follows. Statement (c) is a consequence of lemma 5 and lemma 23 applied to the $\mathbb{D}_{G/U}$-module G''^{U}. □

For every group $U \in \mathbb{G}$ with $(|U'/U''|, |U''|) = 1$ one has $(U'/U'', U'') \in \mathbb{M}$ by lemma 22. Since $\mathbb{D}_{U'/U''}$ is viewed as an abstract group, this module structure is not unique, because there is not just one way to name the elements of $\mathbb{D}_{U'/U''}$. With help of the methods from [R], this connection can be described. Let H be a finite group and let A be an H-module. One can define different equivalence relations on the set $\mathrm{Hom}(H, \mathrm{Aut}(A))$.
Let $\rho, \tau \in \mathrm{Hom}(H, \mathrm{Aut}(A))$. Then

(I) $\tau \equiv \rho :\Leftrightarrow \exists \psi \in \mathrm{Aut}(A)$ such that $\psi \circ \rho(g) \circ \psi^{-1} = \tau(g) \, \forall g \in H$.

(II) $\tau \equiv \rho :\Leftrightarrow \exists \psi \in \mathrm{Aut}(A)$ and $\exists \phi \in \mathrm{Aut}(H)$ such that $\psi \circ \rho(g) \circ \psi^{-1} = \tau(\phi(g)) \, \forall g \in H$.

(III) $\tau \equiv \rho :\Leftrightarrow$ the subgroups $\mathrm{Im}(\rho)$ and $\mathrm{Im}(\tau)$ are conjugate in $\mathrm{Aut}(A)$.

Lemma 26. *Let V and U be split extensions of a finite group A by a finite group H defined by $\rho, \tau \in \mathrm{Hom}(H, \mathrm{Aut}(A))$. Then the following hold:*

(a) The H-module structures on A corresponding to ρ and τ are isomorphic if and only if $\rho \equiv \tau$ by (I).

(b) ρ and τ are equivalent by (II) if and only if there is an isomorphism $f : V \to U$ such that $f(A) = A$ and $f(H) = H$.

(c) If U and V are groups from $\mathbb{G}$ such that $V'' \cong U'' \cong A$ and $U/U'' \cong V/V'' \cong H$, then $V \cong U$ if and only if $\rho \equiv \tau$ by (II).

(d) If ρ or τ is injective, then they are equivalent by (II) if and only if they are equivalent by (III).

(e) If each isomorphism between factor groups of H can be lifted to an automorphism of H, then (II) $\Leftrightarrow$ (III). (This is the case if H is dihedral or cyclic but not if $H \cong C_4 \times C_2$ for example.)

Proof. a: This is an immediate consequence of the definitions.
b: One may suppose that the underlying set of U and V is $H \times A$ and identify the groups H and A with the subgroups $H \times \{1\}$ and $\{1\} \times A$ of V and U. If ρ and τ are conjugate by (II) with ψ and ϕ (which means $\psi \circ \rho(g) \circ \psi^{-1} = \tau(\phi(g)) \forall g \in H$), then the bijective map $f : H \times A \to H \times A : (g, a) \mapsto (\phi(g), \psi(a))$ is an isomorphism from V to U, because

$$\begin{aligned} f(g,a) \cdot_\tau f(h,b) &= (\phi(g), \psi(a)) \cdot_\tau (\phi(h), \psi(b)) \\ &= (\phi(g \cdot h), \tau(\phi(h))(\psi(a)) \cdot \psi(b)) \\ &= (\phi(g \cdot h), \psi((\psi^{-1} \circ (\tau \circ \phi)(h) \circ \psi)(a) \cdot \psi(b))) \\ &= (\phi(g \cdot h), \psi(\rho(h)(a) \cdot (b))) \\ &= f((g,a) \cdot_\rho (h,b)) \end{aligned}$$

If on the other hand an isomorphism $f : V \to U$ restricts to A and to H (that means $f(H) = H$ and $f(A) = A$), then the same calculation shows that $\phi := f|_H$ and $\psi := f|_A$ define an equivalence (II) between ρ and τ.
c: If $f : V \to U$ is an isomorphism, then $f(U'') = V''$. One may assume that V and U possess the same set, which contains H, and as consequence of lemma 22 (c) one may assume $f(H) = H$.
d, e: The statements (d) and (e) follows from $H/\mathrm{Ker}(\rho) \cong \mathrm{Im}(\rho)$ and $H/\mathrm{Ker}(\tau) \cong \mathrm{Im}(\tau)$. □

Proposition 4. *Let $(G, A), (G, B) \in \mathbb{M}$. Then the following hold:*

(i) $\mathbb{D}_G \ltimes A, \in \mathbb{G}$.

(ii) There is an isomorphism of groups $\mathbb{D}_G \ltimes A \cong \mathbb{D}_G \ltimes B$ if and only if the $\mathbb{D}_G$-modules A and B are conjugate according to the notation on page 10.

Proof. The first statement follows from lemma 23 and the second one is a consequence of lemma 26 (c). □

Example: *Let A be a finite abelian group. Then there is a group $G \in \mathbb{G}$ such that $A \cong G''$ and $G'/G'' \cong C_3$ if and only if $|A|$ and 3 are coprime and there is an abelian group B such that $A \cong B \oplus B$. G is uniquely determined by B in this case.*

Proof. Without lost of generality one may assume $A \neq \{1\}$.
"⇒": Corollary 2 of lemma 18 shows that $|A|$ and 3 are coprime and by lemma 22 (e) the second statement follows.
"⇐": If $A = B \oplus \tilde{B}$ with $B \cong \tilde{B}$, then $H := \langle \varphi = \begin{pmatrix} \mathbb{1} & -\mathbb{1} \\ 0 & -\mathbb{1} \end{pmatrix}, \sigma = \begin{pmatrix} 0 & -\mathbb{1} \\ \mathbb{1} & -\mathbb{1} \end{pmatrix} \rangle$ defines a subgroup of $\mathrm{Aut}(A)$ isomorphic to $\mathbb{S}_3$ and makes A into an $\mathbb{S}_3$-module. Let (a, b) be a fixed point of σ. Then $a = b^{-1}$, $b = a \cdot b^{-1}$ and therefore $b^3 = 1$. This shows that $a = b = 1$ and by lemma 23 one has $G := H \ltimes A \in \mathbb{M}$.
Uniqueness: If τ is any fixed point free automorphism of an abelian group of order 3, then $\tau^3 - 1 = 0$ and $\tau - 1$ is an automorphism. Therefore $\tau + \tau^{-1} = -1$. Because of lemma 11 (c) it is sufficient to show the following: Let $\varphi, \tilde{\varphi}, \sigma, \tilde{\sigma}$ be automorphisms of the abelian group A such that there are subgroups $B, \tilde{B}$ of A with $A = B \oplus B^\sigma = \tilde{B} \oplus \tilde{B}^{\tilde{\sigma}}$. Let $\begin{pmatrix} \mathbb{1} & -\mathbb{1} \\ 0 & -\mathbb{1} \end{pmatrix}$ be the matrix representations of φ and $\tilde{\varphi}$ on the corresponding decompositions and $\begin{pmatrix} 0 & -\mathbb{1} \\ \mathbb{1} & -\mathbb{1} \end{pmatrix}$ the matrix representations of σ and $\tilde{\sigma}$. Then there is an automorphism f of A such that $\tilde{\sigma} \circ f = f \circ \sigma$ and $\tilde{\varphi} \circ f = f \circ \varphi$: By the theorem of Krull-Remak there is an isomorphism $g : B \to \tilde{B}$. Define $f : B \oplus B^\sigma \to \tilde{B} \oplus \tilde{B}^{\tilde{\sigma}} : a \cdot b^\sigma \mapsto a^g \cdot b^{g \cdot \tilde{\sigma}}$. Since all components in the representations of $\varphi, \tilde{\varphi}, \sigma, \tilde{\sigma}$ are central, a calculation similar to that in lemma 17 shows that f is suitable. □

Examples: The groups $G \in \mathbb{G}$ with $G'' = \{1\}$ are C_2 and $\mathbb{D}_A$ for a finite abelian group A of odd order. The following table shows their identification as SmallGroup from [GAP] for some examples.

G'/G''	Id(G)	Id(G')
$\{1\}$	[2,1]	[1,1]
C_3	[6,1]	[3,1]
C_5	[10,1]	[5,1]
C_7	[14,1]	[7,1]
C_9	[18,1]	[9,1]
$C_3 \times C_3$	[18,4]	[9,2]
C_{15}	[30,3]	[15,1]
$C_9 \times C_3$	[54,7]	[27,2]

Table 1: small groups from $\mathbb{G}$

The other tables below show some examples of groups from $\mathbb{G}$ with $G'' \neq \{1\}$. They have been calculated using [GAP] and lemma 23. In the later chapters, it will be counted how often these groups and the groups from table 1 are related to $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ for certain real quadratic number fields K. The tables contain all groups of $\mathbb{G}$ up to order 2000 where G/G' is isomorphic to a group in $\{C_3, C_5, C_7, C_9, C_3 \times C_3, C_{15}, C_9 \times C_3\}$. As mentioned before, the classification of the modules from $\mathbb{M}$ would give a more extensive description of the groups from $\mathbb{G}$ (at least in the case that $(G' : G'')$ and $|G''|$ are coprime), but it is not useful to work with this description and only the groups in the following tables occur often enough in the number field context. $\mathrm{Id}(G)$ respectively $\mathrm{Id}(G')$ again denotes the identification as SmallGroup according to [GAP] and Ker the kernel of the action of G'/G'' on G''. Let U be a subgroup of G/G'' which is contained in G'/G'', and x an involution of G outside G'. Then $\tilde{C}(U)$ denotes the isomorphism class of the group $C(\langle \hat{U}, x \rangle)$, where U is the subgroup of G with $G'' \leq \hat{U} \leq G'$ corresponding to U. The question mark in the $\mathrm{Id}(G)$-column indicates that there is no identification as SmallGroup in [GAP] for the corresponding group.

G'/G''	G''	$\mathrm{Id}(G)$	$\mathrm{Id}(G')$
C_3	$C_2 \times C_2$	[24,12]	[12,3]
C_3	$C_4 \times C_4$	[96,64]	[48,3]
C_3	C_2^4	[96,227]	[48,50]
C_3	$C_5 \times C_5$	[150,5]	[75,2]
C_3	$C_7 \times C_7$	[294,7]	[147,5]
C_3	$C_8 \times C_8$	[384,568]	[192,3]
C_3	$(C_4 \times C_2)^2$	[384,18123]	[192,1020]
C_3	C_2^6	[384,20164]	[192,1541]
C_3	$C_{10} \times C_{10}$	[600,179]	[300,43]
C_3	$C_{11} \times C_{11}$	[726,5]	[363,2]
C_3	$C_{13} \times C_{13}$	[1014,7]	[507,5]
C_3	$C_{14} \times C_{14}$	[1176,243]	[588,60]
C_3	$C_{16} \times C_{16}$	[1536,408544632]	[768,1083477]
C_3	$(C_8 \times C_2)^2$	[1536,408569052]	[768,1083725]
C_3	C_4^4	[1536,408568994]	[768,1083578]
C_3	$(C_4 \times C_2^2)^2$	[1536,408640850]	[768,1084956]
C_3	C_2^8	[1536,408641062]	[768,1085321]
C_3	$C_{17} \times C_{17}$	[1734,5]	[867,2]
C_3	$C_{19} \times C_{19}$	[2166,15]	[1083,5]
C_3	$C_{20} \times C_{20}$	?	[1200,384]
C_3	$C_{23} \times C_{23}$	[3174,6]	[1587,2]
C_3	$C_{25} \times C_{25}$	?	[1875,16]
C_3	$C_{29} \times C_{29}$	[5046,6]	[2523,2]
C_3	$C_{31} \times C_{31}$	[5766,15]	[2883,5]
C_3	$C_{35} \times C_{35}$	[7350,109]	[3675,18]
C_3	$C_{37} \times C_{37}$	[8214,8]	[4107,5]
C_5	C_2^4	[160,234]	[80,49]
C_5	C_3^4	[810,101]	[405,15]
C_5	$C_{11} \times C_{11}$	[1210,7]	[605,6]
C_5	C_4^4	?	[1280,1116309]

Table 2: small groups from $\mathbb{G}$

G'/G''	G''	Id(G)	Id(G')
C_5	$C_{19} \times C_{19}$	[3610,6]	[1805,2]
C_5	C_2^8	?	[1280,1116356]
C_5	$C_{29} \times C_{29}$	[8410,6]	[4205,2]
C_5	$C_{31} \times C_{31}$	[9610,8]	[4805,6]
C_7	C_2^6	[896,19344]	[448,1394]
C_7	$C_{13} \times C_{13}$	[2366,6]	[1183,2]
C_7	$C_{29} \times C_{29}$	[11774,8]	[5887,7]

Table 2: small groups from $\mathbb{G}$

G'/G''	G''	Id(G)	Id(G')	Ker	$\tilde{C}(C_3)$
C_9	$C_2 \times C_2$	[72,15]	[36,3]	C_3	C_2
C_9	$C_4 \times C_4$	[288,67]	[144,3]	C_3	C_4
C_9	C_2^4	[288,836]	[144,111]	C_3	C_2^2
C_9	$C_5 \times C_5$	[450,11]	[225,3]	C_3	C_5
C_9	$C_7 \times C_7$	[882,17]	[441,7]	C_3	C_7
C_9	$C_8 \times C_8$	[1152,153931]	[576,3]	C_3	C_8
C_9	$(C_4 \times C_2)^2$	[1152,154457]	[576,1445]	C_3	$C_4 \times C_2$
C_9	C_2^6	[1152,157450]	[576,8266]	C_3	C_2^3
C_9	C_2^6	[1152,157853]	[576,8661]	{1}	{1}
C_9	$C_{10} \times C_{10}$	[1800,301]	[900,66]	C_3	C_{10}
C_9	$C_{11} \times C_{11}$	[2178,12]	[1089,3]	C_3	C_{11}
C_9	$C_{13} \times C_{13}$	[3042,18]	[1521,7]	C_3	C_{13}
C_9	$C_{14} \times C_{14}$	?	[1764,91]	C_3	C_{14}
C_9	$C_{17} \times C_{17}$	[5202,12]	[2601,4]	C_3	C_{17}
C_9	$C_{17} \times C_{17}$	[5202,21]	[2601,6]	{1}	{1}
C_9	$C_{19} \times C_{19}$	[6498,27]	[3249,9]	C_3	C_{19}
C_9	$C_{19} \times C_{19}$	[6498,59]	[3249,15]	{1}	{1}
C_9	$C_{35} \times C_{35}$	[22050,225]	[11025,30]	C_3	C_{35}

Table 3: small groups from $\mathbb{G}$

Because a page is small the next table uses the elementary divisor notation for abelian groups (e.g. $[4,2,2]$ for $C_4 \times C_2 \times C_2$) and the last four columns give $\tilde{C}(U_1)$, $\tilde{C}(U_2)$, $\tilde{C}(U_3)$ and $\tilde{C}(U_4)$, where U_1, U_2, U_3 and U_4 are the proper subgroups between G'' and G'.

G'/G''	G''	Id(G)	Id(G')	Ker	$\tilde{C}$	$\tilde{C}$	$\tilde{C}$	$\tilde{C}$
$C_3 \times C_3$	$C_2 \times C_2$	[72,43]	[36,11]	C_3	[2]	[]	[]	[]
$C_3 \times C_3$	$C_4 \times C_4$	[288,401]	[144,68]	C_3	[4]	[]	[]	[]
$C_3 \times C_3$	C_2^4	[288,1026]	[144,184]	{1}	[2]	[2]	[]	[]
$C_3 \times C_3$	C_2^4	[288,1036]	[144,194]	C_3	[2,2]	[]	[]	[]
$C_3 \times C_3$	$C_5 \times C_5$	[450,21]	[255,5]	C_3	[5]	[]	[]	[]
$C_3 \times C_3$	$C_7 \times C_7$	[882,39]	[441,12]	C_3	[7]	[]	[]	[]
$C_3 \times C_3$	C_8^2	[1152,154139]	[576,1070]	C_3	[8]	[]	[]	[]
$C_3 \times C_3$	$(C_4 \times C_2)^2$	[1152,155474]	[576,5127]	{1}	[4]	[2]	[]	[]

Table 4: small groups from $\mathbb{G}$

G'/G''	G''	Id(G)	Id(G')	Ker	$\tilde{C}$	$\tilde{C}$	$\tilde{C}$	$\tilde{C}$
$C_3 \times C_3$	$(C_4 \times C_2)^2$	[1152,157128]	[576,7440]	C_3	[4,2]	[]	[]	[]
$C_3 \times C_3$	C_2^6	[1152,157861]	[576,8663]	{1}	[2,2]	[2]	[]	[]
$C_3 \times C_3$	C_2^6	[1152,157862]	[576,8664]	{1}	[2]	[2]	[2]	[]
$C_3 \times C_3$	C_2^6	[1152,157874]	[576,8678]	C_3	[2,2,2]	[]	[]	[]
$C_3 \times C_3$	$C_{10} \times C_{10}$	[1800,579]	[900,98]	{1}	[5]	[2]	[]	[]
$C_3 \times C_3$	$C_{10} \times C_{10}$	[1800,691]	[900,141]	C_3	[10]	[]	[]	[]
$C_3 \times C_3$	$C_{11} \times C_{11}$	[2178,23]	[1089,5]	C_3	[11]	[]	[]	[]
$C_3 \times C_3$	$C_{13} \times C_{13}$	[3042,57]	[1521,12]	C_3	[13]	[]	[]	[]
$C_3 \times C_3$	$C_{14} \times C_{14}$	?	[1764,167]	{1}	[7]	[2]	[]	[]
$C_3 \times C_3$	$C_{14} \times C_{14}$	?	[1764,219]	C_3	[14]	[]	[]	[]
$C_3 \times C_3$	$C_{17} \times C_{17}$	[5202,26]	[2601,7]	C_3	[17]	[]	[]	[]
$C_3 \times C_3$	$C_{19} \times C_{19}$	[6498,86]	[3249,21]	C_3	[19]	[]	[]	[]
$C_3 \times C_3$	$C_{35} \times C_{35}$	[22050,304]	[11025,35]	{1}	[7]	[5]	[]	[]
$C_3 \times C_3$	$C_{35} \times C_{35}$	[22050,427]	[11025,39]	C_3	[35]	[]	[]	[]

Table 4: small groups from $\mathbb{G}$

G'/G''	G''	Id(G)	Id(G')	Ker	$\tilde{C}(C_3)$	$\tilde{C}(C_5)$
C_{15}	$C_2 \times C_2$	[120,38]	[60,9]	C_5	[]	[2]
C_{15}	$C_4 \times C_4$	[480,258]	[240,32]	C_5	[]	[4]
C_{15}	C_2^4	[480,1201]	[240,204]	C_5	[]	[2,2]
C_{15}	C_2^4	[480,1195]	[240,199]	C_3	[2,2]	[]
C_{15}	$C_5 \times C_5$	[750,27]	[375,6]	C_5	[]	[5]
C_{15}	$C_7 \times C_7$	[1470,14]	[735,5]	C_5	[]	[7]
C_{15}	$C_8 \times C_8$	[1920,237224]	[960,216]	C_5	[]	[8]
C_{15}	$(C_4 \times C_2)^2$	[1920,239647]	[960,9667]	C_5	[]	[4,2]
C_{15}	C_2^6	[1920,240395]	[960,11366]	{1}	[2,2]	[2]
C_{15}	C_2^6	[1920,240413]	[960,11390]	C_5	[]	[2,2,2]
C_{15}	C_3^4	?	[1215,69]	C_3	[3,3]	[]
C_{15}	$C_{10} \times C_{10}$	?	[1500,166]	C_5	[]	[10]
C_{15}	$C_{11} \times C_{11}$	[3630,42]	[1815,6]	C_3	[11]	[]
C_{15}	$C_{11} \times C_{11}$	[3630,45]	[1815,8]	C_5	[]	[11]
C_{15}	$C_{13} \times C_{13}$	[5070,32]	[2535,6]	C_5	[]	[13]
C_{15}	$C_{14} \times C_{14}$	?	[2940,174]	C_5	[]	[14]
C_{15}	$C_{17} \times C_{17}$	[8670,12]	[4335,3]	C_5	[]	[17]
C_{15}	$C_{19} \times C_{19}$	[10830,19]	[5415,5]	C_3	[19]	[]
C_{15}	$C_{19} \times C_{19}$	[10830,40]	[5415,8]	C_5	[]	[19]

Table 5: small groups from $\mathbb{G}$

Let x, y denote generators of $G'/G'' \cong C_9 \times C_3$ of order 9 and 3. One can choose them in such a way (for every group a new choise) that the kernel of the action of G'/G'' on G'' is always contained in $\left\{\{1\}, \langle y\rangle, \langle x^3\rangle, \langle x\rangle, \langle x^3, y\rangle\right\}$. In the following table $G'/G'' \cong C_9 \times C_3$.

G''	Id(G)	Id(G')	Ker	C($\langle x^3, y\rangle$)	C($\langle x\rangle$)	$\tilde{C}(\langle xy\rangle)$	$\tilde{C}(\langle xy^2\rangle)$
$C_2 \times C_2$	[216,93]	[108,18]	$\langle x\rangle$	[]	[2]	[]	[]
$C_2 \times C_2$	[216,94]	[108,20]	$\langle x^3, y\rangle$	[2]	[]	[]	[]
$C_4 \times C_4$	[864,696]	[432,99]	$\langle x\rangle$	[]	[4]	[]	[]
$C_4 \times C_4$	[864,700]	[432,101]	$\langle x^3, y\rangle$	[4]	[]	[]	[]
C_2^4	[864,3994]	[432,525]	$\langle x^3\rangle$	[]	[2]	[2]	[]
C_2^4	[864,3995]	[432,524]	$\langle x^3\rangle$	[2]	[2]	[]	[]
C_2^4	[864,4020]	[432,551]	$\langle x\rangle$	[]	[2,2]	[]	[]
C_2^4	[864,4021]	[432,553]	$\langle x^3, y\rangle$	[2,2]	[]	[]	[]
$C_5 \times C_5$	[1350,44]	[675,8]	$\langle x\rangle$	[]	[5]	[]	[]
$C_5 \times C_5$	[1350,45]	[675,10]	$\langle x^3, y\rangle$	[5]	[]	[]	[]
$C_7 \times C_7$	?	[1323,39]	$\langle x\rangle$	[]	[7]	[]	[]
$C_7 \times C_7$	?	[1323,41]	$\langle x^3, y\rangle$	[7]	[]	[]	[]
$C_8 \times C_8$	?	[1728,1285]	$\langle x\rangle$	[]	[8]	[]	[]
$C_8 \times C_8$	?	[1728,1289]	$\langle x^3, y\rangle$	[8]	[]	[]	[]
$(C_4 \times C_2)^2$	?	[1728,12470]	$\langle x^3\rangle$	[2]	[4]	[]	[]
$(C_4 \times C_2)^2$	?	[1728,12471]	$\langle x^3\rangle$	[]	[4]	[2]	[]
$(C_4 \times C_2)^2$	?	[1728,12474]	$\langle x^3\rangle$	[4]	[2]	[]	[]
$(C_4 \times C_2)^2$	?	[1728,18304]	$\langle x\rangle$	[]	[4,2]	[]	[]
$(C_4 \times C_2)^2$	?	[1728,18316]	$\langle x^3, y\rangle$	[4,2]	[]	[]	[]
C_2^6	?	[1728,46126]	$\langle x^3\rangle$	[2,2]	[2]	[]	[]
C_2^6	?	[1728,46127]	$\langle x^3\rangle$	[2]	[2,2]	[]	[]
C_2^6	?	[1728,46128]	$\langle x^3\rangle$	[]	[2,2]	[2]	[]
C_2^6	?	[1728,46133]	$\langle x^3\rangle$	[2]	[2]	[2]	[]
C_2^6	?	[1728,46134]	$\langle x^3\rangle$	[]	[2]	[2]	[2]
C_2^6	?	[1728,46176]	$\langle x\rangle$	[]	[2,2,2]	[]	[]
C_2^6	?	[1728,46178]	$\langle x^3, y\rangle$	[2,2,2]	[]	[]	[]
C_2^6	?	[1728,47903]	$\langle y\rangle$	[]	[]	[]	[]

Table 6: small groups from $\mathbb{G}$

Corollary. *Two groups G and H from table 1-6 are isomorphic if and only if $G'/G'' \cong H'/H''$, $H'' \cong G''$ and if there is an isomorphism $f : G/G'' \to H/H''$ such that $\tilde{C}(U) \cong \tilde{C}(f(U))$ for every subgroup $U \leq G'/G''$. If the tables contain a group G, then they contain all groups $H \in \mathbb{G}$ with $G'/G'' \cong H'/H''$ and $H'' \cong G''$.*

Proof. This can be calculated with [GAP]. □

Remark: The fact that G'/G'', G'' and the $\tilde{C}(U)'s$ determine G is not typical for groups from $\mathbb{G}$. The reason is that the G's from the table are so small that the $\mathbb{D}_{G'/G''}$-module G'' has only one indecomposable summand or different indecomposable summands have different kernel of $\mathbb{D}_{G'/G''}$-action.

3.5 The Group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$

Let K be a quadratic number field. This chapter expresses the results from before in terms of number fields. Recall from chapter 2 that K_1 and K_2 denote the first and second

Hilbert class field of a number field K.

Proposition 5. *Let K be a quadratic number field with odd class number. Then the following hold:*

(a) ([No]) If $\mathrm{rk}_p(\mathrm{Cl}(K)) > 1$ for an odd prime p, then $p \mid h_{K_1}$.

(b) The extension $\mathrm{Gal}(K_2/\mathbb{Q})$ of $\mathrm{Gal}(K_2/K_1)$ by $\mathrm{Gal}(K_1/\mathbb{Q})$ splits if and only if $\mathrm{Cl}(K)$ is cyclic.

Proof. Theorem 2 from [No] shows that an odd prime p divides the class number of the p-class field of K, if $\mathrm{rk}_p(\mathrm{Cl}(K)) > 1$. This is statement (a).
Denote $G := \mathrm{Gal}(K_2/\mathbb{Q})$, $H := \mathrm{Gal}(K_2/K)$, $A := \mathrm{Gal}(K_2/K_1)$ and define $U_p \leq H$ to be the normal subgroup of H corresponding to the p-class field of K for an odd prime p. One has $G' = H$ and $H' = A$ by proposition 1. Suppose that the extension from (b) splits. Then lemma 20 together with theorem 2 from [No] shows that $\mathrm{Syl}_p(H/A)$ is cyclic. This holds for all odd primes p and hence $H/A \cong \mathrm{Cl}(K)$ is cyclic. If on the other hand $\mathrm{Cl}(K)$ is cyclic, then $G \in \mathbb{G}$ by definition, and the extension splits by lemma 22. □

Remark: Bond [Bon] proves this proposition for imaginary quadratic number fields. The proof given here is a combination of methods from [C-R2] and [No] and similar to his one.

Let L/F be a Galois extension of number fields and M be the subfield of L_1 containing L such that $\mathrm{Gal}(L_1/M) \cong \mathrm{Cl}_{(L:F)}(L)$. Then M/F is a Galois extension and $\mathrm{Gal}(M/L)$ is a finite $\mathrm{Gal}(L/F)$-module. Define the **non-central coprime Hilbert class field** N of L over F to be the fix field $N = M^G$ by the group $G := \mathrm{Gal}(M/L)^{\mathrm{Gal}(L/F)}$. Then as immediate consequence N/F is Galois and N/L is abelian and unramified. One does not use M to avoid summands of $\mathrm{Cl}_{\neq(L:F)}(F)$ to appear in $\mathrm{Gal}(N/L)$ and by lemma 2.10 using N is the only way to do so. In the notation of Cohen-Lenstra the field N should correspond to the good part of the relative class group $\mathrm{Cl}(L/F)$ (see chapter 4.1).

Let K be a quadratic number field. Then $K_{1,f}$ denotes the non-central coprime Hilbert class field of K over $\mathbb{Q}$ and $K_{2,f}$ denotes the non central coprime Hilbert class field of $K_{1,f}$ over K, which is also called second non-central coprime Hilbert class field of K.

Remark: For every abelian number field L one gets a tower

$$L \leq L_{1,f} \leq L_{2,f} \leq L_{3,f} \leq \cdots$$

this way and one can show (similar as it will be done in proposition 7) that $L_{i,f}/\mathbb{Q}$ is Galois, $\mathrm{Gal}(L_{i,f}/L_{j,f})' \cong \mathrm{Gal}(L_{i,f}/L_{j+1,f})$ and that the extensions

$$\{1\} \to \mathrm{Gal}(L_{k,f}/L_{i,f}) \to \mathrm{Gal}(L_{k,f}/L_{j,f}) \to \mathrm{Gal}(L_{i,f}/L_{j,f}) \to \{1\}$$

are split for all $-1 \leq j < i < k$ with $L_{0,f} := L$ and $L_{-1,f} := \mathbb{Q}$.

Proposition 6. *Let K be a quadratic number field and set $G := \mathrm{Gal}(K_{1,f}/\mathbb{Q})$. Then the following is true:*

(a) $\mathrm{Gal}(K_{1,f}/K) \cong \mathrm{Cl}_{\neq 2}(K)$

(b) $G' = \mathrm{Gal}(K_{1,f}/K)$

(c) $G \cong \mathbb{D}_{\mathrm{Cl}_{\neq 2}(K)}$

(d) $K_{1,f} = K_1$, *if and only if the class number of* K *is odd.*

Proof. This is a consequence of proposition 1 and the definition of $K_{1,f}$. □

Proposition 7. *Let* K *be a quadratic number field and set* $G := \mathrm{Gal}(K_{2,f}/\mathbb{Q})$, *set* $H := \mathrm{Gal}(K_{2,f}/K)$ *and set* $A := \mathrm{Gal}(K_{2,f}/K_{1,f})$. *Then the following is true:*

(a) $K_{2,f}/\mathbb{Q}$ *is a Galois extension of number fields.*

(b) $G' = H$, $G'' = A$, $G''' = \{1\}$.

(c) G *is a factor group of* $\mathrm{Gal}(K_2/\mathbb{Q})$, H *is a factor group of* $\mathrm{Gal}(K_2/K)$ *and* A *is isomorphic to a factor group of* $\mathrm{Gal}(K_2/K_1)$.

(d) $G \in \mathbb{G}$ *and* $(H/A, A) \in \mathbb{M}$.

(e) $\mathrm{Gal}(K_{2,f}/\mathbb{Q}) \cong \mathbb{D}_{\mathrm{Gal}(K_{1,f}/K)} \ltimes \mathrm{Gal}(K_{2,f}/K_{1,f})$ *and* $\mathrm{Gal}(K_{1,f}/K)$ *acts on the group* $\mathrm{Gal}(K_{2,f}/K_{1,f})$ *without any common fixed point (except* 1*).*

(f) The group $\mathrm{Gal}(K_{1,f}/K)$ *is finite abelian and of odd order* n *and the Galois group* $\mathrm{Gal}(K_{2,f}/K_{1,f})$ *is a finite direct sum of groups* $(C_{p^e})^r$, *where* e *is any integer,* p *is a prime not dividing* n *and* r *is any of the integer* $\mathrm{lcm}(2, f_p)$, *where* f_p *is defined by* $f_p := \min_k(p^k \equiv 1(q), k > 0)$ *and* q *runs through the prime divisors of* n. *In particular* $\mathrm{Gal}(K_{2,f}/K_{1,f})$ *is the direct product of two isomorphic abelian groups.*

(g) If L *is another quadratic number field, then* $\mathrm{Gal}(K_{2,f}/K) \cong \mathrm{Gal}(L_{2,f}/L)$ *if and only if* $\mathrm{Gal}(K_{2,f}/\mathbb{Q}) \cong \mathrm{Gal}(L_{2,f}/\mathbb{Q})$.

(h) If $L \neq K$ *is another quadratic number field, then* $K_{2,f} \cap L_{2,f} = \mathbb{Q}$ *(remember from chapter 2 that all number fields are understood to be subfields of a fixed algebraic closure of* $\mathbb{Q}$*).*

(i) If $\mathrm{Cl}(K) \cong C_{p^e}$ *for an odd prime* p, *then* $K_{1,f} = K_1$ *and* $K_{2,f} = K_2$.

(j) If $\mathrm{Cl}(K)$ *is not cyclic or if* h_K *is even, then* $K_{2,f}$ *is a proper subfield of* K_2.

Proof. a: This is true, because $\mathrm{Gal}(K_{2,f}/K_{1,f})$ is also a $\mathrm{Gal}(K_{1,f}/\mathbb{Q})$-module (see argumentation in the proof of lemma 2.10).
b: By lemma 18 and by the definition, one has $H' = A$, $A' = \{1\}$ and $H/A = (G/A)'$, so $H/A = (G'A)/A$, which implies $H = G'A$ and hence $H = G'H'$. Since $H' \leq G'$, this shows $H = G'$.
c: The first two statements of (c) are obvious because $K_{2,f}$ is a subfield of K_2. If $U := \mathrm{Gal}(K_2/K)$ and $N := \mathrm{Gal}(K_2/K_{2,f})$, then $A \cong (U/N)' \cong (U' \cdot N)/N \cong U'/(N \cap U')$ and $U' \cong \mathrm{Gal}(K_2/K_1)$.
d: By (b) one has $G \in \mathbb{G}$ and by lemma 22 one has $(H/A, A) \in \mathbb{M}$.
e: This is a consequence of (d) and lemma 22.
f: This follows from the first corollary to the classification of the modules from $\mathbb{M}$ on page 26.
g: Suppose that $\mathrm{Gal}(K_{2,f}/K) \cong \mathrm{Gal}(L_{2,f}/L)$. Define $B := \mathrm{Gal}(L_{2,f}/L_{1,f})$ and define $U := \mathrm{Gal}(K_{1,f}/K)$. Then by assumption one can choose an isomorphism of groups such that $U \cong \mathrm{Gal}(L_{1,f}/L)$ and therefore the conjugation in $\mathrm{Gal}(K_{1,f}/\mathbb{Q})$ respectively in $\mathrm{Gal}(L_{1,f}/\mathbb{Q})$ makes the abelian groups A and B into $\mathbb{D}_U$-modules. By the assumption and by lemma 26, these modules are conjugate as U-modules according to the notation on page 10. That means, there is an automorphism ϕ of U such that the modules A and

${}^{\phi}B$ are isomorphic as U-modules. Let $x \in \mathbb{D}_{\mathbb{U}} \setminus U$ be an involution and y be any element of U. If one defines $\hat{\phi} \in \mathrm{Aut}(\mathbb{D}_G)$ by $x \mapsto x$ and $y \mapsto \phi(y)$, then ${}^{\phi}B$ is the restriction of the $\mathbb{D}_U$-module ${}^{\hat{\phi}}B$ to U and by lemma 17 one has ${}^{\hat{\phi}}B \cong A$ as $\mathbb{D}_U$-modules. With lemma 26 one gets statement (g).
h: The intersection $M := K_{2,f} \cap L_{2,f}$ is a solvable Galois extension of $\mathbb{Q}$. The maximal abelian subextension of $M/\mathbb{Q}$ is contained in $K \cap L = \mathbb{Q}$ by (b). This implies (h).
i: Since p is odd, one has $K_1 = K_{1,f}$. By assumption $\mathrm{Gal}(K_2/\mathbb{Q}) \in \mathbb{G}$ and by a corollary to lemma 18 one has $p \nmid h_{K_2}$ and therefore $(\mathrm{Cl}(K), \mathrm{Gal}(K_2/K_1)) \in \mathbb{M}$. If N is the central class field of K_1 over K, then also $(\mathrm{Cl}(K), \mathrm{Gal}(N/K_1)) \in \mathbb{M}$, because of lemma 9. This means in particular $\mathrm{Gal}(N/K_1)^{\mathrm{Cl}(K)} = \{1\}$, and hence $N = K_1$ and $K_{2,f} = K_2$.
j: $K_{2,f}$ is a subfield of K_2 by definition. If h_K is even, then by genus theory the factor group $\mathrm{Gal}(K_2/\mathbb{Q})/\mathrm{Gal}(K_2/\mathbb{Q})'$ is not isomorphic to C_2. Hence $K_2 \neq K_{2,f}$ by (b). If $\mathrm{Cl}(K)$ is non cyclic but h_K is odd, then $K_1 = K_{1,f}$ by proposition 6 and by proposition 5 the degrees $(K_{1,f} : K)$ and $(K_2 : K_{1,f})$ are not coprime. But by (d) $(K_{1,f} : K)$ and $(K_{2,f} : K_{1,f})$ are coprime. □

Remark: Statements (f) or (d) do not imply that all such groups occur for a suitable real quadratic number field K. For conjectures concerning this question, see chapter 4.

Proposition 7 lists the important properties of the field extension $K_{2,f}/K$ for a real quadratic number field K. The following lemma and the propositions give information for the computation of $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ for concrete real quadratic number fields. The proposition 8 is a summary of all class group relations from before in the context of the field extension $K_{1,f}/\mathbb{Q}$.

Lemma 27. *Let K be a real quadratic number field and $N \leq K_{1,f}$ be a non Galois subfield. For a number field M, let $\tilde{M}_1$ be the maximal unramified abelian extension of M such that $(\tilde{M}_1 : M)$ is coprime to $n := (K_{1,f} : K)$. Then $\tilde{N}_1 \leq K_{2,f}$.*

Proof. The field N_1 is contained in $(K_{1,f})_1$ and therefore $\tilde{N}_1$ is contained in $(\tilde{K_{1,f}})_1$. The field K_1 is also a subfield of $(\tilde{K_{1,f}})_1$. One may assume that $NK = K_{1,f}$. Define $G := \mathrm{Gal}((\tilde{K_{1,f}})_1/\mathbb{Q})$, $H := \mathrm{Gal}((\tilde{K_{1,f}})_1/K)$ and $A := \mathrm{Gal}((\tilde{K_{1,f}})_1/K_{1,f})$. Then by lemma 2.10 one has the decomposition $A = I_H A \oplus A^H$ of G-modules and by the theorem of Zassenhaus, there is an abelian subgroup U of odd order $n = (K_{1,f} : K)$ such that $H = U \ltimes (A^H \oplus I_H A) = (U \ltimes I_H A) \oplus A^H$. By lemma 18 one has the equation $\mathrm{Gal}((\tilde{K_{1,f}})_1/K_1) = H' = I_H A$ and by definition $\mathrm{Gal}((\tilde{K_{1,f}})_1/K_{2,f}) = A^H$. Because of the remark after proposition 1, there is an involution $x \in G \setminus H$ such that $G = \langle x \rangle \ltimes H$. Since all non Galois subfields of $K_{1,f}$, whose composition with K equals $K_{1,f}$, are conjugate, one may assume that $\langle x, A \rangle$ is the fix group of N in G. If $T_1 = \langle x u_1 a_1 b_1 \rangle, ..., T_r = \langle x u_r a_r b_r \rangle$ with $u_i \in U, a_i \in I_H A, b_i \in A^H$ are the inertia subgroups of the ramified primes of $(\tilde{K_{1,f}})_1/\mathbb{Q}$, then also by that remark $G = \langle T_1, ..., T_r \rangle$. By proposition 1, modulo $I_H A$ the involution x inverts every element of U. Hence $(x u_i a_i b_i)^{(u^{\frac{n-1}{2}})} = x c_i b_i$ for a suitable $c_i \in I_H A$ and $S_i := \langle x c_i b_i \rangle$ is an inertia subgroup of $(\tilde{K_{1,f}})_1/N$. Since elements of A^H commute with elements of U and $I_H A$, one has $A = A^H \cdot I_H A = \langle S_1 I_H A, ..., S_r I_H A \rangle = \langle S_1, ..., S_r \rangle I_H A$. Using lemma 2.10, this implies $A^H \leq \langle S_1, ..., S_r \rangle$ and therefore the maximal unramified extension of N in $(\tilde{K_{1,f}})_1$ is contained in $K_{2,f}$. □

Corollary. *Let K be a real quadratic field, N a non Galois subfield of $K_{1,f}$ and let $\tilde{N}$ be the maximal unramified abelian extension of N such that $(\tilde{N} : N)$ and $(K_{1,f} : K)$ are*

coprime. Let $G := \mathrm{Gal}(K_{2,f}/\mathbb{Q})$ *and* $V := \mathrm{Gal}(K_{2,f}/N)$.
Then $\mathrm{Gal}(K_{2,f}/\tilde{N}) = \langle V', T \cap V \mid T$ *complement of* G' *in* $G\rangle$.

Proof. Since all the complements T of G' in G are conjugate by lemma 22, they all are inertia subgroups in the extension $K_{2,f}/\mathbb{Q}$, because $K_{2,f}/K$ is unramified. Therefore $W := \mathrm{Gal}(K_{2,f}/M) = \langle V', T \cap V \mid T$ complement of G' in $G\rangle$, if M is the maximal unramified abelian extension of N in $K_{2,f}$. By lemma 25 V/W is isomorphic to a subgroup of G'' and so $(V : W)$ is coprime to $(K_{1,f} : K)$. Hence $\tilde{N} = M$. □

Proposition 8. *(see [C-M] chapter 7) Let* K *be a real quadratic number field,* $N \leq K_{1,f}$ *a non Galois subfield such that* $K_{1,f} = N \cdot K$ *and define* $n := (K_{1,f} : K)$. *Then the following hold:*

(a) If $A := \mathrm{Gal}(K_{2,f}/K_{1,f})$, V *is a non normal subgroup of* $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ *containing* A *and* $U := V \cap \mathrm{Gal}(K_{2,f}/K)$, *then* $\mathrm{Cl}_{\neq n}(K_{2,f}^V) \oplus \mathrm{Cl}_{\neq n}(K_{2,f}^V) \cong A^U$.

(b) $\mathrm{Cl}_{\neq n}(N) \oplus \mathrm{Cl}_{\neq n}(N) \cong \mathrm{Gal}(K_{2,f}/K_{1,f})$.

(c) If $H := \mathrm{Gal}(K_{1,f}/K)$ *and* $\sum_{M \leq H} a_M \cdot 1_M^H = 0$ *with* $a_M \in \mathbb{Z}$ *is a relation on induced principal characters and* $L_M \leq K_{1,f}$ *is a non Galois subfield such that* $K \cdot L_M = K_{1,f}^M$, *then* $\bigoplus_{M \leq H} \mathrm{Cl}_{\neq n}(L_M)^{a_M} \cong \{1\}$.

Proof. Since the maximal unramified abelian extension of degree coprime to n of $K_{2,f}^V$ is contained in $K_{2,f}$ by lemma 27, lemma 25 and the corollary to lemma 27 show that $A^V \cong \mathrm{Cl}_{\neq n}(K_{2,f}^V)$ and $A^U \cong A^V \oplus A^V$. This implies (a), and (b) is a special case (a). By lemma 2 one has $\bigoplus_{M \leq H}(A^M)^{a_M} \cong \{1\}$, where A is an H-module in the obvious way. Therefore (a) implies (c). □

Remark: This is a special case of a more general phenomenon which is explained in chapter 7 of [C-M].

Remark: This proposition together with proposition 2 helps to calculate the isomorphism type of the group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ by calculating class groups of certain dihedral number fields (see chapter 5).

Proposition 9. *Let* K *be a real quadratic number field such that* $(K_{2,f} : K_{1,f}) = m^2 > 1$ *and let* M *be one of the fields of degree* $(M : \mathbb{Q}) = m^2$ *such that* $K_{2,f} = M \cdot K_{1,f}$. *Let* $\hat{M}$ *be the Galois closure of* M *over* $\mathbb{Q}$. *Then* $\mathrm{Gal}(\hat{M}/\mathbb{Q}) \cong \mathrm{Gal}(K_{2,f}/\mathbb{Q})/Z(\mathrm{Gal}(K_{2,f}/K))$, M *is totally real and* $d_M = d_K^{\frac{m \cdot (m-1)}{2}}$.

Proof. A field M with $(M : \mathbb{Q}) = m^2$ and $K_{2,f} = M \cdot K_{1,f}$ exists, because of proposition 7. As subfield of $K_{2,f}$ it is totally real and the statement about the Galois group follows by lemma 24. Denote $n := (K_{1,f} : K)$ and let N be a non Galois subfield of $K_{1,f}$ such that $K_{1,f} = K \cdot N$. Since $(\mathrm{Gal}(K_{1,f}/K), \mathrm{Gal}(K_{2,f}/K_{1,f})) \in \mathbb{M}$, the group $G := \mathrm{Gal}(K_{2,f}/N)$ has the structure described in lemma 21, because of lemma 11a and lemma 12. If $\tilde{N}$ denotes the maximal abelian unramified extension of N such that $(\tilde{N} : N)$ is coprime to n and T a subfield of $K_{2,f}$ of index 2 containing $\tilde{N}$, then $d_T^2 \cdot d_{K\tilde{N}} = d_{\tilde{N}}^2 \cdot d_{K_{2,f}}$ by lemma 21 and lemma 8. Because of the ramification, $d_{K\tilde{N}} = d_K^{m \cdot n}$ and $d_{\tilde{N}} = d_N^m$ and by proposition 2, one has $d_N = d_K^{\frac{n-1}{2}}$. Hence $\frac{d_{K_{2,f}}}{d_T^2} = d_K^{-m}$. If $\tilde{T}$ is a subfield of $K_{2,f}$ of index 2 containing

M, then by lemma 8 and lemma 6 one has $\frac{d_{K_{2,f}}}{d_{\tilde{T}}^2} \cdot d_{KM} = d_M^2$. The extension KM/K is unramified, therefore $d_{KM} = d_K^{m \cdot m}$ and since all subfields of $K_{2,f}$ of index 2 are conjugate by lemma 22, one has $d_T = d_{\tilde{T}}$ and hence $d_M^2 = d_K^{m \cdot (m-1)}$. □

Remark: This proposition is the analogue for $K_{2,f}$ of one direction of proposition 2. I suppose the other direction holds true, too. A theorem from [Ko] for example implies that if K is a real quadratic number field and M a field of degree 4 with $d_M = d_K$, then the Galois closure $\hat{M}$ is an unramified extension of K and $\mathrm{Gal}(\hat{M}/K) \cong \mathbb{A}_4$.

4 The Heuristic

The aim of this chapter is to give conjectures not theorems. The first part recalls the Cohen-Lenstra heuristic ([C-L]), its generalization by Cohen-Martinet [C-M]) and a conjecture of Malle ([M2]) which tries to describe the behavior of the p-parts of the class groups for some primes which seem to be bad for the Cohen-Lenstra heuristic by numerical data. The second part gives a conjecture for the distribution of the groups $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic number fields which is based on the heuristics mentioned above and needs some further (not proven) assumptions. As defined in chapter 2 every number field is supposed to be a subfield of one fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

4.1 Cohen Lenstra Heuristic

The following **notations** are needed (see [C-L], [M2]). Let n, k be positive integers. Then

$$(n)_k := \prod_{i=1}^{k} (1 - n^{-i})$$

and

$$(n)_\infty := \prod_{i=1}^{\infty} (1 - n^{-i}).$$

If $\mathcal{K}$ is a set of number fields (all contained in one fixed algebraic closure) and $f : \mathcal{K} \to \mathbb{R}$ is any map, then the **density function** $d(f) : \mathbb{N}_{\geq n_0} \to \mathbb{R}$ is a map depending on $\mathcal{K}$ and f which is defined by

$$x \mapsto \frac{\sum_{K \in \mathcal{K}, |d_K| \leq x} f(K)}{|\{K \in \mathcal{K} \mid x \geq |d_K|\}|}$$

and the **density** of $\mathcal{M}(f)$ is defined by

$$\mathcal{M}(f) = \lim_{x \to \infty} d(f)(x),$$

if it exists. The integer n_0 has technical reason and shall avoid zero denominator. An important type of functions are characteristic functions $\chi_{\{P(K)\}}$ for a property P of number fields. This is defined as follows:

$$\chi_{\{P(K)\}} = \begin{cases} 1, \, K \textit{ fulfills } P \\ 0, \, \textit{else} \end{cases}$$

A **situation** $\Sigma = (G, e, K_0, \sigma)$ consists of a transitive permutation group G of degree $n \geq 2$, a central idempotent e of $\mathbb{Q}G$ which is orthogonal to $\frac{1}{|G|} \sum_{g \in G} g$, a number field K_0 and a signature σ, which may occur as signature of an extension K/K_0 of number fields such that $\mathrm{Gal}(\hat{K}/K_0)$ is permutation isomorphic to G. The field $\hat{K}$ denotes the Galois closure of K over K_0 here. The set $\mathcal{K}(\Sigma)$ denotes the set of all number fields K (contained in a fixed algebraic closure of K_0) which are extensions of K_0 with permutation group G and signature σ of K/K_0. If G is just a group, then this implies $\hat{K} = K$. To every situation one can attach a finite set S of **bad primes** and for every central irreducible summand e' of e over $\mathbb{Q}$ a rational number (in general not an integer) u' the **unit ranks**. How S and the u' are calculated is described in [C-M] chapter 6. Just the following situations are

needed here: $K_0 = \mathbb{Q}$ and K/K_0 is a totally real Galois extension with Galois group G isomorphic to C_2 or $\mathbb{D}_H$ for a finite abelian group H of odd order. In the $C_2 = \langle g \rangle$-case $e = \frac{1}{2} - \frac{g}{2}$ and otherwise $e = 1 - \frac{1}{|H|}(\sum_{g \in H} g)$. One always has $u' = 1$ and the set of bad primes are the primes which divide the order of G.

Remark: In the second case there are no group theoretic reasons why 2 should be bad (see [C-M]), but the existence of p-th roots of unity in K_0 makes the prime p bad, see [M2].

As defined before the class group of an algebraic number field K is the factor group of the group of fractional ideals of the ring of integers $\mathcal{O}_K$ by the principal fractional ideals of $\mathcal{O}_K$. In theory the computation of class groups is easy (essentially one just calculates relations between the classes of all integral ideals with norm up to a certain bound depending on the number field by principal ideal tests). But it is difficult to answer any interesting **questions about the distribution** of class groups. Only little is known about the distribution of class groups of number field and the following list gives some examples of results for quadratic number fields.

- Every integer occurs as 2-rank of the class group of a quadratic number fields (well known by genus theory; see [Na], page 447).
- Every integer occurs as divisor of the class number of a suitable real quadratic number field (see [Y], page 66).
- Every abelian group occurs at most a finite number of times as class group of an imaginary quadratic number field (by the Brauer-Siegel theorem; see [Na], page 434). For example $h_K = 1$ exactly for those imaginary quadratic fields K whose discriminant d_K is contained in $\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$.
- The theory of Davenport-Heilbronn allows some statements about the distribution of 3-class groups of quadratic number fields (see [D-H]).
- Let r be any integer, $\mathrm{rk}_4(A)$ the 4-rank of the finite abelian group A (e.g. the number of elementary divisors of A which are divisible by 4) and $f : \mathcal{K} \to \mathbb{R}$ be the map defined by $f(K) = \chi_{\{\mathrm{rk}_4(\mathrm{Cl}(K))=r\}}$. Then

$$\mathcal{M}(f) = 2^{-r^2} \cdot \frac{(2)_\infty}{((2)_r)^2},$$

  if $\mathcal{K}$ is the set of imaginary quadratic number fields, and

$$\mathcal{M}(f) = 2^{-r(r+1)} \cdot \frac{(2)_\infty}{(2)_r \cdot (2)_{r+1}},$$

  if $\mathcal{K}$ is the set of real quadratic number fields (see [F-K] theorem 3).

But for most abelian groups A it is unknow how $\mathcal{M}(\chi_{\{\mathrm{Cl}(K) \cong A\}})$ looks like, even in the case where $\mathcal{K}$ is the set of real quadratic number fields. For example it is unknown if there are infinitely many real quadratic number fields K with class number 1 (e.g. K such that $\mathcal{O}_K$ is a unique factorization domain).

If $\mathcal{K}$ is the set of all number fields which belong to a situation and $f : \mathcal{K} \to \mathbb{R}$ a "nice" map (see [C-M] chapter 5) just depending on the class group of $K \in \mathcal{K}$ (and some module structure on it), then the **Cohen-Lenstra heuristic** ([C-L]) is a conjecture which suggests values for $\mathcal{M}(f)$. A particular example is the following conjecture:

For a finite set S of primes $\mathbb{Z}^S$ **denotes** the smallest localization of $\mathbb{Z}$ such that all the elements of S becomes units and for an extension of number fields K/K_0 with Galois closure $\hat{K}$ of K over K_0 the group $\mathrm{Cl}(\hat{K}/K_0)$ denotes the relative class group of $\hat{K}/K_0$. This is the kernel of the norm map from $\mathrm{Cl}(\hat{K})$ to $\mathrm{Cl}(K_0)$. Its subgroups $\mathrm{Cl}_p(\hat{K}/K_0)$ and $\mathrm{Cl}^S(\hat{K}/K_0)$ are the p-Sylow subgroup and largest subgroup of order coprime to all elements from S.

Conjecture 1. *([C-M] chapter 6) Let $\Sigma = (G, e, K_0, \sigma)$ be a situation with unit rank $\underline{u} = (u_1, ..., u_m)$ and set of bad primes S. Let A_p be any finite $e\mathbb{Z}_{\langle p\rangle}G$-module, A any finite $e\mathbb{Z}^SG$-module and $f_p, f : \mathcal{K}(\Sigma) \to \mathbb{R}$ be maps defined by $f_p(K) = \chi_{\{e\mathrm{Cl}_p(\hat{K}/K_0)\cong A_p\}}$ and $f(K) = \chi_{\{e\mathrm{Cl}^S(\hat{K}/K_0)\cong A\}}$. Let $e_1, ..., e_m$ be the central irreducible summands of e in $\mathbb{Q}G$ and let*

$$c_p := (\sum_{B/\cong} \frac{1}{|\mathrm{Aut}_G(B)| \cdot \prod_{i=1}^m |e_iB|^{u_i}})^{-1},$$

where the sum runs through all isomorphism classes of finite $e\mathbb{Z}_{\langle p\rangle}G$-modules. Define c by an analogous sum over the isomorphism classes of all finite $e\mathbb{Z}^SG$-modules. Then

$$\mathcal{M}(f_p) = \frac{c_p}{|\mathrm{Aut}_G(A_p)| \cdot \prod_{i=1}^m |e_iA_p|^{u_i}}$$

and

$$\mathcal{M}(f) = \frac{c}{|\mathrm{Aut}_G(A)| \cdot \prod_{i=1}^m |e_iA|^{u_i}}.$$

Remark:

- All the values c_p and c always exist and the c_p are all non zero. The value c is non zero in those situations where all components of the unit rank are positive ([C-M] theorem 5.6 ii).
- The structure of $e\mathrm{Cl}_p(\hat{K}/K_0)$ as $e\mathbb{Z}_{\langle p\rangle}G$-module is not uniquely defined but the conjecture gives the same values for $\mathcal{M}(f)$ for all possibilities.
- One can choose the idempotent e of a situation (G, e, K_0, σ) such that the group $e\mathrm{Cl}_p(\hat{K}/K_0)$ is isomorphic to $\mathrm{Cl}_p(K/K_0)$ ([C-M] chapter 7).
- If $K_0 = \mathbb{Q}$ or K_0 is any number field with class number 1, then $\mathrm{Cl}(K/K_0) = \mathrm{Cl}(K)$.

If $\Sigma = (G, e, K_0, \sigma)$ is a situation conjecture 1 defines a probability distribution pr_p on the countable set of isomorphism classes of all finite $e\mathbb{Z}_{\langle p\rangle}G$-modules. This is called the local **Cohen-Lenstra probability** for the situation Σ. If all components of the unit rank u corresponding to Σ are positive, then this conjecture describes a probability distribution pr on the countable set of isomorphism classes of the finite $e\mathbb{Z}^SG$-modules, the global Cohen-Lenstra probability. A very interesting explanation about the philosophy behind the Cohen-Lenstra probability and connections to other areas of mathematic is contained in chapter 2 of [Len].

The following example from the number field context is not about class groups. But it is easy to calculate, shows the same problems with global probability as the Cohen-Lenstra heuristic and the same automorphism weighting factors.

Example: *Let G, H be non trivial cyclic groups and*

$$a(x, G) = \frac{|\{K \leq \mathbb{Q}(\zeta_p) \mid p \leq x \ \textit{prime}, G \cong \mathrm{Gal}(K/\mathbb{Q})\}|}{|\{K \leq \mathbb{Q}(\zeta_p) \mid p \leq x \ \textit{prime}\}|}.$$

Then

$$\lim_{x\to\infty}\frac{a(x,G)}{a(x,H)}=\frac{|\mathrm{Aut}(H)|}{|\mathrm{Aut}(G)|}\quad \textit{and}\quad \lim_{x\to\infty}a(x,G)=0.$$

Proof. This is an application of Dirichlet's theorem on prime numbers in arithmetic progressions. □

If the global probability does not exist (e.g. the c-value from the conjecture is zero) one can restrict the probability measure to proper σ-subalgebras of the power set of the set of the isomorphism classes of $e\mathbb{Z}^SG$-modules (see [Len] chapter 5). This can be done in a way which includes interesting examples in the number field context.

The conjecture also claims the distribution of the different p-parts of the class groups of number fields to be independent:

Lemma 1. *([C-M]) Let $\Sigma=(G,e,K_0,\sigma)$ be a situation with bad primes S and unit rank u such that the global Cohen-Lenstra probability* pr *exists. Let* pr_p *be the local probabilities and let A be a finite $e\mathbb{Z}^SG$-modules with localizations A_p at the prime $p\in\mathbb{N}$. Then*

$$\mathrm{pr}(\{A\})=\prod_{p\notin S}\mathrm{pr}_p(\{A_p\}).$$

Proof. This is part of [C-M] theorem 3.6. □

For concrete calculations the formulas in conjecture 1 are inconvenient. Therefore:

Lemma 2. *([C-M]) Let $\Sigma=(G,e,\mathbb{Q},\sigma)$ be a situation with bad primes S and unit rank $(u_1,...,u_m)$. Let $e_1,...,e_m$ be the central irreducible summands of e in $\mathbb{Q}G$. For every i let φ_i be one of the Galois conjugate absolute irreducible constituents of the irreducible $\mathbb{Q}$-character corresponding to e_i. Let K_i be the number field of values of φ_i and $h_i:=\deg(\varphi_i)$. Suppose that the rational prime p decomposes in $r_i(p)$ prime ideals with inertia degree $f_i(p)$ in the abelian extension $K_i/\mathbb{Q}$. Assume that all φ_i have Schur index 1 and that all $u_i>0$. Define*

$$c_p=\prod_{i=1}^{m}\Big(\frac{(p^{f_i(p)})_{(h_i\cdot u_i)}}{(p^{f_i(p)})_\infty}\Big)^{r_i(p)}$$

and

$$c=\Big(\prod_{i=1}^{m}\prod_{j=1}^{\infty}\zeta_{K_i}(u_i\cdot h_i+j)\Big)\cdot\prod_{p\in S}c_p^{-1}.$$

Then the following is true:

(i) If A is any finite $e\mathbb{Z}_{\langle p\rangle}$-module and p any prime outside S, then

$$\mathrm{pr}_p(A)=\frac{c_p^{-1}}{|\mathrm{Aut}_G(A)|\cdot\prod_{i=1}^{m}|e_iA|^{u_i}}.$$

(ii) If B is any finite $e\mathbb{Z}^SG$-module, then

$$\mathrm{pr}(B)=\frac{c^{-1}}{|\mathrm{Aut}_G(B)|\cdot\prod_{i=1}^{m}|e_iB|^{u_i}}.$$

Proof. [C-M] proposition 3.10. □

Remark:

- The c-values in this lemma differ from those of conjecture 1.
- The calculations of the denominator for concrete modules can be done with [GAP] and the calculations of the c-values with [PARI].

Examples: This example uses the notation of lemma 2 and gives the numerators of the formulas from this lemma for the global Cohen-Lenstra probability for some example situations, which are needed in the next chapter. In the situation $(C_2 = \langle g \rangle, \frac{1-g}{2}, \mathbb{Q}, totally\ real)$ one has $m = 1$, $S = \{2\}$, $u_1 = 1$ and $c^{-1} \approx 0.7544581722$. The following table gives the corresponding data for some finite abelian groups H of odd order in the situation $(\mathbb{D}_H, 1 - \frac{1}{|H|}(\sum_{g \in H} g), \mathbb{Q}, totally\ real)$. All components of the unit rank equal 1 and:

H	m	S	c^{-1}
C_3	1	$\{2,3\}$	0.9847258786
C_5	1	$\{2,5\}$	0.9962675558
C_7	1	$\{2,7\}$	0.9982325660
C_9	2	$\{2,3\}$	0.9835218667
$C_3 \times C_3$	4	$\{2,3\}$	0.9402891079
C_{15}	3	$\{2,3,5\}$	0.9921182811
$C_9 \times C_3$	7	$\{2,3\}$	0.9368442843

Table 7: c-values for global Cohen-Lenstra probability

Although [C-M] would allow to handle 2 in the $\mathbb{D}_H$ cases as good prime, the 2-parts are believed to behave according to a different distribution which is defined in [M2]. The next conjecture gives a special case of [M2], conjecture 2.1.

Conjecture 2. *([M2]) Let H be a non trivial finite abelian group of odd order, $(G = \mathbb{D}_H, e = 1 - \frac{1}{|H|}(\sum_{g \in H} g), \mathbb{Q}, totally\ real)$ be a situation, A be any finite $e\mathbb{Z}_{\langle 2 \rangle}G$-module and $f : \mathcal{K}(\Sigma) \to \mathbb{R} : K \mapsto \chi_{\{e\mathrm{Cl}_2(K) \cong A\}}$. Let $e_1, ..., e_m$ be the central irreducible summands of e in $\mathbb{Q}G$. For every i let φ_i be one of the Galois conjugate absolute irreducible constituents of the irreducible $\mathbb{Q}$-character corresponding to e_i. Let K_i be the number field of values of φ_i and $\mathcal{O}_i$ its ring of integers. For every prime p dividing 2 in $\mathcal{O}_i$ denote $r_{p,i} := \frac{1}{2} \cdot \dim_{\mathcal{O}_i/p} e_i A/(p \cdot e_i A)$. Let f_i be the inertia degree of 2 in $\mathcal{O}_i$. Let c_i be constants such that*

$$\mathrm{pr}_{2,H,i}(e_i A) = c_i \cdot \prod_{p|2} 2^{f_i \frac{r_{p,i}(r_{p,i}-1)}{2}} \cdot f_i^{r_{p,i}} \cdot \frac{(2^{f_i})_{r_{p,i}+2}}{(2^{f_i})_2} \cdot \frac{1}{|e_i A| \cdot |\mathrm{Aut}_G(e_i A)|}$$

defines a probability distribution on the set of finite $e_i\mathbb{Z}_{\langle 2 \rangle}G$-modules and define

$$\mathrm{pr}_{2,H}(A) := \prod_{i=1}^{m} \mathrm{pr}_{2,H,i}(e_i A).$$

Then $\mathcal{M}(f) = \mathrm{pr}_{2,H}(A)$.

Remark: The formula in [M2] uses $(K_i : \mathbb{Q})^{r_{p,i}}$ instead of $f_i^{r_{p,i}}$ and it contains a misprint: the factor $\prod_{i=1}^{r+u}(p^i-1)$ should be $\prod_{i=u+1}^{r+u}(p^i-1)$. In all the following cases just one prime divides 2 in $\mathcal{O}_i$, therefore in the following cases $r_{p,i} = \frac{1}{2f_i} \cdot \mathrm{rk}_2(e_iA)$ where $\mathrm{rk}_2(e_iA)$ is the 2-rank of e_iA as abelian group. The c_i values can be calculated with theorem 6.1 (ii) from [C-L] and corollary 2.2 from [A].

Examples: Here the notations of the previous conjecture are used.

- If A is a finite $e\mathbb{Z}_{\langle 2\rangle}\mathbb{S}_3$ module and $r = \frac{\mathrm{rk}_2(A)}{2}$, then

$$\mathrm{pr}_{2,C_3}(A) \approx 0.7864170783 \cdot 2^{(r^2-r)/2} \cdot \frac{(2)_{r+2}}{(2)_2} \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{S}_3}(A)|}.$$

- If A is a finite $e\mathbb{Z}_{\langle 2\rangle}\mathbb{D}_5$ module and $r = \frac{\mathrm{rk}_2(A)}{4}$, then

$$\mathrm{pr}_{2,C_5}(A) \approx 0.9596794718 \cdot 2^{r^2} \cdot \frac{(4)_{r+2}}{(4)_2} \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_5}(A)|}.$$

- If A is a finite $e\mathbb{Z}_{\langle 2\rangle}\mathbb{D}_7$ module and $r = \frac{\mathrm{rk}_2(A)}{6}$, then

$$\mathrm{pr}_{2,C_7}(A) \approx 0.9933431984 \cdot 8^{(r^2-r)/2} \cdot 3^r \cdot \frac{(8)_{r+2}}{(8)_2} \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_7}(A)|}.$$

- If e_i is the central irreducible summand of e over $\mathbb{Q}$ which corresponds to the faithful irreducible $\mathbb{Q}\mathbb{D}_9$-module, A is a finite $e_i\mathbb{Z}_{\langle 2\rangle}\mathbb{D}_9$ module and $r = \frac{\mathrm{rk}_2(A)}{6}$, then

$$\mathrm{pr}_{2,C_9,i}(A) \approx 0.9933431984 \cdot 8^{(r^2-r)/2} \cdot 3^r \cdot \frac{(8)_{r+2}}{(8)_2} \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_9}(A)|}.$$

- If e_i is the central irreducible summand of e over $\mathbb{Q}$ which corresponds to the faithful irreducible $\mathbb{Q}\mathbb{D}_{15}$-module, A is a finite $e_i\mathbb{Z}_{\langle 2\rangle}\mathbb{D}_{15}$ module and $r = \frac{\mathrm{rk}_2(A)}{8}$, then

$$\mathrm{pr}_{2,C_{15},i}(A) \approx 0.9989593535 \cdot 4^{r^2} \cdot \frac{(16)_{r+2}}{(16)_2} \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_{15}}(A)|}.$$

4.2 Heuristic for $\mathrm{Gal}(K_{2,f}/K)$

All the conjectures above concern distributions of abelian groups. This chapter looks at the non-abelian case. It proposes a conjecture about the distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic number fields K.

The idea behind this conjecture should allow to describe the distribution of the groups $\mathrm{Gal}(L_{i,f}/L)$ for integers i, where L runs through all number fields of a totally real Galois situation over $\mathbb{Q}$. It works as follows: Set $L_{0,f} := L$. The factor group $\mathrm{Gal}(L_{i,f}/L)$ of $\mathrm{Gal}(L_i/L)$ should be a generalization of the good part of class groups to higher class groups and it is chosen in a way such that $\mathrm{Gal}(L_{i,f}/L_{i-1,f})$ is the good part of the $\mathrm{Gal}(L_{i-1,f}/\mathbb{Q})$-module $\mathrm{Gal}((L_{i-1,f})_1/L_{i-1,f})$ according to Cohen-Martinet. If $H_0 := G_0$, $G_i := \mathrm{Gal}(L_{i,f}/\mathbb{Q})$ and $H_i := \mathrm{Gal}(L_{i,f}/L_{i-1,f}))$, then the G_i-modules $\mathrm{Gal}(L_{i+1,f}/L_{i,f})$ should essentially be distributed as the Cohen-Lenstra heuristic proposes for the situation $(G_i, 1-e, \mathbb{Q}, \textit{totally real})$, where e is the central idempotent of $\mathbb{Q}G_i$ corresponding to $1_{H_i}^{G_i}$.

In the general case the group theory becomes difficult and it is not possible to give numerical calculations. Therefore the following detailed description refers just to the case of real quadratic fields. In this case $K_{1,f}$ is the $2'$-class field of K by proposition 3.6, which is the good part of K_1 according to Cohen-Lenstra. If $G := \mathrm{Gal}(K_{1,f}/\mathbb{Q})$, then $\mathrm{Gal}(M/K_{2,f}) = \mathrm{Gal}(M/K_{1,f})^{G'}$, where M is maximal abelian unramified extension of $K_{1,f}$ such that $(M : K_{1,f})$ is coprime to $(K_{1,f} : K)$ by the definition on page 40. Hence one has the isomorphism of G-modules $\mathrm{Gal}(K_{2,f}/K_{1,f}) \cong e \cdot \mathrm{Cl}^S(K_{1,f})$ where S is the set of prime divisors of $(K_{1,f} : K)$ and $e = 1 - \frac{1}{|(K_{1,f}:K)|}(\sum_{g\in G'} g)$ (see lemma 2.10). The set S is the set of bad primes (according to Cohen-Martinet) of the situation $\Sigma = (G, e, \mathbb{Q}, \textit{totally real})$. The following conjecture supposes that the G-modules $e \cdot \mathrm{Cl}^S(K_{1,f})$, where K runs through the real quadratic number fields, are distributed in the same way as $e \cdot \mathrm{Cl}^S(L)$, where L runs through all fields of $\mathcal{K}(\Sigma)$. In addition it supposes that $e \cdot \mathrm{Cl}^{S\cup\{2\}}(L)$ and $e \cdot \mathrm{Cl}_2(L)$ are distributed according to conjecture 1 and conjecture 2 independently of each other.

Let pr_{quad} be the Cohen-Lenstra probability on finite abelian groups of odd order defined by the situation $(C_2 = \langle g\rangle, \frac{1-g}{2}, \mathbb{Q}, \textit{totally real})$. Let H be any finite non trivial abelian group of odd order, let S_H be the set of primes dividing $|H|$ and let $e_H := 1 - \frac{1}{|H|}(\sum_{g\in H} g)$. Let $\mathrm{pr}_{CL,H}$ be the Cohen-Lenstra probability on finite $e\mathbb{Z}^{S_H\cup\{2\}}\mathbb{D}_H$-modules which belongs to the situation $(\mathbb{D}_H, e_H, \mathbb{Q}, \textit{totally real})$ and $\mathrm{pr}_{2,H}$ the probability distribution of conjecture 2 on finite $e\mathbb{Z}_{\langle 2\rangle}\mathbb{D}_H$-modules for the same situation. If A is any group, set

$$\mathrm{pr}_{2,\{1\}}(A) = \mathrm{pr}_{CL,\{1\}}(A) = \begin{cases} 1, \ A \cong \{1\} \\ 0, \ else \end{cases}$$

Let $\mathbb{G}_0 := \{U \in \mathbb{G} \mid (U' : U''), |U''| \text{ are coprime}\}$ ($\mathbb{G}$ is defined at the beginning of chapter 3.4). If $U \in \mathbb{G}_0$, then U corresponds to a conjugacy class of finite $e_{U'/U''}\mathbb{Z}^{S_{U'/U''}}\mathbb{D}_{U'/U''}$-module structures on U'' by proposition 3.4 (here module structure means module structure up to isomorphm). Let k_U be the size of this conjugacy class. Then the equation

$$\mathrm{pr}_{\mathbb{G}_0}(U) := k_U \cdot \mathrm{pr}_{quad}(U'/U'') \cdot \mathrm{pr}_{2,U'/U''}(U''_2) \cdot \mathrm{pr}_{CL,U'/U''}(U''_{\neq 2})$$

defines a **probability distribution on** $\mathbb{G}_0$ ($\mathrm{pr}_{2,U'/U''}(U''_2)$ and $\mathrm{pr}_{CL,U'/U''}(U''_{\neq 2})$ are independent of the representative of the conjugacy class). Since by proposition 3.7 one has $\mathrm{Gal}(K_{2,f}/\mathbb{Q}) \in \mathbb{G}_0$, $\mathrm{Gal}(K_{2,f}/\mathbb{Q})' = \mathrm{Gal}(K_{2,f}/K)$ and $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ is uniquely determined by $\mathrm{Gal}(K_{2,f}/K)$ the following conjecture could make sense.

Conjecture 3. *Let $U \in \mathbb{G}_0$, let $\mathcal{K}$ be the set of real quadratic number fields and let the map $f : \mathcal{K} \to \mathbb{R}$ be defined by $f(K) = \chi_{\{\mathrm{Gal}(K_{2,f}/K)\cong U'\}}$. Then $\mathcal{M}(f) = \mathrm{pr}_{\mathbb{G}_0}(U)$.*

Remark: (bad case) The part of $\mathrm{Gal}(K_2/K_{1,f})$ which is not coprime to $(K_{1,f} : K)$ is excluded from the considerations as bad part. Proposition 3.5 shows that this part is distributed in a different way. N. Boston, M. Bush and F. Hajir define a probability distribution on certain pro-p-groups which should describe the higher p-class field towers of imaginary quadratic number fields for an odd prime p (see [B-B-H]). It is difficult to calculate higher p-class field towers of real quadratic number fields, so there are almost no numerical data. Those which are available show that under the first 235 real quadratic number fields K with $\mathrm{Cl}(K_1) \cong \mathrm{Cl}(K) \cong C_3 \times C_3$ one has 73 fields with second class group $\mathrm{Gal}(K_2/\mathbb{Q}) \cong \mathrm{SG}(162, 19)$, 97 fields have $\mathrm{Gal}(K_2/\mathbb{Q}) \cong \mathrm{SG}(162, 20)$ and 65 fields have $\mathrm{Gal}(K_2/\mathbb{Q}) \cong \mathrm{SG}(162, 22)$ ($SG(i, j)$ denotes the SmallGroup $[i, j]$ of [GAP]).

Remark: Let $(G, A) \in \mathbb{M}$, let $U := G \ltimes A$ be the semidirect product corresponding to the module structure and let k_U be the number of isomorphism classes of $\mathbb{D}_G$-modules which are conjugate to A. It is an easy calculation with the methods used in lemma 3.26 to show:

$$k_U = \frac{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_G}(A)| \cdot |G| \cdot |\mathrm{Aut}(G)|}{|\mathrm{Aut}(U)|}.$$

Therefore

$$\frac{\mathrm{pr}_{\mathbb{G}_0}(U)}{\mathrm{pr}_{\mathbb{G}_0}(V)} = \frac{|\mathrm{Aut}(V)|}{|\mathrm{Aut}(U)|},$$

if $U, V \in \mathbb{G}_0$ are groups such that $|U''|$ and $|V''|$ are odd and $U'/U'' \cong V'/V''$. But this is just coincidence and gives a wrong idea about $\mathrm{pr}_{\mathbb{G}_0}$.

Remark: It is possible to define something like local parts of the good part of higher class groups. Instead of $K_{1,f}$, one just considers the maximal p extension L of K contained in $K_{1,f}$ and for the second step the maximal q extension in $L_{1,f}$, where p and q are distinct primes and p is odd. But the problem is that the group $\mathrm{Gal}(K_{2,f}/K)$ is not uniquely determined by those local parts. The real quadratic field K with $d_K = 568097$ for example has $\mathrm{Cl}(K) \cong C_{15}$ and $\mathrm{Cl}(K_1) \cong C_2^8$, but all proper immediate fields of K_1/K have class number 1. In the case of imaginary quadratic number fields no global Cohen-Lenstra probability exists and therefore one can also not give a global heuristic for $\mathrm{Gal}(K_{2,f}/K)$ for imaginary quadratic fields K.

In chapter 5.2 conjecture 3 is compared with the number field data (tables 20 to 45). The accordance between both is good for large discriminants (that means $d_K > 10^{14}$ where K is the real quadratic field) if there are many fields and it is not good otherwise. But if there are only few fields, then there is not just variation between the numerical data and the heuristic but also between the distributions in different discriminant areas and if one believes that all the density functions are of type $\sum_{i>0} a_i \cdot x^{b_i} \cdot \log(x)^{c_i}$ with real a_i and rational b_i, c_i such that $x^{b_{i+1}} \cdot \log(x)^{c_{i+1}} = o(x^{b_i} \cdot \log(x)^{c_i})$ for $x \to \infty$, one also should believe that small discriminants do not tell the truth. For small discriminants especially groups with high rank occur less frequently.

5 Tables

The previous chapter describes unproven conjectures. Instead of a proof, this chapter gives numerical data which may give a hint that the conjectures are correct. Chapter 5.1 describes how the numerical data has been computed and in chapter 5.2 the result of the computations is compared with the heuristic from before. In many cases one has $K_{2,f} = K_2$. Information about those fields are presented in an internet database at `http://www.mathematik.uni-kl.de/~numberfieldtables/KT_K2Q/doc.html`. Chapter 5.3 explains how to use this database. The program which has been made to construct this database can also create other number field databases. Chapter 5.4 shows how this program works.

5.1 Calculations

This chapter formulates how the group $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ is calculated for a real quadratic number field K. In theory this procedure is simple. At first on computes the Hilbert class field K_1 of K and its subfield $K_{1,f}$. Secondly one computes the class group of $K_{1,f}$ and thirdly one calculates information, which subgroup of $\mathrm{Cl}(K_{1,f})$ corresponds to $K_{2,f}$ and how $\mathrm{Gal}(K_{1,f}/\mathbb{Q})$ acts on $\mathrm{Gal}(K_{2,f}/K_{1,f})$. Basically this is the way the calculation is done in practice and it shows the three problems which occur.

First the calculation of class fields: To avoid these calculations, which are very time consuming, one searches through number field tables for fields, which suitable properties to be contained in the class field of K and calculates $\mathrm{Cl}(K)$, to know if one has found enough fields. The source are the tables from [M1] of totally real number fields N of degree $n = (N : \mathbb{Q})$, such that the Galois closure of N over $\mathbb{Q}$ has Galois group isomorphic to $\mathbb{D}_n$. For $n = 3$ very extensive tables are available, for $n = 9$ and $n = 5$ the tables contain a lot of number fields and a few number fields are in the tables also for $n = 7$. For all other odd n there are (if at all) just examples, not tables. These tables have been calculated by different methods. For $n = 3$ the Belabas algorithm is used. It applies the theory of Davenport-Heilbronn, which relates cubic number fields with binary cubic forms, to enumerate all the fields up to a certain discriminant (see [C] chapter 8). Another method is given by Hunter's theorem ([C] theorem 9.3.1). From this theorem one can deduce effective bounds for the coefficients of normalized polynomials over $\mathbb{Z}$, depending on the degree and discriminant of a number field K, such that there is a primitive element for K, whose minimal polynomial satisfies those bounds (see [C] chapter 9.3). The problem with this method is that the resulting fields almost always have Galois closure $\mathbb{S}_n$. For calculation of dihedral fields of degree 5, Malle used the parametric polynomial

$$X^5 - 2vX^4 - u(5u^2 - 10uv + 4v^2)X^2 + 2u^2(5u - 4v)(u - v)X - 4u^3(u - v)^2 - X^2(X - u)t.$$

The problem of this method is that the parameters of polynomials which generate a number field with small discriminant may be large, such that one does not get complete tables and the incomplete one may show some special behavior. It is also not known if all dihedral number fields of degree 5 are represented by a suitable specialization of this polynomial. Another way of calculating dihedral number fields is given by class field theory and Kummer theory (see [C] chapters 10.1, 10.2). A Galois dihedral extension $\hat{N}$ of $\mathbb{Q}$ is an abelian extension of a quadratic number field K contained in $\hat{N}$ and therefore contained in a ray class field M of K, whose conductor is bounded, depending on the

discriminant $d_{\hat{N}}$ of $\hat{N}$ (M is the Hilbert class field, if one is just interested in such N that $\hat{N}/K$ is unramified, but in [M1] there is no restriction to special ramification). Subfields of M/K can be calculated using Kummer theory. The problem of this method is that it only works for small n in reasonable time.

As consequence of this method in practice the group $\mathrm{Gal}(K_{1,f}/\mathbb{Q})$ is limited to be an abelian group with exponent dividing $9 \cdot 5 \cdot 7$ and the discriminant d_K of the real quadratic field K must be in a region which is covered by the tables from [M1].

The second problem with the calculation is that computing class groups for number fields with large degree or large discriminant is time consuming. With the help of class group relations, one can reduce these calculations to fields of smaller degree. So the cases of $\mathrm{Gal}(K_{1,f}/\mathbb{Q})$ considered in practice reduce to abelian groups of exponent 9, 7, 5 and the group C_{15}.

Since one is interested in tables, just the frequently occurring cases are helpful. This means just the cases, where $\mathrm{Gal}(K_{1,f}/\mathbb{Q}) \in \{C_3, C_5, C_7, C_9, C_3 \times C_3, C_{15}, C_9 \times C_3\}$ and $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ is one of the groups listed in the tables between page 36 and page 39 are considered.

In detail the procedure of calculating $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ for a real quadratic number field, which returns either the description of a group of those tables or the string "other" or the string "can not calculate", works as follows:

1.) Calculate $\mathrm{Cl}(K)$.

2.) If $\mathrm{Cl}_{\neq 2}(K) = \{1\}$, then return C_2.

3.) If $\mathrm{Cl}_{\neq 2}(K) \notin \{C_3, C_5, C_7, C_9, C_3 \times C_3, C_{15}, C_9 \times C_3\}$, then return "can not calculate".

4.) Search in [M1] for all totally real non Galois dihedral number fields $N_1, ..., N_r$ of odd degree $(N_i : \mathbb{Q}) = n_i \mid h_K$ and discriminant $d_{N_i} = d_K^{\frac{n_i - 1}{2}}$.

5.) Set $N = N_1 \cdots N_r$ and set $\hat{N}$ to be the Galois closure of N over $\mathbb{Q}$. If there is no isomorphism $\mathrm{Gal}(\hat{N}/K) \cong \mathrm{Cl}_{\neq 2}(K)$, then return "can not calculate".

6.) Set $n := (N : \mathbb{Q})$ and calculate for all subfields $M \leq N$ such that $\mathrm{Gal}(\hat{M}/K)$ is cyclic the class group $\mathrm{Cl}_{\neq n}(M)$.

7.) Choose a class group relation in $\mathrm{Cl}_{\neq 2}(K)$ according to lemma 3.7 to calculate $\mathrm{Cl}_{\neq n}(N)$ by proposition 3.8 and the results of 6.).

8.) If $\mathrm{Cl}_{\neq n}(N) = \{1\}$ return $\mathbb{D}_{\mathrm{Cl}_{\neq 2}(K)}$, else search in the tables between page 36 and page 39 for a group G with $G'/G'' \cong \mathrm{Cl}_{\neq 2}(K)$, $G'' \cong \mathrm{Cl}_{\neq n}(N) \oplus \mathrm{Cl}_{\neq n}(N)$ and where G fulfills the following condition: There is an isomorphism $f : \mathrm{Gal}(\hat{N}/\mathbb{Q}) \to G/G''$ such that $\mathrm{Cl}_{\neq n}(M) \cong \tilde{C}(f(\mathrm{Gal}(\hat{N}/M)))$ for every subfield M of N such that $\mathrm{Gal}(\hat{M}/K)$ is cyclic.

9.) If 8.) has found a group return it, else return "other".

Proposition 1. *Let K be a real quadratic number field such that this procedure returns the group G (and not one of the strings "other" or "can not calculate").*
Then $G \cong \mathrm{Gal}(K_{2,f}/\mathbb{Q})$.

Proof. If the procedure returns at step 2, then proposition 3.6 proves the statement. Let otherwise N be the field constructed in step 5. By the propositions 3.2 and 3.6 the field $\hat{N}$ equals $K_{1,f}$. By proposition 3.7, the group $H := \mathrm{Gal}(K_{2,f}/\mathbb{Q})$ is from $\mathbb{G}$ and hence $H'/H'' \cong \mathrm{Cl}_{\neq 2}(K) \cong G'/G''$ by proposition 3.6 and $H'' \cong \mathrm{Cl}_{\neq n}(N) \oplus \mathrm{Cl}_{\neq n}(N) \cong G''$ by proposition 3.8. This proposition and lemma 3.25 also imply that there is a group isomorphism $g : \mathrm{Gal}(\hat{N}/\mathbb{Q}) \to H/H''$ such that $\mathrm{Cl}_{\neq n}(M) \cong \tilde{C}(g(\mathrm{Gal}(\hat{N}/M)))$ for every subfield M of N such that $\mathrm{Gal}(\hat{M}/K)$ is cyclic. Hence there is an isomorphism of groups $h : G/G'' \to H/H''$, such that $\tilde{C}(U) \cong \tilde{C}(h(U))$ for every subgroup U of G/G'' contained in G'/G'' such that $(G'/G'')/U$ is cyclic. Therefore $G \cong H$ by the corollary to the tables 1-5 on page 39. □

Remark: The description of this procedure is not detailed enough to call it algorithm and if the tables [M1] contain no information about dihedral extensions of $\mathbb{Q}$ containing the real quadratic field K, then it does not calculate $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$. Therefore the name procedure is used.

This procedure has been implemented in [PARI] and leads to the tables and the database of the next sections. The class group calculation in [PARI] uses discriminant bounds, which depend on the generalized Riemann hypothesis (GRH). Therefore (if GRH fails) the class groups may be larger and the groups calculated here may be just factor groups of $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$.

5.2 Tables

Tables 8 to 19 shall indicate that the groups $\mathrm{Gal}(K_{2,f}/K_{1,f})$ where K runs through all real quadratic number fields such that $\mathrm{Gal}(K_{1,f}/\mathbb{Q}) \cong \mathbb{D}_H$ for a fixed finite abelian group H of odd order are distributed in the same way as the good parts of the class groups corresponding to the idempotent $e_H := 1 - \frac{1}{|H|}(\sum_{g \in H} g)$ of all the totally real fields L with $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{D}_H$. The columns labeled with $1, 2, 3, 4, 5$ show the class group distribution of totally real fields N of degree $|H|$ with Galois group $\mathrm{Gal}(\hat{N}/\mathbb{Q}) \cong \mathbb{D}_H$. Let K be the unique quadratic subfield of $\hat{N}$. The column 1 considers those N with $\hat{N} = K_1$, column 2 those with $\hat{N} = K_{1,f}$ but $\hat{N} \neq K_1$, column 3 those fields where $\hat{N}$ is the maximal unramified abelian extension M of K such that $(M : K)$ is just divisible by the prime divisors of $|H|$ and which do not appear in a previous column, colum 4 those fields where $\hat{N}/K$ is unramified and which do not appear in a previous column, and finally column 5 considers those fields N where $\hat{N}/K$ is not unramified. The fields N in the first 4 columns fulfill $e_H \mathrm{Cl}^S(\hat{N}) \cong \mathrm{Cl}^S(N) \times \mathrm{Cl}^S(N)$ as group where S is the set of primes dividing $|H|$ by proposition 3.8. But this fact is also true for the N in column 5 (see [C-M] chapter 7).

d_N area	number of fields	1	2	3	4	5
up to 10^8	6246698	0.8271	0.8506	0.8410	0.8432	0.8474
about 10^8	1000000	0.8196	0.8401	0.8334	0.8357	0.8374
about 10^9	1000000	0.8103	0.8245	0.8211	0.8241	0.8228
about 10^{10}	1000000	0.8036	0.8136	0.8112	0.8121	0.8112
about 10^{11}	1000000	0.7980	0.8055	0.8033	0.8041	0.8039
about 10^{12}	1000000	0.7937	0.7995	0.7988	0.7966	0.7985
about 10^{13}	1000000	0.7923	0.7963	0.7955	0.7947	0.7945

Table 8: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with 2-class group isomorphic to $\{1\}$

d_N area	number of fields	1	2	3	4	5
about 10^{14}	1000000	0.7895	0.7928	0.7917	0.7931	0.7939
about 10^{15}	1000000	0.7875	0.7911	0.7921	0.7906	0.7921
about 10^{16}	1000000	0.7860	0.7893	0.7879	0.7887	0.7888
about 10^{17}	1000000	0.7886	0.7882	0.7892	0.7888	0.7880

Table 8: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with 2-class group isomorphic to $\{1\}$

d_N area	number of fields	1	2	3	4	5
up to 10^8	6246698	0.1456	0.1275	0.1349	0.1337	0.1313
about 10^8	1000000	0.1507	0.1354	0.1407	0.1397	0.1384
about 10^9	1000000	0.1572	0.1470	0.1497	0.1464	0.1483
about 10^{10}	1000000	0.1612	0.1541	0.1569	0.1540	0.1561
about 10^{11}	1000000	0.1644	0.1597	0.1612	0.1607	0.1609
about 10^{12}	1000000	0.1672	0.1633	0.1640	0.1661	0.1648
about 10^{13}	1000000	0.1692	0.1656	0.1655	0.1673	0.1672
about 10^{14}	1000000	0.1698	0.1681	0.1684	0.1671	0.1665
about 10^{15}	1000000	0.1704	0.1696	0.1673	0.1690	0.1682
about 10^{16}	1000000	0.1722	0.1698	0.1697	0.1706	0.1704
about 10^{17}	1000000	0.1702	0.1711	0.1708	0.1699	0.1708

Table 9: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with 2-class group isomorphic to C_2

d_N area	number of fields	1	2	3	4	5
up to 10^8	6246698	0.0169	0.0150	0.0159	0.0153	0.0143
about 10^8	1000000	0.0181	0.0162	0.0170	0.0161	0.0157
about 10^9	1000000	0.0191	0.0177	0.0177	0.0181	0.0178
about 10^{10}	1000000	0.0197	0.0188	0.0182	0.0192	0.0192
about 10^{11}	1000000	0.0205	0.0196	0.0196	0.0195	0.0200
about 10^{12}	1000000	0.0213	0.0204	0.0206	0.0205	0.0205
about 10^{13}	1000000	0.0207	0.0206	0.0209	0.0208	0.0207
about 10^{14}	1000000	0.0215	0.0211	0.0218	0.0208	0.0212
about 10^{15}	1000000	0.0212	0.0209	0.0219	0.0212	0.0210
about 10^{16}	1000000	0.0217	0.0216	0.0224	0.0216	0.0216
about 10^{17}	1000000	0.0220	0.0213	0.0211	0.0217	0.0215

Table 10: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with 2-class group isomorphic to C_4

d_N area	number of fields	1	2	3	4	5
up to 10^8	6246698	0.0067	0.0042	0.0051	0.0048	0.0044
about 10^8	1000000	0.0076	0.0050	0.0058	0.0056	0.0054
about 10^9	1000000	0.0088	0.0068	0.0075	0.0078	0.0073

Table 11: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with 2-class group isomorphic to $C_2 \times C_2$

d_N area	number of fields	1	2	3	4	5
about 10^{10}	1000000	0.0103	0.0087	0.0088	0.0098	0.0087
about 10^{11}	1000000	0.0113	0.0100	0.0101	0.0103	0.0100
about 10^{12}	1000000	0.0120	0.0110	0.0112	0.0115	0.0108
about 10^{13}	1000000	0.0119	0.0117	0.0121	0.0115	0.0117
about 10^{14}	1000000	0.0124	0.0121	0.0124	0.0126	0.0125
about 10^{15}	1000000	0.0140	0.0122	0.0121	0.0127	0.0126
about 10^{16}	1000000	0.0132	0.0129	0.0134	0.0129	0.0129
about 10^{17}	1000000	0.0129	0.0127	0.0125	0.0131	0.0131

Table 11: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with 2-class group isomorphic to $C_2 \times C_2$

d_N area	number of fields	1	2	3	4	5
up to 10^8	6246698	0.9870	0.9867	0.9871	0.9872	0.9884
about 10^8	1000000	0.9862	0.9861	0.9864	0.9864	0.9875
about 10^9	1000000	0.9855	0.9853	0.9848	0.9857	0.9863
about 10^{10}	1000000	0.9853	0.9853	0.9851	0.9848	0.9857
about 10^{11}	1000000	0.9850	0.9848	0.9847	0.9849	0.9850
about 10^{12}	1000000	0.9846	0.9847	0.9858	0.9847	0.9847
about 10^{13}	1000000	0.9849	0.9849	0.9839	0.9849	0.9845
about 10^{14}	1000000	0.9842	0.9847	0.9846	0.9836	0.9847
about 10^{15}	1000000	0.9848	0.9846	0.9849	0.9852	0.9849
about 10^{16}	1000000	0.9850	0.9845	0.9848	0.9839	0.9845
about 10^{17}	1000000	0.9851	0.9847	0.9845	0.9849	0.9851

Table 12: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with $6'$-class group isomorphic to $\{1\}$

d_N area	number of fields	1	2	3	4	5
up to 10^8	6246698	0.0086	0.0086	0.0085	0.0084	0.0079
about 10^8	1000000	0.0090	0.0089	0.0089	0.0087	0.0084
about 10^9	1000000	0.0094	0.0095	0.0102	0.0092	0.0088
about 10^{10}	1000000	0.0095	0.0095	0.0094	0.0097	0.0093
about 10^{11}	1000000	0.0095	0.0095	0.0095	0.0099	0.0097
about 10^{12}	1000000	0.0098	0.0099	0.0092	0.0098	0.0098
about 10^{13}	1000000	0.0096	0.0097	0.0106	0.0096	0.0101
about 10^{14}	1000000	0.0101	0.0100	0.0102	0.0106	0.0098
about 10^{15}	1000000	0.0101	0.0099	0.0097	0.0096	0.0098
about 10^{16}	1000000	0.0094	0.0100	0.0098	0.0105	0.0102
about 10^{17}	1000000	0.0097	0.0099	0.0098	0.0100	0.0095

Table 13: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with $6'$-class group isomorphic to C_5

d_N area	number of fields	1	2	3	4	5
up to 10^8	6246698	0.0029	0.0030	0.0028	0.0029	0.0025
about 10^8	1000000	0.0030	0.0031	0.0030	0.0029	0.0028
about 10^9	1000000	0.0031	0.0032	0.0031	0.0033	0.0030
about 10^{10}	1000000	0.0034	0.0033	0.0033	0.0037	0.0031
about 10^{11}	1000000	0.0036	0.0035	0.0038	0.0035	0.0034
about 10^{12}	1000000	0.0033	0.0032	0.0030	0.0033	0.0034
about 10^{13}	1000000	0.0034	0.0034	0.0032	0.0034	0.0034
about 10^{14}	1000000	0.0037	0.0033	0.0036	0.0034	0.0034
about 10^{15}	1000000	0.0032	0.0034	0.0033	0.0033	0.0033
about 10^{16}	1000000	0.0035	0.0034	0.0035	0.0034	0.0034
about 10^{17}	1000000	0.0033	0.0032	0.0033	0.0032	0.0034

Table 14: proportion of totally real $\mathbb{S}_3$-fields N of degree 3 with $6'$-class group isomorphic to C_7

d_N area	number of fields	1	2	3	4	5
up to 10^{16}	806309	0.9823	0.9843	0.9833	0.9839	0.9852
10^{16} to 10^{18}	2019477	0.9775	0.9786	0.9779	0.9782	0.9795
about 10^{27}	833458	0.9592	0.9585	0.9587	0.9585	0.9591

Table 15: proportion of totally real $\mathbb{D}_5$-fields N of degree 5 with 2-class group isomorphic to $\{1\}$

d_N area	number of fields	1	2	3	4	5
up to 10^{16}	806309	0.0175	0.0154	0.0165	0.0159	0.0145
10^{16} to 10^{18}	2019477	0.0220	0.0210	0.0216	0.0212	0.0202
about 10^{27}	833458	0.0398	0.0402	0.0400	0.0400	0.0400

Table 16: proportion of totally real $\mathbb{D}_5$-fields N of degree 5 with 2-class group isomorphic to $C_2 \times C_2$

d_N area	number of fields	1	2	3	4	5
up to 10^{16}	806309	0.9966	0.9966	0.9966	0.9962	0.9963
10^{16} to 10^{18}	2019477	0.9962	0.9963	0.9963	0.9960	0.9963
about 10^{27}	833458	0.9963	0.9961	0.9962	0.9959	0.9962

Table 17: proportion of totally real $\mathbb{D}_5$-fields N of degree 5 with $10'$-class group isomorphic to $\{1\}$

d_N area	number of fields	1	2	3	4	5
up to 10^{16}	806309	0.0015	0.0016	0.0016	0.0020	0.0017
10^{16} to 10^{18}	2019477	0.0017	0.0017	0.0017	0.0017	0.0017
about 10^{27}	833458	0.0017	0.0017	0.0017	0.0018	0.0016

Table 18: proportion of totally real $\mathbb{D}_5$-fields N of degree 5 with $10'$-class group isomorphic to C_{11}

d_N area	number of fields	1	2	3	4	5
up to 10^{16}	806309	0.0013	0.0013	0.0013	0.0013	0.0014
10^{16} to 10^{18}	2019477	0.0016	0.0015	0.0015	0.0017	0.0014
about 10^{27}	833458	0.0016	0.0016	0.0015	0.0018	0.0018

Table 19: proportion of totally real $\mathbb{D}_5$-fields N of degree 5 with $10'$-class group isomorphic to $C_3 \times C_3$

The following tables compare conjecture 4.3 with the number field data which has been calculated. If $\mathrm{Gal}(K_{1,f}/K) \cong C_3$ or $\mathrm{Gal}(K_{1,f}/K) \cong C_3 \times C_3$ there are complete number field tables. Therefore the conjecture can be compared with the data directly. This is done in tables 20 to 29. The column "number of fields" shows how many real quadratic fields are in the examined discriminant range. The last four columns show the proportion of quadratic fields K in the corresponding discriminant range with $\mathrm{Gal}(K_{2,f}/K) \cong \mathrm{SG}(i,j)$ where $[i,j]$ is the heading of the column and $\mathrm{SG}(i,j)$ a SmallGroup of [GAP].

d_K area	number of fields	[1,1]	[3,1]	[12,3]	[48,3]
up to 10^8	30396325	7.7275E-1	9.6940E-2	1.5223E-2	1.7819E-3
about 10^8	4774207	7.6873E-1	9.6902E-2	1.6179E-2	1.9337E-3
about 10^9	4645345	7.6373E-1	9.6989E-2	1.7644E-2	2.1314E-3
about 10^{10}	4557478	7.6021E-1	9.7475E-2	1.8689E-2	2.2813E-3
about 10^{11}	4503762	7.5833E-1	9.7381E-2	1.9462E-2	2.3949E-3
about 10^{12}	4459930	7.5673E-1	9.7356E-2	1.9991E-2	2.5079E-3
about 10^{13}	4441829	7.5627E-1	9.7440E-2	2.0363E-2	2.5195E-3
about 10^{14}	4420949	7.5584E-1	9.7377E-2	2.0696E-2	2.5965E-3
about 10^{15}	4397540	7.5505E-1	9.7618E-2	2.0964E-2	2.5869E-3
about 10^{16}	4406448	7.5505E-1	9.7248E-2	2.0979E-2	2.6613E-3
about 10^{17}	4396820	7.5474E-1	9.7540E-2	2.1173E-2	2.6424E-3
conjecture		7.5446E-1	9.7376E-2	2.1301E-2	2.6626E-3

Table 20: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[48,50]	[75,2]	[9,2]	[36,11]
up to 10^8	30396325	5.6142E-4	8.5767E-4	5.1763E-4	3.1895E-4
about 10^8	4774207	6.5959E-4	8.7742E-4	5.6282E-4	3.4205E-4
about 10^9	4645345	8.5419E-4	9.3169E-4	5.6207E-4	4.2107E-4
about 10^{10}	4557478	1.0890E-3	9.3517E-4	6.0143E-4	4.3511E-4
about 10^{11}	4503762	1.2379E-3	9.4166E-4	6.0971E-4	4.8293E-4
about 10^{12}	4459930	1.3657E-3	9.6997E-4	6.1301E-4	5.1481E-4
about 10^{13}	4441829	1.4386E-3	9.5726E-4	6.1168E-4	5.1645E-4
about 10^{14}	4420949	1.4974E-3	9.8848E-4	6.2046E-4	5.2161E-4
about 10^{15}	4397540	1.5395E-3	9.8532E-4	6.4377E-4	5.3917E-4
about 10^{16}	4406448	1.5961E-3	9.7879E-4	6.0911E-4	5.3286E-4
about 10^{17}	4396820	1.5748E-3	9.9117E-4	6.1840E-4	5.2038E-4
conjecture		1.6641E-3	9.7376E-4	6.2809E-4	5.4958E-4

Table 21: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[192,3]	[147,5]	[192,1020]	[300,43]
up to 10^8	30396325	2.1203E-4	2.9556E-4	9.4880E-5	1.2623E-4
about 10^8	4774207	2.3690E-4	3.0309E-4	1.1374E-4	1.4893E-4
about 10^9	4645345	2.6026E-4	3.1193E-4	1.6425E-4	1.6877E-4
about 10^{10}	4557478	2.7669E-4	3.2364E-4	2.0955E-4	1.8168E-4
about 10^{11}	4503762	2.9464E-4	3.4238E-4	2.2803E-4	1.8651E-4
about 10^{12}	4459930	3.0965E-4	3.1301E-4	2.5337E-4	2.0180E-4
about 10^{13}	4441829	3.1046E-4	3.3635E-4	2.7196E-4	2.0239E-4
about 10^{14}	4420949	3.2165E-4	3.3002E-4	2.7664E-4	2.0697E-4
about 10^{15}	4397540	3.3018E-4	3.3974E-4	2.9607E-4	2.0443E-4
about 10^{16}	4406448	3.3996E-4	3.3269E-4	3.0001E-4	2.0810E-4
about 10^{17}	4396820	3.2660E-4	3.1932E-4	3.1682E-4	1.9833E-4
conjecture		3.3283E-4	3.3121E-4	3.1203E-4	2.1301E-4

Table 22: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[144,184]	[363,2]	[588,60]	[144,68]
up to 10^8	30396325	7.3759E-5	7.1160E-5	4.3558E-5	3.7044E-5
about 10^8	4774207	8.8811E-5	6.7027E-5	5.2365E-5	3.9378E-5
about 10^9	4645345	1.0893E-4	7.9004E-5	6.0275E-5	4.6929E-5
about 10^{10}	4557478	1.2222E-4	7.3506E-5	6.1657E-5	5.2880E-5
about 10^{11}	4503762	1.5276E-4	8.1265E-5	7.2384E-5	5.6175E-5
about 10^{12}	4459930	1.6390E-4	8.1391E-5	6.9284E-5	6.2109E-5
about 10^{13}	4441829	1.6705E-4	7.5870E-5	6.6864E-5	6.7315E-5
about 10^{14}	4420949	1.6241E-4	7.8942E-5	7.5323E-5	5.7228E-5
about 10^{15}	4397540	1.8169E-4	8.0500E-5	6.8220E-5	6.2308E-5
about 10^{16}	4406448	1.7066E-4	7.4209E-5	7.4436E-5	7.1486E-5
about 10^{17}	4396820	1.7808E-4	8.9838E-5	6.8913E-5	6.6412E-5
conjecture		1.8033E-4	8.0476E-5	7.2452E-5	6.8698E-5

Table 23: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[192,1541]	[507,5]	[576,5127]	[144,194]
up to 10^8	30396325	2.5661E-6	4.1518E-5	1.7436E-5	1.1087E-5
about 10^8	4774207	5.4459E-6	4.4196E-5	2.2412E-5	1.3615E-5
about 10^9	4645345	9.4718E-6	4.6713E-5	2.5832E-5	2.2603E-5
about 10^{10}	4557478	1.9748E-5	5.0467E-5	3.3791E-5	2.7427E-5
about 10^{11}	4503762	2.3980E-5	4.7738E-5	3.7524E-5	3.1085E-5
about 10^{12}	4459930	3.8341E-5	4.5741E-5	3.5202E-5	3.6772E-5
about 10^{13}	4441829	3.8047E-5	4.8854E-5	3.8047E-5	3.6021E-5
about 10^{14}	4420949	4.0715E-5	4.7275E-5	4.2525E-5	3.9810E-5
about 10^{15}	4397540	4.5025E-5	5.0710E-5	4.4343E-5	4.0932E-5
about 10^{16}	4406448	5.1288E-5	5.0608E-5	3.9261E-5	4.0168E-5
about 10^{17}	4396820	5.1856E-5	4.3213E-5	4.7534E-5	3.7300E-5

Table 24: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[192,1541]	[507,5]	[576,5127]	[144,194]
conjecture		5.7576E-5	4.8016E-5	4.5083E-5	4.2936E-5

Table 24: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[768,1083477]	[768,1083725]	[576,8663]	[1200,384]
up to 10^8	30396325	2.3950E-5	1.1218E-5	4.9677E-6	1.4245E-5
about 10^8	4774207	2.6392E-5	1.3405E-5	5.4459E-6	1.8432E-5
about 10^9	4645345	2.9061E-5	1.8298E-5	1.3347E-5	2.1957E-5
about 10^{10}	4557478	3.6424E-5	2.6769E-5	1.2946E-5	2.1503E-5
about 10^{11}	4503762	4.0411E-5	3.0419E-5	1.6875E-5	2.1760E-5
about 10^{12}	4459930	3.9014E-5	3.0494E-5	2.0180E-5	2.6458E-5
about 10^{13}	4441829	4.0299E-5	2.9492E-5	2.7466E-5	2.2964E-5
about 10^{14}	4420949	4.3656E-5	3.2798E-5	2.3298E-5	2.6917E-5
about 10^{15}	4397540	3.9568E-5	3.9795E-5	2.8425E-5	2.9562E-5
about 10^{16}	4406448	4.1530E-5	3.3814E-5	2.7460E-5	2.7687E-5
about 10^{17}	4396820	4.3895E-5	4.1848E-5	2.6610E-5	2.8202E-5
conjecture		4.1604E-5	3.9003E-5	2.8177E-5	2.6626E-5

Table 25: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[576,8664]	[255,5]	[867,2]	[900,98]
up to 10^8	30396325	6.5139E-6	1.7469E-5	1.8621E-5	8.1260E-6
about 10^8	4774207	9.6351E-6	2.0946E-5	1.9270E-5	7.9594E-6
about 10^9	4645345	1.3993E-5	1.7006E-5	2.2603E-5	1.0763E-5
about 10^{10}	4557478	1.7992E-5	2.1942E-5	1.7334E-5	9.8739E-6
about 10^{11}	4503762	2.1093E-5	2.1760E-5	2.5090E-5	1.5765E-5
about 10^{12}	4459930	2.1525E-5	2.6682E-5	2.7130E-5	1.5695E-5
about 10^{13}	4441829	2.5440E-5	2.1613E-5	2.1613E-5	1.7785E-5
about 10^{14}	4420949	2.1941E-5	3.0763E-5	1.9679E-5	1.9227E-5
about 10^{15}	4397540	2.6378E-5	2.1830E-5	1.9784E-5	1.4554E-5
about 10^{16}	4406448	2.1786E-5	2.4736E-5	2.4283E-5	1.5205E-5
about 10^{17}	4396820	2.5473E-5	2.6838E-5	2.3426E-5	1.6148E-5
conjecture		2.6298E-5	2.5124E-5	2.1059E-5	1.6487E-5

Table 26: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[1083,5]	[768,10834956]	[576,1070]	[441,12]
up to 10^8	30396325	1.1876E-5	7.2377E-7	4.0136E-6	5.9218E-6
about 10^8	4774207	1.6338E-5	1.0473E-6	3.7703E-6	7.3311E-6
about 10^9	4645345	1.3347E-5	2.1527E-6	4.9512E-6	8.1802E-6
about 10^{10}	4557478	1.2507E-5	3.9496E-6	7.2408E-6	7.2408E-6

Table 27: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[1083,5]	[768,10834956]	[576,1070]	[441,12]
about 10^{11}	4503762	2.0205E-5	5.5509E-6	8.6594E-6	9.3255E-6
about 10^{12}	4459930	1.5023E-5	7.3992E-6	5.6055E-6	6.7266E-6
about 10^{13}	4441829	1.6885E-5	9.4556E-6	5.6283E-6	6.3037E-6
about 10^{14}	4420949	1.4477E-5	1.0631E-5	7.6907E-6	7.4645E-6
about 10^{15}	4397540	1.5236E-5	1.0460E-5	8.4138E-6	1.0915E-5
about 10^{16}	4406448	1.4524E-5	9.7584E-6	9.3045E-6	7.7160E-6
about 10^{17}	4396820	1.2509E-5	1.3646E-5	9.7798E-6	9.3249E-6
conjecture		1.4986E-5	1.2595E-5	8.5872E-6	8.5455E-6

Table 27: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[1587,2]	[576,7440]	[1875,16]	[768,1083578]
up to 10^8	30396325	7.3035E-6	2.3029E-6	5.0993E-6	1.1186E-6
about 10^8	4774207	6.4932E-6	1.8851E-6	5.8648E-6	1.8851E-6
about 10^9	4645345	6.8886E-6	2.7985E-6	8.6108E-6	2.7985E-6
about 10^{10}	4557478	7.2408E-6	5.0467E-6	5.7049E-6	3.5107E-6
about 10^{11}	4503762	7.1052E-6	4.2187E-6	9.1035E-6	4.6628E-6
about 10^{12}	4459930	8.7445E-6	6.7266E-6	9.6414E-6	5.6055E-6
about 10^{13}	4441829	7.8796E-6	4.9529E-6	9.0053E-6	4.0524E-6
about 10^{14}	4420949	8.5954E-6	7.0121E-6	6.3335E-6	6.3335E-6
about 10^{15}	4397540	9.5508E-6	8.8686E-6	7.7316E-6	5.2302E-6
about 10^{16}	4406448	9.5315E-6	7.0351E-6	7.9429E-6	4.5388E-6
about 10^{17}	4396820	8.1877E-6	7.5054E-6	6.1408E-6	5.2311E-6
conjecture		8.3671E-6	8.0505E-6	7.7901E-6	6.5006E-6

Table 28: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

d_K area	number of fields	[900,141]	[2523,2]	[2883,5]	[3675,18]
up to 10^8	30396325	2.3687E-6	2.3358E-6	2.1384E-6	2.0068E-6
about 10^8	4774207	2.9324E-6	3.7703E-6	3.1419E-6	4.3986E-6
about 10^9	4645345	1.2916E-6	4.3054E-6	2.7985E-6	3.0138E-6
about 10^{10}	4557478	3.7301E-6	3.0719E-6	2.8525E-6	3.9496E-6
about 10^{11}	4503762	3.5526E-6	5.1068E-6	3.9967E-6	2.8865E-6
about 10^{12}	4459930	5.3813E-6	3.5875E-6	4.4844E-6	3.8117E-6
about 10^{13}	4441829	5.8534E-6	4.7278E-6	3.1519E-6	3.8273E-6
about 10^{14}	4420949	3.3929E-6	4.2977E-6	2.0358E-6	3.1667E-6
about 10^{15}	4397540	7.5042E-6	3.8658E-6	2.5014E-6	2.2740E-6
about 10^{16}	4406448	6.1274E-6	4.5388E-6	5.2196E-6	3.1772E-6
about 10^{17}	4396820	5.4585E-6	4.0939E-6	3.1841E-6	2.7292E-6
conjecture		5.4958E-6	4.1352E-6	3.3776E-6	3.3121E-6

Table 29: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K in SmallGroup notation of [GAP]

The following tables contain distribution data of the group $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K where $\mathrm{Gal}(K_{1,f}/K) \cong C_5, C_7, C_9, C_{15}, C_9 \times C_3$. Since the number field tables are not complete in these cases they just count the proportion of $\mathrm{Gal}(K_{2,f}/K)$ where K runs through all real quadratic fields with one fixed group $\mathrm{Gal}(K_{1,f}/K)$. Hence the data for the group U' with $U \in \mathbb{G}_0$ is not compared with conjecture 4.3 directly but with $\mathrm{pr}_{\mathbb{G}_0}(U)/\mathrm{pr}_{quad}(U'/U'')$. Apart from that table 30 to 45 have the same structure as table 20. Except in the case $\mathrm{Gal}(K_{1,f}/K) \cong C_5$ the discriminant of K is very small and there are just a few fields in the number field tables, so following tables rather examples.

d_K area	number of fields	[5,1]	[80,49]	[405,15]
up to 10^8	569572	9.8042E-1	1.5921E-2	1.2922E-3
10^8 to 10^9	1414415	9.7468E-1	2.1140E-2	1.5017E-3
about $10^{13.5}$	587974	9.5490E-1	3.9983E-2	1.5494E-3
conjecture		9.5610E-1	3.9215E-2	1.4755E-3

Table 30: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_5$ in SmallGroup notation of [GAP]

d_K area	number of fields	[605,6]	[1280,1116309]	[1805,2]
up to 10^8	569572	1.5801E-3	2.2824E-4	2.7389E-4
10^8 to 10^9	1414415	1.6226E-3	3.2664E-4	3.0189E-4
about $10^{13.5}$	587974	1.6123E-3	6.7010E-4	3.1294E-4
conjecture		1.5803E-3	6.1273E-4	2.9427E-4

Table 31: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_5$ in SmallGroup notation of [GAP]

d_K area	number of fields	[1280,1116356]	[4205,2]	[4805,6]
up to 10^8	569572	2.6336E-5	5.7938E-5	5.4427E-5
10^8 to 10^9	1414415	9.9688E-5	7.2822E-5	6.6459E-5
about $10^{13.5}$	587974	5.7656E-4	8.3337E-5	7.1432E-5
conjecture		3.2551E-4	8.1204E-5	6.6327E-5

Table 32: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_5$ in SmallGroup notation of [GAP]

d_K area	number of fields	[7,1]	[448,1394]	[1183,2]	[5887,7]
up to 10^8	10793	9.9666E-1	1.9457E-3	9.2653E-4	4.6326E-4
conjecture		9.9159E-1	6.6389E-3	1.4668E-3	1.2633E-4

Table 33: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_7$ in SmallGroup notation of [GAP]

d_K area	number of fields	[9,1]	[36,3]	[144,3]
up to about $15 \cdot 10^6$	17133	8.2525E-1	1.3850E-1	1.4825E-2

Table 34: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9$ in SmallGroup notation of [GAP]

d_K area	number of fields	[9,1]	[36,3]	[144,3]
conjecture		7.6831E-1	1.6807E-1	2.1008E-2

Table 34: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9$ in SmallGroup notation of [GAP]

d_K area	number of fields	[144,111]	[225,3]	[576,8661]
up to about $15 \cdot 10^6$	17133	5.0196E-3	6.4204E-3	1.1673E-3
conjecture		1.3130E-2	7.6831E-3	5.1349E-3

Table 35: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9$ in SmallGroup notation of [GAP]

d_K area	number of fields	[576,3]	[441,7]	[576,1445]
up to about $15 \cdot 10^6$	17133	1.5759E-3	2.6265E-3	7.5877E-4
conjecture		2.6261E-3	2.6133E-3	2.4619E-3

Table 36: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9$ in SmallGroup notation of [GAP]

d_K area	number of fields	[15,1]	[60,9]	[240,199]	[240,32]
up to 10^8	47436	8.0390E-1	1.4407E-1	1.4462E-2	1.6464E-2
conjecture		7.4798E-1	1.6362E-1	3.0679E-2	2.0453E-2

Table 37: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_{15}$ in SmallGroup notation of [GAP]

d_K area	number of fields	[240,204]	[960,11366]	[960,216]	[735,5]
up to 10^8	47436	6.5773E-3	2.8670E-3	2.0449E-3	2.3611E-3
conjecture		1.2783E-2	6.7110E-3	2.5566E-3	2.5442E-3

Table 38: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_{15}$ in SmallGroup notation of [GAP]

d_K area	number of fields	[960,9667]	[1815,6]	[1815,8]	[960,11390]
up to 10^8	47436	1.0751E-3	1.2438E-3	5.2703E-4	8.4324E-5
conjecture		2.3968E-3	1.2363E-3	6.1817E-4	4.4226E-4

Table 39: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_{15}$ in SmallGroup notation of [GAP]

d_K area	number of fields	[27,2]	[108,18]	[108,20]	[432,525]
up to 10^8	1387	4.5854E-1	2.1629E-1	8.8681E-2	4.4701E-2
conjecture		3.5122E-1	2.3049E-1	7.6829E-2	5.0419E-2

Table 40: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9 \times C_3$ in SmallGroup notation of [GAP]

d_K area	number of fields	[432,524]	[432,99]	[432,551]	[1728,12471]
up to 10^8	1387	3.6049E-2	1.6583E-2	6.4888E-3	1.3699E-2
conjecture		5.0419E-2	2.8811E-2	1.8007E-2	1.2605E-2

Table 41: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9 \times C_3$ in SmallGroup notation of [GAP]

d_K area	number of fields	[1728,46133]	[675,8]	[432,101]	[1728,46128]
up to 10^8	1387	1.0094E-2	1.5862E-2	9.3727E-3	2.1629E-3
conjecture		1.1029E-2	1.0537E-2	9.6036E-3	7.8780E-3

Table 42: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9 \times C_3$ in SmallGroup notation of [GAP]

d_K area	number of fields	[1728,47903]	[1728,12470]	[1728,12474]	[432,553]
up to 10^8	1387	2.8839E-3	6.4888E-3	2.8839E-3	2.1629E-3
conjecture		7.0419E-3	6.3024E-3	6.3024E-3	6.0023E-3

Table 43: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9 \times C_3$ in SmallGroup notation of [GAP]

d_K area	number of fields	[1728,46127]	[1728,46126]	[1728,1285]	[1323,39]
up to 10^8	1387	2.1629E-3	7.2098E-4	2.8839E-3	3.6049E-3
conjecture		3.9390E-3	3.9390E-3	3.6014E-3	3.5839E-3

Table 44: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9 \times C_3$ in SmallGroup notation of [GAP]

d_K area	number of fields	[675,10]	[1728,18304]	[1323,41]	[1728,18316]
up to 10^8	1387	6.4888E-3	1.4420E-3	7.2098E-4	7.2098E-4
conjecture		3.5122E-3	3.3763E-3	1.1946E-3	1.1254E-3

Table 45: distribution of $\mathrm{Gal}(K_{2,f}/K)$ for real quadratic fields K with $\mathrm{Gal}(K_{1,f}/K) \cong C_9 \times C_3$ in SmallGroup notation of [GAP]

5.3 Database

Some example data of second Hilbert class fields K_2 of real quadratic number fields is presented on `http://www.mathematik.uni-kl.de/~numberfieldtables/KT_K2Q/doc.html`. Which fields exactly is described on this internet page. This number field table is part of the number field database `http://www.mathematik.uni-kl.de/~numberfieldtables/`. The number field tables belonging to this database may have different content, but the internet access to those tables always is the same and will be explained now at the example of the table of the K_2 fields.

Apart from `http://www.mathematik.uni-kl.de/~numberfieldtables/KT_K2Q/doc.html`

also `http://www.mathematik.uni-kl.de/~numberfieldtables/KT_K2Q/download.html` and `http://www.mathematik.uni-kl.de/~numberfieldtables/KT_K2Q/suche.html` belong to the table of the K_2 fields. It is obvious how to use the first two pages (at least with a browser). The third page is a search form, which is useful if you do not want to download the whole table (which may be large). It consists of two field sets. The first one gives the search criteria. For example you could enter there that you are just interested in those K_2 fields where $d_K > 10^{15}$ and $h_K = 3$. If you do not enter anything here, all data would fulfill the search criteria. At the second field set you can choose how the result should be presented. `show examples` gives some records on an `html-page` which fits to the search criteria and `download` starts to download all those records. They are stored in a [PARI] readable list (at least after decompressing them) and if you do not know how large the result of a search request is, you should always download the compressed data. The other possibilities in this field set tell the search script to make a statistic. Therefore you have to specify a component and the search script counts which entry appears how often in this component of those records which fits to the search criteria of the first field set. The meaning of the components is explained on `doc.html` and depending on the search criteria making statistic may take some minutes. So wait for the browser to present the result and just use this search form if you know what you are doing.

5.4 The Database Program

This chapter explains the database program which has been used to create web-interface of the number field database `http://www.mathematik.uni-kl.de/~numberfieldtables/`. It can be downloaded from this page. If you have number field tables and an `http`-server, and you want to present the tables in an internet database you can use this database creation program to generate it.

The internet database consists of three main `html`-pages and any number of single tables. These three pages are `index.html`, `tab.html` and `links.html`. The first should be used to give general information about the database, the second gives links to the single tables of the database and the third is a possibility to give links to other internet-pages. Each single table consists of three `html`-pages again (`doc.html`, `download.html`, `suche.html`), a search script and any number of files containing number field tables. The single tables are independent of each other and the content of the database is grouped into these single tables. On `doc.html` you should present the documentation of the content of the single table, on `download.html` you should give direct download-links for the number field table files and `suche.html` is a search form which is created by the program and allows to search in all of the number field tables of the corresponding single table. To enable the search script to search in the number field tables, they all have to have the same structure (see below).

The database creation program gets the information how the `html`-pages should look like and how the search script should search from the following text files which can be modified with any notepad program: `mainlist.txt`, `pagelayout.txt` and one `txt`-file for every single table. `pagelayout.txt` specifies the look of all database-pages, `mainlist.txt` describes the content of `index.html`, `links.html` and `tab.html`, and the `txt`-file of a single table describes the content of the `html`-pages of the single table and how the search script should work.

Installation of database creation program If you have downloaded the program, you should have a folder database with the content:

```
dblogo.jpg
readme.pdf
pagelayout.txt
mainlist.txt
erznfdb.cpp
nfdbfkt.h
nfdberzfkt.h
nfdbsuchfkt.h
nfdbfkt.cpp
nfdberzfkt.cpp
nfdbsuchfkt.cpp
KT_example.txt
example_table
```

To install it you need a `c++` compiler like `gcc` with `STL` and `zlib`. The following description refers to `gcc`. At first you have to modify the strings `L_DB`, `L_CGI`, `P_WWW`, `P_DB`, `P_CGI`, `TMP_LOG_DAT` in the first 50 lines of `nfdbfkt.h` for configuration. `L_DB` gives the `http`-path of the database pages, `L_CGI` gives the `http`-path of the `cgi`-files of the search scripts and `P_WWW` is the directory where the `cgi`-files try to open the number field tables. These strings should depend on the configuration of your `http`-server. `P_DB` and `P_CGI` are the directories which the database program writes the `html`-pages of the database and the source code of the search scripts to (if there is no direct access to `P_WWW` without administrator then `P_DB` and `P_WWW` can differ). `TMP_LOG_DAT` is a temporary file, the search scripts (and only them) must be able to write and delete.

After that you can compile the database creation program, for example:
`g++ -static nfdbfkt.cpp nfdberzfkt.cpp erznfdb.cpp -o erznfdb.out`.

Creation of database This paragraph describes how to create the database. If you want to modify, remove or add single tables the procedure is very similar. At first you have to know how you group your number field tables into the single tables of the database. Then you modify `mainlist.txt` and create the single table-description files (see below). If you just want to see how the program works, you can generate the prepared example database which contains one single table: `KT_example`. In this case you do not have to make changes in `mainlist.txt`, and you can use the file `KT_example.txt` as single table description file.

If `mainlist.txt` is modified and if you have created all single table description files, move them in the database folder and execute `erznfdb.out`. This program creates the `html`-pages and directories of the database in the root directory `P_DB`. Then it waits until you have copied the number field tables into corresponding directories in `P_DB`. For the example database `example_table` has to be copied to
`P_DB/KT_example/Tabellen/example_table`.
If this has been done the program may check if the tables which should be accessible by the search script have correct structure (see below). The search script can not detect errors in this tables, so if you are not sure if their structure is correct, you should test them which

can take a long time. After that the program writes the source code of the search scripts and information how to compile them (the file `komp`) to the directory `P_cgi`.

Now you should ask an administrator to copy the content of `P_DB` to `P_WWW` and to compile the search scripts (execute `./komp`) and install them such that they can be accessed via `L_CGI`, can open files in `P_WWW` and can write and delete `TMP_LOG_DAT`.

Adaptation of mainlist.txt The easiest way to understand how this file affects the creation of the database is to create the example database (see before) and see what of its content has which effect. If you want to create a new `mainlist.txt` use the one from the example database and modify it. `mainlist.txt` consists of three sections of content which are separated by `#`-sections. The `#`-sections help the program to identify the content, so `#`-sections may not be separated, assembled, created or removed and if a `#`-section should not be taken into account, use a blank line. In the content part you only should use `ASCII`-symbols between 0-127, or you make sure that it is not stored as unicode. The first section is a list of lines. Each line has to start with `n:` , `a:` , or `u:` (after the colon there has to be a space). These lines describe the table with the links to the single tables on `tab.html`. After `u:` there is a heading on the list, after `n:` or `a:` there has to be the name of the single table description file. If it is `a:` , then there will be a link to the single table on `tab.html`, but the search script and the `html`-pages for this single table will not be created (again), otherwise it will be done. The second part describes the content of `index.html`. It has to be written in `html`, but you can deal with it as if this `html`-text would be enclosed by `<html><head><title></title></head><body>` and `</body></html>`. The third section describes the `links.html`-page as the second does for `index.html`.

Creation of single table description files The easiest way to understand how this file affects the creation of the database is to create the example database (see before) and see what of the content of `KT_example.txt` has which effect. If you want to create a new single table description file use `KT_example.txt` and modify it. A single table description file consists of 14 sections of content which are separated by `#`-sections. The `#`-sections help the program to identify the content, so `#`-sections may not be separated, assembled, created or removed and if a `#`-section should not be taken into account, use a blank line. After the last `#`-section there has to be a blank line. In the content part you only should use `ASCII`-symbols between 0-127, or you make sure that it is not stored as unicode. The following list gives a description about the content of the 14 sections. For examples see `KT_example.txt`.

1. A short description of the title of the single table (about 10 symbols) has to be here.
2. A description of the single table on the list at `tab.html` (about one sentence) has to be here.
3. `html`-text which appears on the `doc.html`-page of the single table has to be here.
4. `html`-text which appears under Tables on `download.html` has to be here.
5. `html`-text which appears under Statistics on `download.html` has to be here. Use a blank line if you do not want this section to be used.

6. `html`-text which appears under Scripts on `download.html` has to be here. Use a blank line if you do not want this section to be used.

The remaining sections are necessary to give information how the search script should work:

7. This section describes how the search form of the single table under `suche.html` looks like. It is a list of lines of the structure

   text left `#` name of condition `#` text right.

   It creates a text input form on the search form. Left of this input box is text left and on the right text right. The names `erg`, `stko`, `true`, `stpr` can not be used as names for conditions. The name of a condition should only contain English letters digits and the symbol `_` . If the internet user starts a search, then he uses these input boxes to communicate with the search script.

8. This section is a vector in [PARI]-style which tells the search script the structure of the number field tables. Its components are vectors which are generated by the same grammar or data types such that this vector coincides with every record of a number field table of this single table if one replaces the content of the records by their data-types (see structure of tables below).

9. Here has to be a decimal integer which tells the maximal length of a record of the database in byte (or more precisely in `sizeof(char)` of the `c++` compiler which generates the search scripts). The database creation program can correct this value, if you let it check the tables.

10. There are two kinds of conditions under point 7. Table conditions and component conditions. In this section the table conditions are specified. Therefore this section consists of a list `condition#value#table 1#table 2# ....` `condition` is the name of a condition of section 7 and if the internet user inputs `value`, the search script opens `table 1`, `table 2`,... `table 1`, `table 2`, ... are the names of the files which belong to this single table and contain the information about the number fields. If you do not want to use specific table conditions you have to write `true##table 1#table 2# ...` such that the search script knows which tables it should open.

11. Here it is described how the component conditions are used in the search script. Each condition which appears in the search form under 7 and is not a table condition is a component condition and has to appear here. This section consists of a list of

    `component#search function# condition 1(#condition 2(#condition 3)).`

    A search function takes one component (the component `component`) of a vector of a record of the database and up to three values specified by the internet user as input and returns true or false. The search script returns a record of the database if all functions listed here return true. The possible search functions are listed below and the components of a vector are counted starting with 0 ignoring the depth. For example a is in component 0 of both of the vectors $[a, b, c]$, $[[a, b], c]$. At component 0 you have to use the function `<=s<=`.

12. The internet user has two possibilities how he wants to use the search script. He can get all records which fulfill his search criteria, or he can select a component and the search script counts how the values of this component are distributed among all records which meet the search criteria. Here has to be a 0-1-sequence which determines for which component the internet user is allowed to make statistic. Again the components are counted beginning at 0 and ignoring the depth, so b is in component 1 of all of the following vectors: $[a, b, c]$, $[a, [b, c]$, $[[a, b], c]$.
13. The records of each file of a single table have to be ordered according to component 0 (see structure of tables below). If they should be ordered by absolute value enter `betrag` in this section, otherwise enter `normal`.
14. This section must consist of a blank line.

Adaptation of layout This can be done by modifications in the `pagelayout.txt` file. `pagelayout.txt` consists of six section of content which are separated by `#`-sections. The `#`-sections help the program to identify the content, so `#`-sections may not be separated, assembled created or removed. They contains the `html`-code of the internet-pages of the database with 6 placeholders. The database creation program replaces them by other strings. `1###1`, `3###3`, `4###4` are always replaced by `HTMLTITEL`, `HTMLTITELRECHTS` and `BILDCHEN` defined in the first lines of `nfdbfkt.h`. `2###2` becomes database on the pages `index.html`, `tab.html` and `links.html` and otherwise it becomes the name of the single table the corresponding `html`-page belongs to. `6###6` is replaced by the actual content of the corresponding page, and `5###5` is build from the other sections in `pagelayout.txt` to give links to the other pages of the database.

Structure of tables In the single table description file, you can specify files which can be accessed through the search-script. For every single table that can be an arbitrary number of files, but each of those files must not be larger then 2GB and it must be an `ASCII` encoded list of lines (see `example_table`). A line is terminated by Windows or Linux line termination symbol and it represents a record of the single table of the database. A record is stored as a vector in [PARI]-style, that means components are separated by a comma and the vector starts with `[` and ends with `]`. Each entry is again a vector or it is one of the data-types z, i, s, c, g, f, a, which are explained in the following table.

data-type	description	example
z	number string of any length	`-1234567`
i	number string which is short enough to be of c++ type long long int on the system where the search scripts are compiled	`-1234567`
s	string without spaces, commas,], [, ", and line termination symbols; more precisely: a string which contains just `ASCII` symbols between 33 and 126 except 34, 44, 91 and 93	`X^2-5`
c	abelian group in descending elementary divisor notation; each elementary divisor has to be of type i	`[12,2,2]`
g	`IdSmallGroup` of [GAP]; both entries have to be of type i	`[4,2]` for $C_2 \times C_2$

data-type	description	example
f	prime factorization of a non zero integer	`[]` for 1 `[2,1]` for 2 `[-1,1;2,2;3,1]` for -12
a	string in quotation marks; more precisely a string with char(34) as first and last element, where the other elements are `ASCII` symbols between 32 and 126, except 34.	`"[67[,77"`

A new entry of the vector starts directly after `[` or a comma, so there must not be spaces after the commas which separate the entries. The structure of the records which belongs to the same single table, has to be identical and it can be described by a vector, whose entries are the data-types. The first entry of every vector has to be of type z or i and the records of every file of a single table have to be ordered according to this component (here first entry of $[[a,b],c]$ means a, not $[a,b]$ for example). There are two possibilities to order them, but it has to be the same for all files belonging to the same single table. The records always must rise up, but they can be ordered in the usual way or by absolute value: $-2 < -1 < 0 < 1 < 2 < 3$ or $0 < 1 = -1 < 2 = -2 <$. The following vectors are correct examples for the structure-type [z,s,i,c]:

```
[5,X^2-X-1,1,[]]
[8,X^2-2,1,[]]
[12,X^2-3,"$","$"]
```

Every entry of a record which is not the first can also be equal to `"$"`. This is independent of the data type of the entry and allows to indicate unknown entries.

All vectors of this type especially every output of the search script can be read with [PARI], but the data-type f differs a bit form the [PARI]-factorization of integers.

Search functions This gives a list of all search functions which can be used in the search scripts to test components. The first column shows how the function has to be named in the single table description files, the second column describes of which data-type the component of the records which is tested by this function has to have, third column gives the number of user arguments which the function expects and in the last column there is a description how this function works. The first argument given by the user is called a_1 in this table, the second and third (if they exist) a_2 and a_3. The content of the component which should be tested is denoted by c.

function	data-types		description
`x==`	i,z,s,a,c,g	1	This function returns true if a_1 is the empty string or if $a_1 = c$, otherwise it returns false.
`<=x`	i,z,c	1	This function returns true if a_1 is the empty string or if $a_1 \leq c$, otherwise it returns false.

function	data-types		description
`x<=`	i,z,c	1	This function returns true if a_1 is the empty string or if $c \leq a_1$, otherwise it returns false.
`<=x<=`	i,z,c	2	This function returns true if a_1 and a_2 are empty strings. If a_1 is the empty string it works like `x<=` and if a_2 is the empty string it works like `<=x`. If both a_1 and a_2 are non empty strings then it returns ($a_1 \leq c \leq a_2$).
`p==`	i,c	2	This function returns true if a_2 is the empty string. If a_1 is the empty string it returns ($c = a_2$), otherwise it returns true if the a_1-part of c equals a_2 and false if they differ.
`<=p`	i,c	2	This behaves to `p==` as `<=x` to `x==`.
`p<=`	i,c	2	This behaves to `p==` as `x<=` to `x==`.
`<=p<=`	i,c	3	This behaves to `p==` as `<=x<=` to `x==`.
`r==`	c	2	This function returns true if a_2 is the empty string. If a_1 is the empty string it returns $\mathrm{rk}(c) = a_2$, otherwise it returns $\mathrm{rk}_{a_1}(c) = a_2$. Here rk is the rank of the abelian group c and rk_{a_1} is the a_1-rank of c (the number of elementary divisors of c which are divisible by a_1).
`<=r`	c	2	This behaves to `r==` as `<=x` to `x==`.
`r<=`	c	2	This behaves to `r==` as `x<=` to `x==`.
`<=r<=`	c	3	This behaves to `r==` as `<=x<=` to `x==`.
`o==`	g	1	This function returns true if a_1 is the empty string, otherwise it returns true if the first component of c equals a_1 or false if they differ.
`<=o`	g	1	This behaves to `o==` as `<=x` to `x==`.
`o<=`	g	1	This behaves to `o==` as `x<=` to `x==`.
`<=o<=`	g	2	This behaves to `o==` as `<=x<=` to `x==`.
`teilt`	i,z	1	This function returns true if a_1 is the empty string or a divisor of c.
`prim`	f	1	If a_1 equals 1, yes or y and c is a prime or if a_1 is the empty string, this function returns true, otherwise it returns false.
`primpotenz`	f	1	If a_1 equals 1, yes or y and c is the power of a prime or if a_1 is the empty string, this function returns true, otherwise it returns false.
`primteiler`	f	1	If a_1 is the empty string or a prime divisor of c this function returns true, otherwise it returns false.
`quaddisk`	f	1	If a_1 is the empty string or if c is an a_1-th power of a fundamental discriminant this function returns true, otherwise it returns false.
`quadrat`	f	1	If a_1 equals 1, yes or y and c is a square or if a_1 is the empty string, this function returns true, otherwise it returns false.

References

[A] G. Andrews: *The theory of partitions*, Encyclopedia of Mathematics and its Applications, Vol. 2. Addison-Wesley, 1976.

[Bae] R. Baer: *Dualism in abelian groups*, Bull. Amer. Math. Soc. **43** (1937) no. 2, 121-124.

[Bau] K. Baur: *Homologische Algebra und modulare Darstellungstheorie*, lecture notes, ETHZ, HS 2008.

[B-B-H] N. Boston, M. Bush, F. Hajir: Oberwolfach-Report No 35/2011, DOI: 10.4171/OWR/2011/35, *Explicit methods in number theory.*

[Be] D. J. Benson: *Representations and cohomology I*, Cambridge university press, 1995.

[Bon] R. J. Bond: *On the splitting of the Hilbert class field*, Journal of Number Theory **42** (1992), 349-360.

[Bos] N. Boston: *Embedding 2-groups in groups generated by involutions*, Journal of Algebra **300** (2006), 73-76.

[BP] N. Boston, D. Perry: *Maximal 2-extensions with restricted ramification*, J. Algebra **232** (2000), 664-672.

[Br] R. Brauer: *Beziehung zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. **4** (1951) no. 139, 158-174.

[C] H. Cohen: *Advanced topics in computational number theory*, Springerverlag, 1999.

[C-L] H. Cohen, H.W. Lenstra: *Heuristics on class groups of number fields*, Number Theory, Noordwijkerhout, 1983 (H. Jager, ed.), Lecture Notes in Math., vol. 1068, Springer-Verlag, Berlin and New York, 1984, 33-62.

[C-M] H. Cohen, J. Martinet: *Etude heuristique des groupes de classes des corps de nombres*, J. reine angew. Math. **404** (1990), 39-76.

[C-R1] G. Cornell, M. Rosen: *Group-theoretic constraints on the structure of the class group*, Journal of Number Theory **13** (1981),1-11.

[C-R2] G. Cornell, M. Rosen: *A note on the splitting of the Hilbert class field*, Journal of Number Theory **28** (1988), 152-158.

[D-H] H. Davenport, H. Heilbronn: *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. Lond. A. **322** (1971), 405-420.

[F-K] E. Fouvry, J. Klüners: *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167**(2007), 455-513.

[GAP] *GAP – Groups, algorithms, and programming, Version 4.4.10*; 2007, `http://www.gap-system.org`.

[Go] D. Gorenstein: *Finite groups*, AMS Chelsea Publishing, 1980.

[Ha] H. Hasse: *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörper theoretischer Grundlage*, Math. Zeitschr. **31** (1930), 565-582.

[Ho] T. Honda: *On absolute class fields of certain algebraic number fields*, J. reine angew. Math. **203** (1960), 80-89.

[I] I. M. Isaacs: *Character theory of finite groups*, AMS Chelsea Publishing, 1976.

[K-N] T. Komatsu, S.Nakano: *On the Galois module structure of ideal class groups*, Nagoya Math. J. **164** (2001), 133-146.

[Ko] T. Kondo: *Algebraic number fields with discriminant equal to that of a quadratic number field*, J. Math. Soc. Japan **47** (1995), no. 1, 31-36.

[Lem1] F. Lemmermeyer: *Galois action on class groups*, Journal of Algebra **264** (2003), 553-564.

[Lem2] F. Lemmermeyer: *Class groups of dihedral extensions*, Math. Nachr. **278** (2005), 679-691.

[Len] J. Lengler: *The Cohen-Lenstra heuristic for finite abelian groups*, PhD thesis, Universität des Saarlandes, Saarbrücken, 2009.

[M1] G. Malle: *The totally real primitive number fields of discriminant at most* 10^9, Alg. number theory, 114-123, Lecture Notes in Comp. Sci., **4076**, Springer, 2006.

[M2] G. Malle: *On the distribution of class groups of number fields*, Experiment. Math. **19** (2010), 465-474.

[Na] W. Narkiewicz: *Elementary and analytic theory of algebraic numbers*, Springerverlag, 2004.

[Ne1] J. Neukirch: *Klassenkörpertheorie*, Bibliogr. Inst., 1969.

[Ne2] J. Neukirch: *Algebraische Zahlentheorie*, Springerverlag, 1992.

[No] A. Nomura: *On the existence of unramified p-extensions*, Osaka J. Math. **28** (1991), 55-62.

[PARI] The PARI group, *pari-gp* (version 2.4.2), Bordeaux, 2006, `http://pari.math.u-bordeaux.fr`.

[R] D.J.S. Robinson: *Applications of cohomology to the theory of groups*, Groups - St. Andrews (1981), LMS Lecture Note Series **71**, 46-80.

[Se] J-P. Serre: *Local fields*, Springerverlag, 1979.

[Su] M. Suzuki: *Group theory I*, Springerverlag, 1982.

[Wa] C. D. Walter: *Brauer's class number relation*, Acta Arithmetica **35** (1979), 33-40.

[Wr] D. Wright: *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. **58** (1989),17-50.

[Y] Y. Yamamoto: *On unramified Galois extensions of quadratic number fields*, Osaka J. Math **7** (1970), 57-76.

Nomenclature

$(G, A) \in \mathbb{M}$ ..... A is a $\mathbb{D}_G$-module with some special properties, page 20

$(n)_k$ ..... combinatorial formula, page 44

$(n)_\infty$ ..... combinatorial formula, page 44

1_H^G ..... induced principal character, page 15

$\chi_{\{P\}}$ ..... characteristic function of property P, page 44

$\hat{H}^i(G, A)$ ..... i-th Tate-cohomology group of the G-module A, page 8

$\hat{K}$ ..... Galois closure of a number field K, page 13

$\ltimes$ with $=$ ..... internal semidirect product, page 9

$\ltimes$ with $\cong$ ..... external semidirect product, page 9

$\mathbb{C}$ ..... complex numbers, page 12

$\mathbb{D}_G$ ..... $C_2 \ltimes_{inv} G$, for an abelian group G , page 6

$\mathbb{F}_p$ ..... finite field with p elements, page 6

$\mathbb{Q}$ ..... rational numbers, page 12

$\mathbb{R}$ ..... real numbers, page 12

$\mathbb{Z}$ ..... rational integers, page 6

$\mathbb{Z}^S$ ..... smallest localization of $\mathbb{Z}$ such that all elements from S become units, page 46

$\mathcal{K}(\Sigma)$ ..... set of number fields belonging to a situation Σ, page 45

$\mathcal{M}(f)$ ..... density, page 44

$\mathcal{O}_K$ ..... ring of integers in a number field K, page 12

$\oplus$ with $=$ ..... internal direct sum, page 7

$\oplus$ with $\cong$ ..... external direct sum, page 7

$\overline{K}$ ..... algebraic closure of a field K, page 24

$\tilde{C}(U)$ ..... group theoretic interpretation of class groups, page 35

ζ_K ..... Dedekind zeta function of the number field K, page 12

${}^\phi A$ ..... conjugate module, page 10

A^G ..... submodule of fixed points of a G-module A, page 9

A_p ..... p-Sylow subgroup of an abelian group A, page 6

$A_{\neq n}$ ..... direct sum of all A_p with $p \nmid n$, page 6

A_n ..... direct sum of all A_p with $p \mid n$, page 6

$d(f)$ ..... density function, page 44

d_K ..... absolute discriminant of a number field K, page 12

$F(G)$ ..... Frattini subgroup of the group G, page 6

$G \in \mathbb{G}$ ..... G is a group with some special properties, page 29

G' ..... derived subgroup of the group G, page 6

h_K ..... class number of a number field K, page 12

$I_G A$ ..... augmentation submodule of a G-module A, page 9

K_1 ..... Hilbert class field of a number field K, page 12

K_2 ..... second Hilbert class field of a number field K, page 12

$K_{1,f}$ ..... non-central coprime Hilbert class field, page 40

$K_{2,f}$ ..... second non-central coprime Hilbert class field, page 40

Tr_H^G ..... trace map, page 7

$\mathrm{Aut}(G)$ ..... automorphisms of a group G, page 10

$\mathrm{Cl}(K)$ ..... ideal class group of the number field K, page 12

$\mathrm{Cl}(L/K)$ ..... relative class group of field extension L/K, page 46

$\mathrm{Cl}^S(K)$ ..... largest subgroup of $\mathrm{Cl}(K)$ of order coprime to all elements from S, page 46

$\mathrm{Cl}_p(K)$ ..... p-Sylow subgroup of $\mathrm{Cl}(K)$ for a prime p and a number field K , page 12

$\mathrm{End}_G(A)$ ..... abelian group of $\mathbb{Z}G$-endomorphisms of the G-module A, page 6

$\mathrm{Hom}_G(A, B)$ .... see $\mathrm{End}_G(A)$, page 7

$\mathrm{Inn}(G)$ ..... automorphisms of G, induced by conjugation with some $g \in G$, page 10

$\mathrm{Out}(G)$ ..... $\mathrm{Aut}(G)/\mathrm{Inn}(G)$, page 10

pr ..... global Cohen-Lenstra probability, page 46

pr_p ..... local Cohen-Lenstra probability, page 46

Wissenschaftlicher Werdegang

1983	geboren in Stuttgart
2003	Abitur
seit 2003	Studium der Mathematik an der TU Kaiserslautern
2008	Diplom in Mathematik, TU Kaiserslautern
seit 2008	Promotion bei Prof. Dr. Malle, TU Kaiserslautern

Curriculum Vitae

1983	born in Stuttgart, Germany
2003	Abitur
since 2003	Study of mathematics at TU Kaiserslautern, Germany
2008	Diplom in mathematics, TU Kaiserslautern
since 2008	Ph.D. studies with Prof. Dr. Malle, TU Kaiserslautern