ON THE SECOND CLASS GROUP OF REAL QUADRATIC NUMBER FIELDS

by

Maximilian Boy

Abstract. — The Cohen-Lenstra heuristic for the class groups of real quadratic number fields is generalized to higher class groups. A "good part" of higher class group is defined. In general this is a non abelian proper factor group of the higher class group. Properties of the good part of the second class group of real quadratic fields are described, a probability distribution on the set of those groups is introduced and proposed as generalization of the Cohen-Lenstra heuristic. The agreement with number field tables is close.

Résumé. — Les heuristiques de Cohen-Lenstra pour les groupes de classes des corps quadratiques réels sont généralisés à des groupes de classes supérieurs. Nous définissons une partie « bonne » de ces groupes de classes supérieurs : il s'agit en général d'un groupe non-abélien facteur propre du groupe des classes supérieurs. En particulier, nous obtenons des propriétés de la partie « bonne » du deuxième groupe de classes des corps quadratiques réels et nous décrivons un modèle probabilistique sur l'ensemble de ces groupes en généralisant les heuristiques de Cohen-Lenstra. Les résultats numériques obtenues sont convaincants.

1. Introduction

Class groups are interesting objects of algebraic number theory and 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 of K. 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 iterating this approach leads to the higher class groups which are finite and solvable groups. Class groups are also mysterious, but the (mostly unproven) Cohen-Lenstra heuristic ([**C-L**], [**C-M**]) allows to describe the distribution of class groups in good accordance with number field tables.
The aim of this work is to do the same for the second class groups of real quadratic number fields as Cohen-Lenstra did for the class groups and it is an application of [**C-M**]. The structure is as follows: Chapter 2 defines a good part of higher class groups and in Chapter 3

2010 ***Mathematics Subject Classification.*** — 11R29.
Key words and phrases. — class groups, real quadratic fields, Cohen-Lenstra heuristic.

properties of the good parts of second class groups of quadratic number fields are explained. Chapter 4 describes some parts of the Cohen-Lenstra heuristic and gives the new heuristic for the distribution of the good parts of second class groups of real quadratic number fields (see Conjectures 12 and 14). The idea is to apply the Cohen-Lenstra heuristic to each step in the derived series of the good part of the second class group. This procedure should work for any higher class group of totally real abelian number fields, but in cases different from real quadratic fields the group theory which is necessary to calculate the Cohen-Lenstra heuristic becomes difficult and it is also difficult to compute number field tables to compare them with the heuristic. The last two chapters show how the second class groups of real quadratic number fields can be calculated. Class group relations reduce their computation to the computation of class groups of number fields which can be found in the tables from [**M1**] (with their class group; these tables are also available in the database at `http://www.mathematik.uni-kl.de/~numberfieldtables`).

The following **notations** are used: Let G be a finite group, A a G-module and n an integer. The module A is a multiplicatively written right module. The n-th Tate cohomology group is denoted by $\hat{H}^n(G,A)$, $A^G := \{a \in A \mid a^g = a \text{ for all } g \in G\}$ and $I_G A := \{a^{g-1} \mid g \in G, a \in A\}$. If k is a positive integer, then $(n)_k := \prod_{i=1}^{k}(1-n^{-i})$ and $(n)_\infty := \prod_{i=1}^{\infty}(1-n^{-i})$. The set of all prime numbers is $\mathbb{P}$. If S is a subset of $\mathbb{P}$ and B a finite abelian group, then $\mathbb{Z}^S$ denotes the smallest localization of $\mathbb{Z}$ in $\mathbb{Q}$ such that all elements from S are units in $\mathbb{Z}^S$ and B^S denotes the largest subgroup of B of order coprime to all elements of S. If K is a number field, then $\mathrm{Cl}(K)$ denotes the class group of K and $\mathcal{O}_K$ the ring of integers in K. If L/K is an extension of number fields, then $\mathrm{Cl}(L/K)$ is the relative class group of L/K (the kernel of the norm map: $\mathrm{Cl}(L) \to \mathrm{Cl}(K)$).

2. Good Part of Higher Class Groups

If K is a number field the maximal abelian and unramified extension of K (in one fixed algebraic closure of $\mathbb{Q}$) is called **Hilbert class field** of K and denoted by K_1. The Hilbert class field K_2 of K_1 is called second Hilbert class field and so on. One gets a sequence $K \le K_1 \le K_2 \le \cdots$ of number fields where K_i/K is Galois, unramified and solvable. Since $\mathrm{Cl}(K) \cong \mathrm{Gal}(K_1/K)$ one defines $\mathrm{Gal}(K_i/K)$ to be the ***i*-th class group** of K.

Lemma 1. — *(*[**Su**, 2.5.17]*) Let A be a finite G-module over a finite group G and $N \le G$ be a normal subgroup such that $|N|$ and $|A|$ are coprime. Define $e := \frac{1}{|N|}\sum_{g\in N} g$. Then $A = A^N \oplus I_N A$ is a direct decomposition into G-modules, both summands are the unique direct complements of each other, $I_N A = A^{1-e}$ and $A^N = A^e$.*

Let L/K be a Galois extension of number fields and N be the maximal subfield of L_1 containing L such that $(N:L)$ and $(L:K)$ are coprime. Then N/L is a Galois extension and $\mathrm{Gal}(N/L)$ is a finite $\mathrm{Gal}(L/K)$-module ($\mathrm{Gal}(L/K)$ acts by conjugation on $\mathrm{Gal}(N/L)$). Define the **non-central coprime Hilbert class field** M of L over K to be the fixed field $M = N^G$ by the group $G := \mathrm{Gal}(N/L)^e$ where $e = \frac{1}{(L:K)}\sum_{g\in \mathrm{Gal}(L/K)} g$ is a central idempotent of the

group ring $\mathbb{Q}\mathrm{Gal}(L/K)$. Let L be a Galois number field. Then $L_{1,f}$ denotes the non-central coprime Hilbert class field of L over $\mathbb{Q}$, $L_{2,f}$ denotes the non central coprime Hilbert class field of $L_{1,f}$ over L, which is also called second non-central coprime Hilbert class field of K. This approach leads to a sequence $L \leq L_{1,f} \leq L_{2,f} \leq L_{3,f} \leq \cdots$ of number fields.
The group $\mathrm{Gal}(L_{i,f}/L)$ is called **good part of the i-th class group** of L. In general it is a proper factor group of the i-th class group (see [**Bo**, Proposition 3.7]). The idea of its definition is to have a factor group of the i-th class group, where consecutive steps in the derived series have coprime order and where the i-th step corresponds to a subgroup of $\mathrm{Cl}(L_{i-1,f}/L_{i-2,f})$ which is good in the sense of Cohen-Martinet. This also prevents excluded parts of some step of the derived series to appear later. The whole theory also works if one excludes some additional primes for the order in some of the steps in the derived series (and is able to use some more in some others; as long as consecutive steps remain to have coprime order).

Remark. — The part of $\mathrm{Gal}((L_{i,f})_1/L_{i,f})$ which is not coprime to $(L_{i,f} : L_{i-1,f})$ is excluded from the considerations as bad part. 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**]).

Proposition 2. — *Let L be an abelian number field and set $L_{0,f} := L$ and $L_{-1,f} := \mathbb{Q}$. Let $-1 \leq j < i < k$ be integers, $G_i := \mathrm{Gal}(L_{i,f}/\mathbb{Q})$, $H_k := \mathrm{Gal}(L_{k,f}/L_{k-1,f}))$, $H_0 := G_0$ and $e_i = \frac{1}{(L_{i,f}:L_{i-1,f})} \sum_{g \in H_i} g$. Then the following hold:*
(a) $L_{i,f}/\mathbb{Q}$ is Galois,
(b) $\mathrm{Gal}(L_{i+1,f}/L_{i,f})^{\mathrm{Gal}(L_{i,f}/L_{i-1,f})} = \{1\}$,
(c) $\hat{H}^n(\mathrm{Gal}(L_{i,f}/L_{j,f}), \mathrm{Gal}(L_{i+1,f}/L_{i,f})) = \{1\}$ for every positive integer n,
(d) the exact sequence of groups

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

is split,
(e) $\mathrm{Gal}(L_{i,f}/L_{j,f})' \cong \mathrm{Gal}(L_{i,f}/L_{j+1,f})$,
(f) $\mathrm{Cl}^{S_i}(L_{i,f}/L_{i-1,f}) = \mathrm{Cl}^{S_i}(L_{i,f})^{1-e_i} \cong \mathrm{Gal}(L_{i+1,f}/L_{i,f})$, where S_i is the set of primes dividing $(L_{i,f} : L_{i-1,f})$,
(g) the central idempotent e_i of $\mathbb{Q}G_i$ corresponds to the $\mathbb{Q}$-character $1_{H_i}^{G_i}$.

Proof. — Statement (a) follows by induction and (b) is a consequence of Lemma 1. Define $G := \mathrm{Gal}(L_{i+1,f}/L_{i-1,f})$ and $A := \mathrm{Gal}(L_{i+1,f}/L_{i,f})$. Since $(G : A)$ and $|A|$ are coprime, one has $\hat{H}^n(G/A, A) = \{1\}$ ([**Ne1**, Theorem 1.3.16]) for every integer n. By induction the inf-res-sequence ([**Ne1**, Theorem 1.4.7]) shows that the Tate cohomology $\hat{H}^n(\mathrm{Gal}(L_{i,f}/L_{j,f}), \mathrm{Gal}(L_{i+1,f}/L_{i,f})) = \{1\}$ for each integer $n \geq 1$ which proves (c). The cohomological version of the Schur-Zassenhaus theorem (see [**Su**, Chapter 2.7]) and a short calculation show (d). Let H be a complement of A in G. If $x, y \in H$ and $a, b \in A$, then $x^{-1}a^{-1}y^{-1}baxb^{-1}y = a^{x(y-1)}b^{y(x-1)}$. This implies $G' = I_G A$ and therefore

$G' = A$ because of Lemma 1. Statement (e) follows by induction. The natural action of $\mathrm{Aut}(L_{i,f})$ on $\mathcal{O}_{L_{i,f}}$ makes $\mathrm{Cl}(L_{i,f})$ into a $\mathrm{Gal}(L_{i,f}/L_{i-1,f})$-module which is isomorphic to the $\mathrm{Gal}(L_{i,f}/L_{i-1,f})$-module $\mathrm{Gal}((L_{i,f})_1/L_{i,f})$ via Artin isomorphism ([**Ne1**, Theorem 2.1.11]). Because of [**Lem1**, Proposition 1] the relative class group $\mathrm{Cl}^{S_i}(L_{i,f}/L_{i-1,f})$ can be replaced by $\mathrm{Cl}^{S_i}(L_{i,f})^{(1-e_i)} \cong \mathrm{Gal}(M/L_{i,f})^{(1-e_i)}$, where M is the maximal unramified abelian S_i'-extension of $L_{i,f}$. The definition of $L_{i+1,f}$ implies (f). If N is a normal subgroup of a finite group U and χ denotes the characteristic function, then $1_N^U(x) = \frac{1}{|N|} \cdot |\{g \in U \mid x^g \in N\}| = (U:N) \cdot \chi_{\{x \in N\}}$ for all $x \in U$. Therefore $\mathrm{Ker}(1_N^U) = \mathrm{Ker}(\varphi) = N$ for every irreducible $\mathbb{C}U$ constituent φ of 1_N^U and $\langle 1_N^U, \varphi \rangle = \varphi(1)$ by Frobenius reciprocity. Theorem 2.12 from [**I**] shows $e_N^U = \frac{1}{N} \sum_{g \in N} g$, if e_N^U is the central $\mathbb{C}U$-idempotent corresponding to 1_N^U, which is even from $\mathbb{Q}U$. This shows (g). □

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 $a \mapsto a^{\phi^{-1}(g)}$.

Proposition 3. — *(see* [**R**] *for used methods) Let G and A be finite groups and let A be abelian. Let $M \subset \mathrm{Hom}(G, \mathrm{Aut}(A))$ be the subset of all ρ for which $\{1\} \times A$ equals the last non trivial term in the derived series of $G \ltimes_\rho A$ and $\hat{H}^1(G, A) = \{1\}$ and $A^G = \{1\}$ with regard to the G-module structure on A which is defined by ρ. Then one has:*

(a) If $\varphi, \psi \in M$, then $G \ltimes_\varphi A \cong G \ltimes_\psi A$ if and only if the G-module structures on A defined by φ and ψ are conjugate.

(b) Let $\varphi \in M$ and k_φ be the number of isomorphism classes of module structures of G on A which are conjugate to the G-module structure on A defined by φ. Then

$$k_\varphi = \frac{|A| \cdot |\mathrm{Aut}_G(A)| \cdot |\mathrm{Aut}(G)|}{|\mathrm{Aut}(G \ltimes_\varphi A)|}.$$

Proof. — Let $\rho, \rho_1, \rho_2 \in \mathrm{Hom}(G, \mathrm{Aut}(A))$. Let A_ρ denote the G-module which corresponds to ρ. The group $H := \mathrm{Aut}(G) \times \mathrm{Aut}(A)$ acts from the left on $\mathrm{Hom}(G, \mathrm{Aut}(A))$ by ${}^{(\Phi,\Psi)}\rho = i_\Psi \circ \rho \circ \Phi^{-1}$, if i_Ψ denotes the left conjugation with Ψ in $\mathrm{Aut}(A)$. Let U denote the normal subgroup $\{1\} \times \mathrm{Aut}(A)$ of H. The U-stabilizer of ρ is $\mathrm{Aut}_G(A_\rho)$. The two homomorphisms ρ_1, ρ_2 are in the same U-orbit, if and only if $A_{\rho_1} \cong A_{\rho_2}$ as G-modules and they are in the same H-orbit, if and only if A_{ρ_1} and A_{ρ_2} are conjugate. Therefore the H-orbit of ρ decomposes under the action of the normal subgroup $U \leq H$ into k_ρ orbits of the same length $\frac{|\mathrm{Aut}(A)|}{|\mathrm{Aut}_G(A_\rho)|}$. The following gives another description of the H-orbits:

(i) Let $\mathrm{Comp}(\rho)$ be the subset of $\mathrm{Aut}(G) \times \mathrm{Aut}(A)$ consisting of all (Φ, Ψ), such that $f : G \ltimes_\rho A \to G \ltimes_\rho A : (g, a) \mapsto (\Phi^{-1}(g), \Psi^{-1}(a))$ is an automorphism. Then $\mathrm{Comp}(\rho)$ is the H-stabilizer of ρ.

(ii) ρ_1, ρ_2 are in the same H-orbit, if and only if there is an isomorphism $f : G \ltimes_{\rho_1} A \to G \ltimes_{\rho_2} A$ with $f(\{1\} \times A) = \{1\} \times A$ and $f(G \times \{1\}) = G \times \{1\}$.

(iii) $\varphi, \psi \in M$ are in the same H-orbit if and only if $G \ltimes_\varphi A \cong G \ltimes_\psi A$.

(iv) If $\varphi \in M$, then $|\mathrm{Comp}(\varphi)| \cdot |A| = |\mathrm{Aut}(G \ltimes_\varphi A)|$.

If $g,h \in G$, $a,b \in A$, $(\Phi,\Psi) \in \mathrm{Aut}(G) \times \mathrm{Aut}(A)$ and $f : G \times A \to G \times A : (g,a) \mapsto (\Phi^{-1}(g), \Psi^{-1}(a))$ is a map, then

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

This calculation implies (i) and (ii). If $\varphi, \psi \in M$, then an isomorphism $f : G \ltimes_\varphi A \to G \ltimes_\psi A$ maps $\{1\} \times A$ to $\{1\} \times A$ and $G \times \{1\}$ to a complement of $\{1\} \times A$ by the assumption on M. Since $\hat{H}^1(G,A) = \{1\}$ theorem 2.8.8 from **[Su]** implies that $f(G \times \{1\})$ and $G \times \{1\}$ are conjugate in $G \ltimes_\psi A$ and statements (iii) and (a) are implied by (ii). This also shows $\mathrm{Aut}(G \ltimes_\varphi A) = \mathrm{Comp}(\varphi) \cdot i(A)$, if $i : A \to \mathrm{Inn}(G \ltimes_\varphi A)$ denotes the homomorphism which maps $a \in A$ to the left conjugation with a in $G \ltimes_\varphi A$. By assumption $A^G = \{1\}$. A short calculation gives $\mathrm{Comp}(\varphi) \cap i(A) = \{1\}$ and $|A| = |i(A)|$ and hence (iv). If $\varphi \in M$ the size of its H-orbit equals

$$\frac{|\mathrm{Aut}(G)| \cdot |\mathrm{Aut}(A)|}{|\mathrm{Comp}(\varphi)|} = \frac{|\mathrm{Aut}(G)| \cdot |\mathrm{Aut}(A)| \cdot |A|}{|\mathrm{Aut}(G \ltimes_\varphi A)|} = k_\varphi \cdot \frac{|\mathrm{Aut}(A)|}{|\mathrm{Aut}_G(A_\rho)|}.$$

This implies (b). □

Remark. — If L is an abelian number field, then for any integer $i > 0$ and some $\rho \in \mathrm{Hom}(\mathrm{Gal}(L_{i-1,f}/\mathbb{Q}), \mathrm{Aut}(\mathrm{Gal}(L_{i,f}/L_{i-1})))$ by Proposition 2 one has $\mathrm{Gal}(L_{i,f}/\mathbb{Q}) \cong \mathrm{Gal}(L_{i-1,f}/\mathbb{Q}) \ltimes_\rho \mathrm{Gal}(L_{i,f}/L_{i-1})$ and $\rho \in M$ according to the notation of Proposition 3.

3. Good Part of Second Class Groups of Real Quadratic Fields

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. The group G is identified as normal subgroup of $\mathbb{D}_G$.
The following lemma is well-known (see **[Bo]** for a proof for example):

Lemma 4. — *Let K_1 be the Hilbert class field of a quadratic number field K. Then* $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathbb{D}_{\mathrm{Cl}(K)}$.

Let $\mathbb{M}$ **denote** the 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, $|G|$ and $|A|$ are coprime and $A^G = \{1\}$. The notation $(G,A) \in \mathbb{M}$ is used for a $\mathbb{D}_G$-module A from $\mathbb{M}$. Let $\mathbb{G}$ denote the set of isomorphism classes of all groups G with the following properties: $|G| < \infty$, $G/G' \cong C_2$, $G''' = \{1\}$ and $|G'/G''|$ and $|G''|$ are coprime. If K is a quadratic number field, then $(\mathrm{Gal}(K_{1,f}/K), \mathrm{Gal}(K_{2,f}/K_{1,f})) \in \mathbb{M}$ and $\mathrm{Gal}(K_{2,f}/\mathbb{Q}) \in \mathbb{G}$ by Proposition 2. With the

proof of this proposition it is easy to see, that for $G \in \mathbb{G}$ one has $G \cong \mathbb{D}_{G'/G''} \ltimes G''$ and $(G'/G'', G'') \in \mathbb{M}$.

Lemma 5. — *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 trivially 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.

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 1 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). 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 non trivial 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 property (b) follows. □

Remark. — This lemma is a generalization of [**Su**, 2.5.23] and [**C-R**, Proposition 4]. 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 6. — *Let $(G, A) \in \mathbb{M}$ and let $\varphi \in \mathbb{D}_G \setminus G$ be any involution. Then:*
(a) If $G = \langle \sigma \rangle$ is cyclic, then $A = A^{\langle \varphi \rangle} \oplus (A^{\langle \varphi \rangle})^\sigma$.
(b) $A = A^{\langle \varphi \rangle} \oplus K$ as group, where $K \cong A^{\langle \varphi \rangle}$ as subgroup of A.
(c) There is a subgroup $M \leq A$ such that $A = M \oplus M^\varphi$ and $M \cong A^{\langle \varphi \rangle}$ (as groups).

Proof. — If G is cyclic, statements (a) and (b) are special cases of [**Ho**, Theorem 4]. By Lemma 5 the $\mathbb{D}_G$-module A has a direct 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 of (b) reduces to the cyclic case. 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 for proving (c):

Case 1: $2 \nmid |A|$: Because $|\langle\varphi\rangle|$ and $|A|$ are coprime, A has trivial Tate cohomology as $\langle\varphi\rangle$-module and one has $A = A^{\langle\varphi\rangle} \oplus I_{\langle\varphi\rangle}A$ (Lemma 1). The automorphism φ of A is trivial on the first summand and inverts every element of the second summand. Statement (b) implies that there is an isomorphism of groups $f : A^{\langle\varphi\rangle} \to I_{\langle\varphi\rangle}A$. Set $M := \langle a \cdot f(a) | a \in A^{\langle\varphi\rangle}\rangle$. Since $2 \nmid |A|$ any element of A is a square $a^2 \cdot f(b^2)$ with $a, b \in A^{\langle\varphi\rangle}$. 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 therefore $A = M \cdot M^\varphi$. Since $|A| = |A^{\langle\varphi\rangle}|^2 = |M| \cdot |M^\varphi|$ one has $A = M \oplus M^\varphi$.
Case 2: A is a 2-group: By (b) $A^{\langle\varphi\rangle}$ has a group theoretical complement $M := K \leq A$ which is isomorphic to $A^{\langle\varphi\rangle}$. 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 $A^{\langle\varphi\rangle}$ and so $y^\varphi = y$. Since $y \in M$, $y = 1$ follows. This is a contradiction. Because $|A| = |M| \cdot |\varphi(M)|$, one has $A = M \oplus M^\varphi$. □

Proposition 7. — *Let K, L be quadratic fields. Then* $\mathrm{Gal}(K_{2,f}/\mathbb{Q}) \cong \mathrm{Gal}(L_{2,f}/\mathbb{Q})$ *if and only if* $\mathrm{Gal}(K_{2,f}/K) \cong \mathrm{Gal}(L_{2,f}/L)$.

Proof. — Suppose that $\mathrm{Gal}(K_{2,f}/K) \cong \mathrm{Gal}(L_{2,f}/L)$ (the other direction is implied by Proposition 2 (e)). Define $A := \mathrm{Gal}(K_{2,f}/K_{1,f})$, $B := \mathrm{Gal}(L_{2,f}/L_{1,f})$ and $G := \mathrm{Gal}(K_{1,f}/K)$. Then by Proposition 2 (e) one can choose an isomorphism of groups such that $G \cong \mathrm{Gal}(L_{1,f}/L)$ and therefore the conjugation with $\mathrm{Gal}(K_{1,f}/\mathbb{Q})$ respectively with $\mathrm{Gal}(L_{1,f}/\mathbb{Q})$ makes the abelian groups A and B into $\mathbb{D}_G$-modules. By Proposition 3, these modules are conjugate as G-modules. That means there is an automorphism ϕ of G such that the modules A and ${}^\phi B$ are isomorphic as G-modules. Let $x \in \mathbb{D}_\mathbb{G} \setminus G$ be an involution and y be any element of G. 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 $\mathbb{D}_G$-module ${}^{\hat{\phi}} B$ to G ($\hat{\phi}$ is well defined since the action of x on G is contained in the center of $\mathrm{Aut}(G)$). It will be shown that A and $C := {}^{\hat{\phi}} B$ are isomorphic as $\mathbb{D}_G$-modules:
1. Case: $G = \langle g \rangle$ is cyclic: By Lemma 6 one has $A = A^{\langle x\rangle} \oplus (A^{\langle x\rangle})^g$. This is a decomposition into $g + g^{-1}$ invariant subgroups which are $g + g^{-1}$ isomorphic. The same holds true for C. By the theorem of Krull-Remak there is a $g + g^{-1}$ invariant isomorphism $f : A^{\langle x\rangle} \to C^{\langle x\rangle}$. Define $\hat{f} : A \to C$ by $\hat{f}(a \cdot b^g) = f(a) \cdot f(b)^g$ for $a, b \in A^{\langle x\rangle}$. By definition $\hat{f}$ is a $g + g^{-1}$ invariant isomorphism of abelian groups. The following calculation shows that it is also an isomorphism of $\mathbb{D}_G$-modules. If $a, b \in A^{\langle x\rangle}$, then:

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

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

2. Case: Reduction to cyclic case: One can apply case 1 to every summand in the decomposition described in Lemma 5. Hence A and ${}^{\hat{\phi}}B$ are isomorphic as $\mathbb{D}_G$-modules and the proposition follows from Proposition 3. □

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 to $\{1\}$ (see [**Be**, Definition 3.6.1]). For finite A the notion "A is relatively hereditary" is a generalization of "$|G|$ and $|A|$ are coprime" and it causes that every submodule of A with a group theoretic complement also has a module theoretic complement ([**Be**, Proposition 3.6.4]; theorem of Maschke) and that this property transfers to submodules and factor modules of A.

Lemma 8. — *Let $(G,A)\in\mathbb{M}$. Then the following hold:*
(a) If B is a $\mathbb{D}_G$-submodule of A, then $(G,B),(G,A/B)\in\mathbb{M}$.
(b) A is relatively hereditary as $\mathbb{D}_G$-module.

Proof. — For (a) it has to be shown that $(A/B)^G=\{1\}$. By Lemma 1 one has $A^G=A^e$ and therefore $(A/B)^G=(A/B)^e=(A^e\cdot B)/B$, where $e=\frac{1}{|G|}\sum_{g\in G}g$. Thus $(A/B)^G=\{1\}$.
It remains to show that A is relatively projective (to $\{1\}$) as $\mathbb{D}_G$-module: Let φ be the generator of a complement of G in $\mathbb{D}_G$. By Lemma 6 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 proposition 3.6.4 from [**Be**], it suffices to show: $Tr^{\mathbb{D}_G}_{\{1\}}(\frac{1}{|G|}\cdot f)=\mathrm{id}_A$ (since $(G,A)\in\mathbb{M}$, the orders $|A|$ and $|G|$ are coprime and multiplication with $\frac{1}{|G|}$ is a well defined isomorphism; $Tr^{\mathbb{D}_G}_{\{1\}}$ is the trace map (see [**Be**, Definition 3.6.2])). For this let $x\in A$. Then one has:

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

□

The next lemma is a version of "idempotent refinement". Some parts of the proof are almost word for word the same as in [**Ba**, Sätze 3.6, 3.8, 3.9], although these theorems show different statements.

Lemma 9. — *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 [**Ba**], [**Go**]) Statement (a) is a consequence of the theorem of Krull-Remak and Lemma 8 (a).
Assume A to be indecomposable. In lemma 5.2.1 and theorem 5.2.2 [**Go**] proves $A \cong (C_{p^e})^r$ for suitable prime p and integers e, r under the assumption that $|G|$ has to be coprime to $|A|$. Gorenstein [**Go**] uses the coprimeness assumption just to ensure that submodules with group theoretic complement also have module theoretic complements. By Lemma 8 (b) the module A is relative hereditary. This suffices to use Gorenstein's proofs and it shows that A is projective as $(\mathbb{Z}/p^e\mathbb{Z})G$-module since A is free as $(\mathbb{Z}/p^e\mathbb{Z})$-module. The same argumentation shows that A/F is a projective $\mathbb{F}_p\mathbb{D}_G$-module and $(A/F)^G = \{1\}$ follows from Lemma 8 (a).
Assume that A/F is not irreducible and hence 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 ([**Be**, Lemma 1.4.4]) shows that $i \circ \varphi$ is an automorphism of A. This is a contradiction to $|N| < |A|$ and shows (b).
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 1, 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).
It remains to show the uniqueness part of (c): Let B be an other indecomposable $\mathbb{D}_G$-module with Frattini-subgroup E, $(G, B) \in \mathbb{M}$, $|B| = |M|^e$ and $B/E \cong M$. By (b) one has $B \cong A \cong (C_{p^e})^{\dim_p(A/F)}$ as groups and A, B are projective R-modules. 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. □

Lemma 9 and Lemma 5 reduce the classification of $\mathbb{M}$ to the well-known classification (see [**I**, Chapters 6, 9]) of the finite faithful $\mathbb{F}_p\mathbb{D}_n$-modules A with $A^{C_n} = \{1\}$ where n is an odd integer coprime to the prime p (Lemma 10).
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 suitable representatives of irreducible $\overline{K}G$-representations.
If $n > 1$ is an odd integer and p a prime not dividing n, then the **notations**

$$f_{p,n} = \min_k(p^k \equiv 1(n), k > 0) \cdot \begin{cases} \frac{1}{2}, & -1 \text{ is a power of } p \bmod n \\ 1, & \text{otherwise} \end{cases}$$

and $r_{p,n} = \frac{\varphi(n)}{2 \cdot f_{p,n}}$ are used in Lemma 10 and in Proposition 11.

Remark. — Let ξ be a primitive n-th root of 1. Then p decomposes in $\mathbb{Q}(\xi + \xi^{-1})/\mathbb{Q}$ into $r_{p,n}$ prime ideals with inertia degree $f_{p,n}$.

Lemma 10. — *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 $\xi_0 = 1, \xi_1, \ldots, \xi_{n-1} \in \overline{\mathbb{F}}_p$, with $r = \frac{n-1}{2}$ and $\xi_i^{-1} = \xi_{i+r}$ for $i = 1, \ldots, r$, be the n-th roots of 1. Let a_p be an integer and let $Y_1, \ldots, Y_{a_p}$ 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 $i \in \{1, \ldots, r\}$ 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) The a_p non similar irreducible faithful $\mathbb{D}_n$-representations over $\mathbb{F}_p$ all have degree $2 \cdot f_{p,n}$ and $a_p = r_{p,n}$.

As consequence one gets the following proposition:

Proposition 11. — *(classification of $\mathbb{M}$) Let G be a finite abelian group of odd order. There is a bijection between the isomorphism classes of indecomposable $\mathbb{D}_G$-modules from $\mathbb{M}$ and the set of all tuples (j, U, e, p) where e is a positive integer, p a prime not dividing the order of G, U a subgroup of G with G/U non trivial and cyclic, $n = (G : U)$ and $1 \leq j \leq r_{p,n}$ such that the module corresponding to (j, U, e, p) is a faithful $\mathbb{D}_G/U$-module and as group isomorphic to $(C_{p^e})^{2 \cdot f_{p,n}}$.*

4. Heuristic

As mentioned before the idea for a heuristic of higher class groups is to apply the Cohen-Lenstra heuristic to every abelian step in the derived series. Therefore in the following some parts of the Cohen-Lenstra heuristic are explained shortly.
A **situation** $\Sigma = (G, K_0, \sigma, S, e)$ consists of a finite group G, a number field K_0, a signature σ and a central idempotent e of $\mathbb{Q}G$. The set $\mathcal{K}(\Sigma)$ denotes the set of all number fields K (contained in one fixed algebraic closure of K_0) such that K/K_0 has signature σ and is Galois with group $\mathrm{Gal}(K/K_0) \cong G$. A situation is called **good**, if $\mathcal{K}(\Sigma)$ is not empty, e is defined in $\mathbb{Z}^S G$, e is orthogonal to $\frac{1}{|G|}\sum_{g \in G} g$ and $\hat{e}\mathbb{Z}_{\langle p \rangle}G$ is a maximal order of $\mathbb{Z}_{\langle p \rangle}$ in $\mathbb{Q}G$ for every prime $p \notin S$ and every central irreducible constituent $\hat{e}$ of e in $\mathbb{Q}G$. Let $\mathcal{K}$ be a non empty set of number fields, A be a finite $e\mathbb{Z}^S G$-module, χ the characteristic function of any property, $f : \mathcal{K} \to \mathbb{R}$ any map,

$$\mathcal{M}_{\mathcal{K}}(f) := \lim_{x \to \infty} \frac{\sum_{K \in \mathcal{K}, |d_K| \leq x} f(K)}{|\{K \in \mathcal{K} \mid x \geq |d_K|\}|}$$

be the **density** of f and $\mathcal{M}_\Sigma(A) := \mathcal{M}_{\mathcal{K}(\Sigma)}(\chi_{\{\mathrm{Cl}^S(K/K_0)^e \cong A\}})$. Densities may not exist, but the **Cohen-Lenstra** heuristic (see **[C-L]** for the idea, **[C-M]** for details or **[Len**, Chapter 2**]** for a nice introduction) is a conjecture which proposes values for $\mathcal{M}_\Sigma(A)$ (and much more), if Σ is a good situation.

Remark. — The $e\mathbb{Z}^S G$-module structure on $\mathrm{Cl}^S(K/K_0)^e$ is just defined up to conjugacy but the Cohen-Lenstra heuristic gives the same values for all possibilities.

In most situations the Cohen-Lenstra heuristic describes $\mathcal{M}_\Sigma$ with a probability distribution; the following cases are needed here: Let H be a finite non trivial abelian group of odd order, $U_1, \ldots, U_m$ be the subgroups of H such that H/U_i is non trivial and cyclic, $n_i := (H : U_i)$, ξ_i a primitive n_i-th root of 1, $K_i := \mathbb{Q}(\xi_i + \xi_i^{-1})$ and $e_H = 1 - \frac{1}{|H|}\sum_{g \in H} g$. Define S_H to be the set containing all prime divisors of $|H|$. Suppose that $p \in S_H$ decomposes in $r_i(p)$ prime ideals with inertia degree $f_i(p)$ in the extension $K_i/\mathbb{Q}$. Set

$$c_2 := \frac{1}{2 \cdot (2)_\infty} \cdot \prod_{j=2}^{\infty} \zeta(j)^{-1},$$

$$c_{2',H} := \prod_{i=1}^{m} \left(\prod_{j=3}^{\infty} \zeta_{K_i}(j)^{-1} \cdot \prod_{p \in S_H \cup \{2\}} \left(\frac{(p^{f_i(p)})_2}{(p^{f_i(p)})_\infty} \right)^{r_i(p)} \right).$$

Then by [**C-M**, Proposition 3.10]

$$\mathrm{pr}_2(A) := c_2 \cdot \frac{1}{|A| \cdot |\mathrm{Aut}(A)|}$$

defines a probability distribution on the set of the isomorphism classes of finite abelian groups of odd order and

$$\mathrm{pr}_{2',\mathrm{H}}(A) := c_H \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_H}(A)|}$$

defines a probability distribution on the set of isomorphism classes of the finite $e_H\mathbb{Z}^{(S_H \cup \{2\})}\mathbb{D}_H$-modules, because both situations are good situations by proposition 7.1 from [**C-M**]. In these cases [**C-M**, Chapter 6] establishes the two conjectures for the densities $\mathcal{M}_\Sigma(A) = \mathrm{pr}_{2',H}(A)$, if $\Sigma = (\mathbb{D}_H, \mathbb{Q}, \text{totally real}, S_H \cup \{2\}, e_H)$ and $\mathcal{M}_\Sigma(A) = \mathrm{pr}_2(A)$, if $\Sigma = (C_2 = \langle g \rangle, \mathbb{Q}, \text{totally real}, \{2\}, \frac{1-g}{2})$.

The notion of a "good situation" in the sense of [**C-M**] seems not to be complete enough. The existence of p-th roots of 1 in the base field of a situation seems to influence the distribution of the p-parts of the class groups of this situation. In the totally real case this affects just the prime number 2. Methods to deal with these p-parts are described in [**M2**, Conjecture 2.1]. As special case one has the probability distribution $\mathrm{pr}_{2,H}$ on the finite $e_H\mathbb{Z}_{\langle 2 \rangle}\mathbb{D}_H$-modules and the conjecture $\mathcal{M}_\Sigma(A) = \mathrm{pr}_{2,H}(A)$ if A is a is such a module and $\Sigma = (\mathbb{D}_H, \mathbb{Q}, \text{totally real}, \mathbb{P} \setminus \{2\}, e_H)$. This distribution is defined as follows: Set

$$c_{2,H} := \prod_{i=1}^{m} \prod_{j=3}^{\infty} \left(1 + \frac{f_i(2)}{2^{f_i(2) \cdot j}} \right)^{-r_i(2)}.$$

Let A be a finite $e_H\mathbb{Z}_{\langle 2 \rangle}\mathbb{D}_H$-module, F its Frattini subgroup and $l_{i,j}$ the number of indecomposable summands of A/F of isomorphism type $(j, U_i, 1, 2)$ (see Proposition 11). Set

$$r_{2,H}(A) := \prod_{i=1}^{m} \prod_{j=1}^{r_i(2)} 2^{f_i(2) \cdot \frac{l_{i,j}(l_{i,j}-1)}{2}} \cdot f_i(2)^{l_{i,j}} \cdot \frac{(2^{f_i(2)})_{l_{i,j}+2}}{(2^{f_i(2)})_2}.$$

Then by [**M2**]

$$\mathrm{pr}_{2,H}(A) = c_{2,H} \cdot r_{2,H}(A) \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_H}(A)|}.$$

The (independent) combination of both probability distributions and conjectures gives the probability distribution

$$\mathrm{pr}_{\mathrm{H}}(A) := \mathrm{pr}_{2,H}(A_2) \cdot \mathrm{pr}_{2',H}(A_{\neq 2}) = c_H \cdot r_H(A) \cdot \frac{1}{|A| \cdot |\mathrm{Aut}_{\mathbb{D}_H}(A)|}$$

on the set of isomorphism classes of finite $e_H\mathbb{Z}^{S_H}\mathbb{D}_H$-modules and the conjecture $\mathcal{M}_\Sigma(A) = \mathrm{pr}_H(A)$, if $\Sigma = (\mathbb{D}_H, \mathbb{Q}, \text{totally real}, S_H, e_H)$, $c_H = c_{2,H} \cdot c_{2',H}$, $r_H(A) = r_{2,H}(A_2)$ and A_2 respectively $A_{\neq 2}$ denotes the 2 and 2′ part of A. By setting $\mathrm{pr}_{\{1\}}(\{1\}) = c_{\{1\}} = r_{\{1\}}(\{1\}) = 1$

and $\mathrm{pr}_{\{1\}}(A) = r_{\{1\}}(A) = 0$ for $A \neq \{1\}$, this probability distribution can be extended to $H = \{1\}$.
All the conjectures above concern distributions of abelian groups. The following conjecture allows to give a heuristic for the distribution of good parts of higher class groups:

Conjecture 12. — *Let G be a finite abelian group, $\mathcal{K}$ the set of all totally real number fields K with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ (in one fixed algebraic closure of $\mathbb{Q}$), $L \in \mathcal{K}$, i a positive integer, $\hat{G} := \mathrm{Gal}(L_{i,f}/\mathbb{Q})$ and H the last non trivial term in the derived series of $\hat{G}$. Set $\hat{\mathcal{K}} = \left\{K_{i,f} \mid K \in \mathcal{K}, \mathrm{Gal}(K_{i,f}/\mathbb{Q}) \cong \hat{G}\right\}$, S to be the set of prime divisors of $|H|$, $e = 1 - \frac{1}{|H|}\sum_{g \in H} g$ and $\Sigma = (\hat{G}, \mathbb{Q}, \text{totally real}, S, e)$. Then*

$$\mathcal{M}_\Sigma(A) = \mathcal{M}_{\hat{\mathcal{K}}}(\chi_{\left\{\mathrm{Cl}^S(K)^e \cong A\right\}})$$

for every finite $e\mathbb{Z}^S\hat{G}$-module A.

For real quadratic number fields this conjecture leads to consider the following probability distribution:

Lemma 13. — *Let $G \in \mathbb{G}$, k_G be the size of the conjugacy class of G/G''-module structures on G'' which belongs to G according to Proposition 3. Then*

$$\mathrm{pr}_{\mathbb{G}}(G) := k_G \cdot \mathrm{pr}_2(G'/G'') \cdot \mathrm{pr}_{G'/G''}(G'')$$

defines a probability distribution on $\mathbb{G}$ and

$$\mathrm{pr}_{\mathbb{G}}(G) = c_2 \cdot c_{G'/G''} \cdot r_{G'/G''}(G'') \cdot \frac{1}{|\mathrm{Aut}(G)|}.$$

Proof. — This is a consequence of Proposition 3 and the definition of $\mathbb{G}$ at the beginning of Chapter 3. □

Since for a quadratic number field K, one has $\mathrm{Gal}(K_{2,f}/\mathbb{Q}) \in \mathbb{G}$, Conjecture 12 and the Cohen-Lenstra heuristic imply the following conjecture (because of Proposition 7 it does not matter if one consider $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ or $\mathrm{Gal}(K_{2,f}/K)$) :

Conjecture 14. — *Let $G \in \mathbb{G}$, let $\mathcal{K}$ be the set of real quadratic number fields and let the map $f : \mathcal{K} \to \mathbb{R}$ be defined by $f(K) = \chi_{\left\{\mathrm{Gal}(K_{2,f}/K) \cong G'\right\}}$. Then $\mathcal{M}_{\mathcal{K}}(f) = \mathrm{pr}_{\mathbb{G}}(G)$.*

Example. — Let K be a real quadratic number and $G = \mathrm{Gal}(K_{2,f}/K)$. Then according to the conjecture a proportion 0.7545 real quadratic fields should have trivial G, 0.0213 should have $G \cong \mathbb{A}_4$ and 0.0000263 should have $G \cong SG(576, 8664)$, where SG denotes the corresponding `SmallGroup` from [**GAP**].

5. Class Group Relations

This chapter collects some lemmas about relations on class groups which are used in the next chapter to compute second class groups of real quadratic fields in practice. The class group relations can all be deduced from the theorems 7.3, 7.6 and 7.8 form **[C-M]** but for concrete calculations with real quadratic fields the following approach is easier to use.

Lemma 15. — *(see* **[C-M**, Chapter 7**]***) Let L/K be a Galois extension of number fields with Galois group G and S the set of primes dividing $(L:K)$.*
(a) If H is a subgroup of G, then $\mathrm{Cl}^S(L^H/K) \cong \mathrm{Cl}^S(L/K)^H$.
(b) If K is a quadratic number field, L/K abelian, $(L:K)$ is odd and N is one of the conjugate subfields of L with $(L:N)=2$, then $\mathrm{Cl}^S(L/K) \cong \mathrm{Cl}^S(N) \oplus \mathrm{Cl}^S(N)$.

Proof. — Statement (a) is well-known (it is Corollaire 7.7 from **[C-M]** for example). Because of Lemma 4 one has $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{D}_G$. Set $A := \mathrm{Cl}^S(L/K)$ and let U be a complement of G in $\mathbb{D}_G$. Proposition 2 (f) and Lemma 1 show that $A^G = \{1\}$ and hence by Lemma 6 one has $A \cong A^U \oplus A^U$ as group. Statement (b) follows from Theorem 7.8 of **[C-M]**. □

Lemma 16. — *(***[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 $\sum_{U \le G} a_U \cdot 1_U^G = 0$ on the induced principal characters. Then:*

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

The following well-known lemma gives the relations of induced principle characters of abelian groups. A proof can be found in **[Bo**, Lemma 3.7**]**.

Lemma 17. — *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 $((G:M) \cdot \chi_{\{N \subseteq M\}} \cdot \chi_{\{N \text{ cyclic}\}})_{N,M}$ in this basis and define $K := \mathrm{Ker}(f)$. Here χ is the characteristic function. Then the following is true:*
(a) If $(a_M)_{M \le G} \in \mathbb{Q}^n$, then $\sum_{M \le G} a_M \cdot 1_M^G = 0$ if and only if $(a_M) \in K$.
(b) Let $H_1, \ldots, H_r$ be the subgroups of G for which G/H_i is not cyclic and let $V_1, \ldots, V_r$ 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 $M_{i,1}, \ldots, M_{i,p_i+1}$ be the subgroups of G between H_i and V_i. Define the vectors $v^1, \ldots, v^r \in \mathbb{Q}^n$ by $v^i_{V_i} = -p_i$, $v^i_{H_i} = -1$, $v^i_{M_{i,j}} = 1$ for all $j = 1, \ldots, p_i+1$ and $v^i_M = 0$ for all other subgroups $M \le G$. Then $v^1, \ldots, v^r$ 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 $\{1\} \neq N \le G$ with G/N not cyclic.

6. Tables

Lemma 18. — *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 $d_N = d_K^{(|G|-1)/2}$.*

Proof. — Let $1, a_1, \ldots, a_{(|G|-1)/2}$ denote representatives of the conjugacy classes of $\mathbb{D}_G$ contained in G and let $\varphi \in \mathbb{D}_G$ be an involution. If H is a group with subgroup U, one can use the definition $1_U^H(x) = \frac{1}{|U|} \cdot |\{g \in H \mid g^{-1}xg \in U\}|$ for all $x \in H$ to calculate the table of character values of $\mathbb{D}_G$. From this one gets

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

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

$$d_{\hat{N}/\mathbb{Q}} \cdot d_{\mathbb{Q}/\mathbb{Q}}^2 = d_{N/\mathbb{Q}}^2 \cdot d_{K/\mathbb{Q}}.$$

In the totally real case, one does not have to distinguish, between $d_{K/\mathbb{Q}}$ and d_K and hence one has $d_{\hat{N}} = d_N^2 \cdot d_K$. Since all occurring fields are totally real and $d_{\mathbb{Q}} = 1$, one has the following equivalences:

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

□

Let K be a real quadratic number field. The calculation of $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ works roughly as follows (the details are explained in [**Bo**, Chapter 5.1]): At first one calculates the class group of K and searches for the dihedral fields contained in $K_{1,f}$ in the tables [**M1**] according to Lemma 18. Their class groups can be found in these tables, too. The three lemmas of the previous chapter allow the calculation of $\mathrm{Cl}^S(L/K_{1,f})$ for all immediate fields L of $K_{2,f}/K_{1,f}$. As in the proof of Proposition 2 (f) one can see that $\mathrm{Cl}^S(L/K_{1,f})$ is isomorphic to the factor commutator group of the subgroup of $\mathrm{Gal}(K_{2,f}/\mathbb{Q})$ which corresponds to L. Now one can use [**GAP**] to look for semidirect products $\mathbb{D}_{\mathrm{Gal}(K_{1,f}/K)} \ltimes \mathrm{Gal}(K_{2,f}/K_{1,f})$ which fulfill the same properties on commutator factor groups of their subgroups.

This procedure does not always work, because the commutator factor groups of subgroups do not determine the group uniquely and because the finite tables from [**M1**] are not complete. There are two non isomorphic groups U, V from $\mathbb{G}$ with $U'/U'' \cong V'/V'' \cong C_5$ and $U'' \cong V'' \cong C_{11}^4$ for example (see [**Bo**, Page 28]). The incompleteness of the tables from [**M1**] restricts the possibilities for $\mathrm{Gal}(K_{1,f}/K)$ to groups with exponent 15 and the possibilities for d_K to some integers smaller then 10^{18}. Nevertheless one can compute the good part of the second class group for a lot of real quadratic number fields in this way. Some of the results can be found in the database `www.mathematik.uni-kl.de/~numberfieldtables`.

Because the conjecture about the distribution of the second class groups of real quadratic number fields depends on Conjecture 12 and the well tested Cohen-Lenstra heuristic, in the following just some tables of number field data are given which shall support Conjecture 12. More evaluations can be found in [**Bo**, Chapter 5.2].

Let H be a finite abelian group of odd order. Let $\mathcal{K}$ be the set of all totally real number fields N (in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$) such that $(N:\mathbb{Q}) = |H|$ and such that $\mathrm{Gal}(\hat{N}/\mathbb{Q}) \cong \mathbb{D}_H$, if $\hat{N}$ denotes the Galois closure of N (in $\overline{\mathbb{Q}}$). Let $\mathcal{K}_1$ denote the subset of $\mathcal{K}$ of all number fields N such that $\hat{N} = K_1$ if K is the quadratic subfield of $\hat{N}$ and $\mathcal{K}_2$ the subset of $\mathcal{K}$ containing all N with $\hat{N} = K_{1,f}$ but $\hat{N} \neq K_1$. The set $\mathcal{K}_3 \subseteq \mathcal{K}$ consists of all N where $\hat{N}$ is unramified over K and contains the maximal abelian unramified p-extensions for all primes dividing $|H|$ and where N is not contained in $\mathcal{K}_i$ for $i < 3$. Let $\mathcal{K}_4$ denote the subset of $\mathcal{K}$ of all N such that N/K is unramified and N is not contained in $\mathcal{K}_i$ for $i < 4$ and $\mathcal{K}_5$ denotes all remaining fields from $\mathcal{K}$. The column labeled with i in the following tables show the proportion of certain class groups in the class group distribution of the fields from $\mathcal{K}_i$ (by Lemma 15 one has $\mathrm{Cl}^S(\hat{N}/K) \cong \mathrm{Cl}^S(N) \oplus \mathrm{Cl}^S(N)$ if S is the set of primes dividing $|H|$).

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

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

Table 2: 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
about 10^{17}	1000000	0.0097	0.0099	0.0098	0.0100	0.0095

Table 2: 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^{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 3: proportion of totally real $\mathbb{D}_5$-fields N of degree 5 with trivial $10'$-class group

References

[Ba] 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, Cambridge 1995.

[Bo] M. Boy: *On the second class group of real quadratic number fields*, Dissertation, TU Kaiserslautern, Kaiserslautern 2012.

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

[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.

[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, Providence 1976.

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

[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.

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

[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*, Springer-Verlag, New York 1979.

[Su] M. Suzuki: *Group theory I*, Springer-Verlag, New York 1982.

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

---

23 mai 2012

Maximilian Boy, Sonnenbergstraße 6E, 70184 Stuttgart • *E-mail :* Maximilian.Boy@p3-group.com