A CLASS GROUP HEURISTIC BASED ON THE DISTRIBUTION OF 1-EIGENSPACES IN MATRIX GROUPS

MICHAEL ADAM AND GUNTER MALLE

Abstract. We propose a modification to the Cohen–Lenstra prediction for the distribution of class groups of number fields, which should also apply when the base field contains non-trivial roots of unity. The underlying heuristic derives from the distribution of 1-eigenspaces in certain generalized symplectic groups over finite rings. The motivation for that heuristic comes from the function field case. We also give explicit formulas for the new predictions in several important cases. These are in close accordance with known data.

1. Introduction

The class group of a number field K is defined as the quotient $\mathrm{Cl}(K) := I_K/P_K$ of the group of fractional ideals I_K by the subgroup of principal ideals P_K in the ring of integers $\mathcal{O}_K$ of K. Despite its importance, not much is known about the behavior of these objects. For instance it is still an open question whether there exist infinitely many number fields with trivial class group. In the early 1980's H. Cohen and H.W. Lenstra [6] proposed a heuristic principle, later extended by Cohen and J. Martinet [7], which makes predictions on how often a given finite abelian p-group should appear as the p-part $\mathrm{Cl}(K)_p$ of the class group in a specified set of number fields. Only very few instances of these conjectures have been proved (see [5, 10] for important recent progress).

In 2008 it was noticed by the second author [13, 14] that when the base field K_0 contains pth roots of unity the probabilities postulated by Cohen and Martinet do not match with computational data. In particular this is always the case for $p = 2$. In the absence of theoretical arguments, on the basis of his computational data the second author came up with a conjectural statement [14, Conj. 2.1] describing the behavior of p-parts of class groups in the presence of pth roots of unity in K_0.

Motivated by the works of J. Achter [1, 2] who considered the analogous problem on the function field side, we develop a method which can be seen as a theoretical justification for the heuristics of Cohen and Martinet and at the same time for the conjecture in [14]. Our main objects are 1-eigenspaces of elements in what we call the m-th symplectic groups $\mathrm{Sp}_{2n}^{(m)}(R)$ over certain finite rings R (see Definition 3.1). The limit for $n \to \infty$ of these eigenspace distributions should then give the right predictions for class group distributions over number fields.

Date: October 1, 2014.

1991 *Mathematics Subject Classification.* Primary 11R29, 15B33; Secondary 20P05.

Key words and phrases. Cohen–Lenstra heuristic, class groups, symplectic groups, 1-eigenspaces.

The authors gratefully acknowledge financial support by the Deutsche Forschungsgemeinschaft.

We use the results proved by the first author [4] to compute distributions in these m-th symplectic groups (see Theorems 4.4 and 4.6) which allows us to make conjectural predictions (see Conjecture 5.1) about the behavior of p-parts of class groups of number fields. For the case when the base field does not contain pth roots of unity, these specialize to the original Cohen–Lenstra–Martinet predictions (see Example 5.2).

2. Cohen–Lenstra heuristic and roots of unity

In this section we recall the heuristic principle introduced by Cohen and Lenstra to predict the distribution of p-parts of class groups of imaginary quadratic number fields and the generalization to arbitrary number fields proposed by Cohen and Martinet. However, our focus lies on a situation where these predictions seem to fail.

2.1. **The Cohen–Lenstra heuristic.** Following Cohen and Lenstra [6] we equip finite groups G with their *CL-weight* $\omega(G) := \dfrac{1}{|\mathrm{Aut}(G)|}$. For integers $q, r \geq 1$ we set

$$(q)_r := \prod_{i=1}^{r}(1-q^{-i}) \quad \text{and} \quad (q)_\infty := \prod_{i=1}^{\infty}(1-q^{-i}).$$

For a prime p, let $\mathcal{G}_p$ denote the set of all isomorphism classes of finite abelian p-groups. From [6, Ex. 5.10] we have:

Corollary 2.1. *The function given by*

$$P_{CL} : \mathcal{G}_p \longrightarrow [0,1],\ G \mapsto \frac{(p)_\infty}{|\mathrm{Aut}(G)|},$$

defines a probability distribution on $\mathcal{G}_p$.

This very natural distribution on the set of finite abelian p-groups occurs also in many other contexts; see [12] for an overview.

In order to present the results of Cohen and Martinet [7] we need to introduce the following setup.

Definition 2.2. We call a triple $\Sigma := (H, K_0, \sigma)$ a *situation*, where
(1) $H \leq \mathfrak{S}_n$ is a transitive permutation group of degree $n \geq 2$,
(2) K_0 is a number field, and
(3) σ is a signature which may occur as signature of a degree n extension K/K_0 with Galois group (of the Galois closure) permutation isomorphic to H.

For a situation $\Sigma = (H, K_0, \sigma)$ we let $\mathcal{K}(\Sigma)$ denote the set of number fields K/K_0 (inside a fixed algebraic closure) as described in (3).

To a given situation Σ one can attach a non-negative rational number $u(\Sigma)$, the *unit rank* and a ring $\mathcal{O}(\Sigma)$. We give the definition of these terms in a very important special case, the general case is explained in [7, Chap. 6].

We write χ for the permutation character attached to the embedding $H \leq \mathfrak{S}_n$. It contains the trivial character 1_H exactly once, and we let $\chi_1 := \chi - 1_H$. We assume that χ_1 is the character of an irreducible (but not necessarily absolutely irreducible) H-module;

and that any absolutely irreducible constituent φ of χ_1 has Schur index 1. Then $\mathcal{O}(\Sigma)$ is the ring of integers of the field of values of any absolutely irreducible constituent of χ_1.

Now for $K \in \mathcal{K}(\Sigma)$ let L denote the Galois closure of K/K_0. The action of H makes $\mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{Q}$ into a $\mathbb{Q}[H]$-module whose character we denote by χ_L. Then

$$u(\Sigma) := \langle \chi_L, \varphi \rangle$$

(see [7, p. 63]), the scalar product of the character χ_L with an absolutely irreducible constituent φ of χ_1. Since χ_L is rational, this does not depend on the choice of φ (nor does it depend on the choice of $K \in \mathcal{K}(\Sigma)$).

Given a situation $\Sigma = (H, K_0, \sigma)$ and a finite $\mathfrak{p}$-torsion $\mathcal{O} = \mathcal{O}(\Sigma)$-module G, where $\mathfrak{p} \trianglelefteq \mathcal{O}$ is a prime ideal, we set

$$\mathcal{N}_\Sigma(G) := \lim_{x\to\infty} \frac{|\{K \in \mathcal{K}(\Sigma) : d_{K/K_0} \leq x,\ \mathrm{Cl}(K/K_0)_{\mathfrak{p}} \cong G\}|}{|\{K \in \mathcal{K}(\Sigma) : d_{K/K_0} \leq x\}|}$$

(if it exists), where d_{K/K_0} denotes the norm of the discriminant of K/K_0 and $\mathrm{Cl}(K/K_0)$ is the relative class group of K/K_0 (the kernel in the class group of K of the norm map from K to K_0). With this we can present the conjecture of Cohen and Martinet [7, Chap. 6] predicting the distribution of $\mathfrak{p}$-parts of relative class groups of number fields over K_0.

Conjecture 2.3 (Cohen and Martinet)**.** *Let G be a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module, with $\mathfrak{p} \nmid n$. Then $\mathcal{N}_\Sigma(G)$ exists and is given by*

$$\frac{(q)_\infty}{(q)_u} \cdot \frac{1}{|G|^u |\mathrm{Aut}_{\mathcal{O}}(G)|},$$

where $u := u(\Sigma)$, $q := |\mathcal{O}/\mathfrak{p}|$, and $\mathrm{Aut}_{\mathcal{O}}(G)$ denotes the group of $\mathcal{O}$-automorphisms of G

Subsequently it was noticed that this conjecture cannot hold for all primes which were originally allowed by Cohen and Martinet. The reason why Cohen and Martinet excluded the primes that divided the extension degree $n = (K/K_0)$ is that by genus theory the conjecture cannot be true for such primes. A few years later and after more computations Cohen and Martinet [8] were forced to enlarge the set of bad primes by those which divide the order of the common Galois group H of the situation Σ. For the bad behavior of these primes one can find theoretical arguments in the spirit of genus theory, too. Much later it was noticed by the second author [13, 14] on the basis of extensive numerical support that the presence of pth roots of unity in the base field K_0 does play a role for the distribution of p-parts of class groups. In an attempt to explain this deviation, one is led to consider the analogous situation on the side of function fields.

2.2. **The function field case.** Three years after [6], E. Friedman and L.C. Washington [11] linked the distribution of p-parts of the divisor class groups of degree 0 of quadratic extensions of $\mathbb{F}_l(t)$ to equi-distributed sequences of matrices over finite fields. This was extended by J. Achter as follows. Let $\mathcal{H}_g(\mathbb{F}_l)$ denote the set of monic separable polynomials of degree g over the finite field $\mathbb{F}_l$ and let $C_{g,f}$ be the hyperelliptic curve of genus g defined by $f \in \mathcal{H}_{2g+1}(\mathbb{F}_l)$. Achter [1, 2] showed that for a finite abelian p-group G

$$\lim_{l\to\infty} \frac{|\{f \in \mathcal{H}_{2g+1}(\mathbb{F}_l) : \mathrm{Cl}^0(C_{g,f})_p \cong G\}|}{|\mathcal{H}_{2g+1}(\mathbb{F}_l)|} = \frac{|\{h \in \mathrm{Sp}_{2g}(\mathbb{F}_p) : \ker(h - \mathbf{1}_{2g}) \cong G\}|}{|\mathrm{Sp}_{2g}(\mathbb{F}_p)|},$$

where $\mathrm{Cl}^0(C_{g,f})_p$ is the Sylow p-subgroup of the Jacobian of $C_{g,f}$. Later Achter [2, Thm. 3.1] established a correspondence between eigenspace distributions in symplectic similitude groups over finite rings and the distribution of the Jacobian of hyperelliptic curves. These distributions were computed explicitely by J.S. Ellenberg, A. Venkatesh and C. Westerland [9] and one consequence of their work is that the distribution of the p-parts of divisor class groups of degree 0 of quadratic function fields over $\mathbb{F}_l$ with $p \not| (l-1)$ (which corresponds on the number field side to the case where pth roots of unity are not contained in the base field) matches the distributions predicted by Cohen–Lenstra and Friedman–Washington. Following [14, §3] the philosophy should now be that the characteristic 0 number field case can be obtained as the limit for the genus $g \to \infty$ of the characteristic l function field cases.

3. Distribution of 1-eigenspaces in matrix groups

The ideas and results from the function field case yield the motivation for a more thorough investigation of eigenspaces in suitable finite matrix groups. Since all finite abelian p-groups should occur as such eigenspaces, and should carry an alternating form coming from the Tate pairing, we are led to consider symplectic groups over finite rings that are not integral domains. We introduce these groups and recall the crucial results shown by the first author in [4].

Definition 3.1. Let $\mathcal{O}$ be the ring of integers of a number field and let $\mathfrak{p} \trianglelefteq \mathcal{O}$ be a non-zero prime ideal. Given natural numbers n and $m \leq f$ we define the *m-th symplectic group* over the ring $\mathcal{O}/\mathfrak{p}^f$ as

$$\mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^f) := \{h \in \mathrm{GL}_{2n}(\mathcal{O}/\mathfrak{p}^f) \mid h^t J_n h \equiv J_n \pmod{\mathfrak{p}^m}\},$$

where $\mathrm{GL}_{2n}(\mathcal{O}/\mathfrak{p}^f)$ is the general linear group and $J_n := \begin{pmatrix} 0 & \mathbf{1}_n \\ -\mathbf{1}_n & 0 \end{pmatrix} \in \mathrm{GL}_{2n}(\mathcal{O}/\mathfrak{p}^f)$.

Remark 3.2. From the definition we obtain the following descending chain of groups:

$$\mathrm{GL}_{2n}(\mathcal{O}/\mathfrak{p}^f) = \mathrm{Sp}_{2n}^{(0)}(\mathcal{O}/\mathfrak{p}^f) \supseteq \mathrm{Sp}_{2n}^{(1)}(\mathcal{O}/\mathfrak{p}^f) \supseteq \cdots \supseteq \mathrm{Sp}_{2n}^{(f)}(\mathcal{O}/\mathfrak{p}^f) = \mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^f),$$

where $\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^f)$ denotes the usual symplectic group over $\mathcal{O}/\mathfrak{p}^f$. Thus, the m-th symplectic groups in a sense 'interpolate' between the general linear and the symplectic group over the non-integral domain $\mathcal{O}/\mathfrak{p}^f$.

Proposition 3.3. *Let $q := |\mathcal{O}/\mathfrak{p}|$ and $f \in \mathbb{N}$. Then:*
(a) $|\mathrm{Sp}_{2n}^{(0)}(\mathcal{O}/\mathfrak{p}^f)| = |\mathrm{GL}_{2n}(\mathcal{O}/\mathfrak{p}^f)| = q^{4n^2(f-1)} \cdot |\mathrm{GL}_{2n}(\mathbb{F}_q)|$.
(b) $|\mathrm{Sp}_{2n}^{(f)}(\mathcal{O}/\mathfrak{p}^f)| = |\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^f)| = q^{(2n^2+n)(f-1)} \cdot |\mathrm{Sp}_{2n}(\mathbb{F}_q)|$.
(c) $|\mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^f)| = q^{4n^2(f-m)} \cdot |\mathrm{Sp}_{2n}(\mathcal{O}/\mathfrak{p}^m)|$ *for* $1 \leq m \leq f-1$.

Proof. See [4, Prop. 2.7]. □

We are interested in the following limit proportion of elements with a given 1-eigenspace

$$P_{m,q}(G) := \lim_{n\to\infty} \frac{|\{g \in \mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^f) : \ker(g - \mathbf{1}_{2n}) \cong G\}|}{|\mathrm{Sp}_{2n}^{(m)}(\mathcal{O}/\mathfrak{p}^f)|},$$

where G denotes a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module. Note that this is trivially a probability measure on the set of finite $\mathfrak{p}$-torsion $\mathcal{O}$-modules. For $m \leq 2$ this distribution was computed explicitely in [4, Thms. 3.8 and 3.23], respectively [3, Rem. 4.27]:

Theorem 3.4. *Let G be a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module annihilated by $\mathfrak{p}^{f-1}$. Then:*

(a) $P_{0,q}(G) = \dfrac{(q)_\infty}{|\mathrm{Aut}_{\mathcal{O}}(G)|}$,

(b) $P_{1,q}(G) = \dfrac{(q)_\infty}{(q^2)_\infty} \cdot \dfrac{(q)_r \cdot q^{\binom{r}{2}}}{|\mathrm{Aut}_{\mathcal{O}}(G)|}$ *with* $r = \mathrm{rk}_{\mathfrak{p}}(G)$,

(c) $P_{2,q}(G) = \dfrac{(q)_\infty}{(q^2)_\infty} \cdot \dfrac{(q)_{r-s}(q)_s \cdot q^{\binom{r}{2}+\binom{s}{2}}}{(q^2)_t \, |\mathrm{Aut}_{\mathcal{O}}(G)|}$ *with* $r = \mathrm{rk}_{\mathfrak{p}}(G)$, $s = \mathrm{rk}_{\mathfrak{p}^2}(G)$, $t = \lfloor \frac{r-s}{2} \rfloor$,

where $q := |\mathcal{O}/\mathfrak{p}|$, *and* $\mathrm{rk}_{\mathfrak{p}}(G)$ *denotes the rank of* G *as a* $\mathfrak{p}$*-module.*

In particular one sees that the limit does not depend on $\mathcal{O}$ and $\mathfrak{p}$, but only on q, and is also independent of f, as long as G is annihilated by $\mathfrak{p}^{f-1}$, which justifies our choice of notation. The value of $|\mathrm{Aut}_{\mathcal{O}}(G)|$ is computed explicitly in [7, Thm. 2.11].

Remark 3.5. We have no closed formulas for $P_{m,q}(G)$ for $m \geq 3$ and general G, but for fixed m and G it is possible to calculate $P_{m,q}(G)$ explicitly, as indicated in [4].

4. u-Probabilities

The concept of u-probability was originally introduced by Cohen and Lenstra (see [6, Chap. 5]). Here we present a modified version used by various other authors (e.g. J. Lengler [12]). Throughout, $\mathcal{O}$ denotes the ring of integers of an algebraic number field, $\mathfrak{p} \trianglelefteq \mathcal{O}$ is a non-zero prime ideal, and $q := |\mathcal{O}/\mathfrak{p}|$. We let $\mathcal{P}$ denote the set of isomorphism classes of finite $\mathfrak{p}$-torsion $\mathcal{O}$-modules.

Definition 4.1. Given a probability distribution P on $\mathcal{P}$ and a natural number u we define the *u-probability distribution* with respect to P by the following recursion formula

$$P^{(u)} : \mathcal{P} \longrightarrow \mathbb{R}, \quad G \mapsto P^{(u)}(G) := \sum_{H \in \mathcal{P}} \sum_{\substack{y \in H \\ H/\langle y \rangle \cong G}} \frac{P^{(u-1)}(H)}{|H|},$$

where $P^{(0)}(G) := P(G)$ for $G \in \mathcal{P}$. Here, $\langle y \rangle$ denotes the $\mathcal{O}$-submodule generated by y. We call $P^{(u)}(G)$ the *u-probability* of G (with respect to P).

Remark 4.2. Note that $P^{(u)}$ is in fact a probability distribution on $\mathcal{P}$, since

$$\sum_{G \in \mathcal{P}} P^{(1)}(G) = \sum_{H \in \mathcal{P}} \sum_{G \in \mathcal{P}} \frac{|\{y \in H \mid H/\langle y \rangle \cong G\}|}{|H|} \cdot P(H) = \sum_{H \in \mathcal{P}} P(H) = 1$$

for any probability distribution P on $\mathcal{P}$, and $P^{(u+1)} = (P^{(u)})^{(1)}$.

We now compute the u-probabilities for the distributions $P_{i,q}$ given in Theorem 3.4. For $G \in \mathcal{P}$ a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module of rank $\mathrm{rk}_{\mathfrak{p}}(G) = r$ and $k \geq 0$ we set

$$w_k(G) := \begin{cases} \dfrac{(q)_k}{(q)_{k-r}|\mathrm{Aut}_{\mathcal{O}}(G)|} & \text{if } k \geq r, \\ 0 & \text{else,} \end{cases}$$

and $w_\infty(G) := |\mathrm{Aut}_\mathcal{O}(G)|^{-1} = \lim_{k\to\infty} w_k(G)$.

With this we recall the following crucial result from [6, Thm. 3.5]:

Proposition 4.3. *Let $Z, G \in \mathcal{P}$. Then for all $0 \le k \le \infty$ we have*

$$\sum_{H\in\mathcal{P}} w_k(H)|\{H_1 \le H : H_1 \cong Z,\ H/H_1 \cong G\}| = w_k(Z)w_k(G).$$

Theorem 4.4. *Let G be a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module, and $q := |\mathcal{O}/\mathfrak{p}|$. Then*

$$P_{0,q}^{(u)}(G) = \frac{(q)_\infty}{(q)_u} \cdot \frac{1}{|G|^u|\mathrm{Aut}_\mathcal{O}(G)|}$$

for all integers $u \ge 0$.

Proof. The induction base $u = 0$ is given by Theorem 3.4, so now let $u \ge 1$. By Proposition 4.3 with $k = \infty$ we have

$$\sum_{H\in\mathcal{P}} \frac{|\{H_1 \le H : H_1 \cong Z,\ H/H_1 \cong G\}|}{|\mathrm{Aut}_\mathcal{O}(H)|} = \frac{1}{|\mathrm{Aut}_\mathcal{O}(Z)||\mathrm{Aut}_\mathcal{O}(G)|}$$

for any $Z \in \mathcal{P}$. With $Z = \mathcal{O}/\mathfrak{p}^n\mathcal{O}$ this gives

$$\sum_{\substack{H\in\mathcal{P}\\ |H|=q^n|G|}} \frac{|\{y \in H : |\langle y\rangle| = q^n,\ H/\langle y\rangle \cong G\}|}{|\mathrm{Aut}_\mathcal{O}(H)|} = \frac{1}{|\mathrm{Aut}_\mathcal{O}(G)|}.$$

Multiplying this equation by $(q^n|G|)^{-u}$ and summing over all $n \in \mathbb{N}$ we obtain

$$\sum_{n\ge 0} \sum_{\substack{H\in\mathcal{P}\\ |H|=q^n|G|}} \frac{|\{y \in H : |\langle y\rangle| = q^n,\ H/\langle y\rangle \cong G\}|}{|H|^u|\mathrm{Aut}_\mathcal{O}(H)|} = \sum_{n\ge 0} \frac{1}{q^{un}|G|^u|\mathrm{Aut}_\mathcal{O}(G)|}$$

which by induction is equivalent to

$$\frac{(q)_{u-1}}{(q)_\infty} \sum_{H\in\mathcal{P}} \sum_{\substack{y\in H\\ H/\langle y\rangle\cong G}} \frac{P_{0,q}^{(u-1)}(H)}{|H|} = \frac{1}{|G|^u|\mathrm{Aut}_\mathcal{O}(G)|} \sum_{n\ge 0} \frac{1}{q^{un}} = \frac{1}{(q^u)_1\,|G|^u|\mathrm{Aut}_\mathcal{O}(G)|}.$$

□

Next, we determine the u-probabilities for the distribution given by the first symplectic groups. For this we show first the following result.

Lemma 4.5. *For $G \in \mathcal{P}$ of $\mathfrak{p}$-rank r and all $u \in \mathbb{N}$ we have*

$$\sum_{\substack{H\in\mathcal{P}\\ \mathrm{rk}_\mathfrak{p}(H)=r}} \frac{|\{y \in H : H/\langle y\rangle \cong G\}|}{|H|^u|\mathrm{Aut}_\mathcal{O}(H)|} = \frac{q^{r+u}-1}{q^r(q^u-1)} \cdot \frac{1}{|G|^u|\mathrm{Aut}_\mathcal{O}(G)|}.$$

Proof. Let $u \in \mathbb{N}$. Splitting up the sum in question according to the order of y we get

$$\sum_{\substack{H\in\mathcal{P}\\ \mathrm{rk}_\mathfrak{p}(H)=r}} \frac{|\{y \in H \mid H/\langle y\rangle \cong G\}|}{|H|^u|\mathrm{Aut}_\mathcal{O}(H)|} = \sum_{n\ge 0} \sum_{\substack{H\in\mathcal{P}\\ \mathrm{rk}_\mathfrak{p}(H)=r}} \frac{|\{y \in H : |\langle y\rangle| = q^n,\ H/\langle y\rangle \cong G\}|}{|H|^u|\mathrm{Aut}_\mathcal{O}(H)|}.$$

Writing $Z_n := \mathcal{O}/\mathfrak{p}^n\mathcal{O}$, the inner sum equals

$$\sum_{\substack{H\in\mathcal{P}\\ \mathrm{rk}_{\mathfrak{p}}(H)=r}} |\mathrm{Aut}_{\mathcal{O}}(Z_n)| \cdot \frac{|\{H_1 \le H : H_1 \cong Z_n,\ H/\langle H_1\rangle \cong G\}|}{|H|^u|\mathrm{Aut}_{\mathcal{O}}(H)|}$$

$$= \frac{|\mathrm{Aut}_{\mathcal{O}}(Z_n)|}{(q)_r|G|^u q^{nu}} \sum_{H\in\mathcal{P}} w_r(H)\,|\{H_1 \le H : H_1 \cong Z_n,\ H/\langle H_1\rangle \cong G\}|$$

$$= \frac{|\mathrm{Aut}_{\mathcal{O}}(Z_n)|}{(q)_r|G|^u q^{nu}}\, w_r(Z_n) w_r(G) \qquad \text{by Proposition 4.3.}$$

Note that the middle sum may be extended over all H, since $w_r(H) = 0$ if $\mathrm{rk}_{\mathfrak{p}}(H) > r$. Now $w_r(Z_0) = 1$ and $w_r(Z_n) = (q)_r/(q)_{r-1}|\mathrm{Aut}_{\mathcal{O}}(Z_n)|^{-1}$ when $n > 0$, so the left hand side in the assertion becomes

$$\frac{w_r(G)}{(q)_r|G|^u}\left(1 + \sum_{n\ge1} \frac{w_r(Z_n)|\mathrm{Aut}_{\mathcal{O}}(Z_n)|}{q^{nu}}\right) = \frac{w_r(G)}{(q)_r|G|^u}\left(1 + \frac{(q)_r}{(q)_{r-1}} \sum_{n\ge1} \frac{1}{q^{nu}}\right)$$

$$= \frac{1}{|G|^u|\mathrm{Aut}_{\mathcal{O}}(G)|}\Big(1 + (1-q^{-r})\frac{1}{q^u-1}\Big)$$

$$= \frac{q^{r+u}-1}{q^r(q^u-1)} \cdot \frac{1}{|G|^u|\mathrm{Aut}_{\mathcal{O}}(G)|}$$

as claimed. □

Theorem 4.6. *Let G be a finite $\mathfrak{p}$-torsion $\mathcal{O}$-module of rank r, and $q := |\mathcal{O}/\mathfrak{p}|$. Then*

$$P_{1,q}^{(u)}(G) = \frac{(q^2)_u(q)_\infty}{(q)_u(q^2)_\infty} \cdot \frac{(q)_{r+u}q^{\binom{r}{2}}}{(q)_u|G|^u|\mathrm{Aut}_{\mathcal{O}}(G)|}.$$

Proof. Let $G \in \mathcal{P}$ of $\mathfrak{p}$-rank r. The case $u = 0$ holds by Theorem 3.4(b). So by induction and Definition 4.1 we need to compute

$$\frac{(q^2)_{u-1}(q)_\infty}{(q)_{u-1}(q^2)_\infty}\Big((q)_{r+u-1}\, q^{\binom{r}{2}}\, X(r) + (q)_{r+u}\, q^{\binom{r+1}{2}} X(r+1)\Big)$$

where

$$X(s) := \sum_{\substack{H\in\mathcal{P}\\ \mathrm{rk}_{\mathfrak{p}}(H)=s}} \sum_{\substack{y\in H\\ H/\langle y\rangle\cong G}} \frac{1}{(q)_{u-1}|H|^u|\mathrm{Aut}_{\mathcal{O}}(H)|} \qquad \text{for } s \in \{r, r+1\}.$$

With

$$Y := \frac{1}{(q)_u|G|^u|\mathrm{Aut}_{\mathcal{O}}(G)|}$$

Lemma 4.5 states that $X(r) = \dfrac{q^{r+u}-1}{q^{r+u}} \cdot Y$, and Theorem 4.4 gives $Y = X(r) + X(r+1)$, so

$$X(r+1) = Y - X(r) = \Big(1 - \frac{q^{r+u}-1}{q^{r+u}}\Big)Y = \frac{1}{q^{r+u}}\,Y.$$

Then the left hand side of the assertion becomes

$$\frac{(q^2)_{u-1}(q)_\infty\, q^{\binom{r}{2}}}{(q)_{u-1}(q^2)_\infty}\Big((q)_{r+u-1}\,\frac{q^{r+u}-1}{q^{r+u}}+(q)_{r+u}\,q^r\,\frac{1}{q^{r+u}}\Big)\,Y$$

$$=\frac{(q^2)_{u-1}(q)_\infty(q)_{r+u}\,q^{\binom{r}{2}}}{(q)_{u-1}(q^2)_\infty q^u}(q^u+1)\,Y=\frac{(q^2)_u(q)_\infty}{(q)_u(q^2)_\infty}\cdot\frac{(q)_{r+u}\,q^{\binom{r}{2}}}{(q)_u|G|^u|\mathrm{Aut}_{\mathcal{O}}(G)|}$$

as claimed. □

5. Distribution of class groups of number fields

We can now present our conjecture about the distribution of p-parts of class groups using the results from the last section. Here we restrict ourselves to situations Σ such that $\mathcal{O}(\Sigma)=\mathbb{Z}$.

Conjecture 5.1. *Let p be a prime, $\Sigma=(H,K_0,\sigma)$ be a situation with $\gcd(p,|H|)=1$ such that $\mathcal{O}(\Sigma)=\mathbb{Z}$, and K_0 be a number field containing the p^mth but not the p^{m+1}th roots of unity. Then a given finite abelian p-group G occurs as the p-part of a relative class group $\mathrm{Cl}(K/K_0)$ for $K\in\mathcal{K}(\Sigma)$ with probability $P_{m,p}^{(u)}(G)$, where $u=u(\Sigma)$.*

Let us consider some special cases of this conjecture in which we have derived explicit formulas.

Example 5.2. In the case $m=0$, which should correspond to situations were no non-trivial pth roots of unity are contained in the base field, Theorem 4.4 yields that the probability in Conjecture 5.1 that a finite abelian p-group G occurs as the p-part of a class group is given by

$$P_{0,p}^{(u)}(G)=\frac{(p)_\infty}{(p)_u}\cdot\frac{1}{|G|^u|\mathrm{Aut}(G)|}.$$

This is exactly the probability predicted by Cohen, Lenstra and Martinet (see Conjecture 2.3).

Example 5.3. Next consider the case $m=1$, which should apply when pth but no higher roots of unity are present. Then by Theorem 4.6 the distribution in Conjecture 5.1 is given by

$$P_{1,p}^{(u)}(G)=\frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty}\cdot\frac{(p)_{r+u}p^{\binom{r}{2}}}{(p)_u|G|^u|\mathrm{Aut}(G)|}.$$

This distribution is exactly the one proposed by the second author in [14, Conj. 2.1] for the case when the base field contains pth but no higher roots of unity. This was derived from, and is in very close accordance with, huge amounts of computational data in a number of situations, see [14] for details, but had no heuristic underpinning. Our approach via eigenspaces in mth symplectic groups gives a theoretical explanation for the above formula. As shown in [14, Prop. 2.2], the probability for a class group to have p-rank r would then equal

$$\frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty}\cdot\frac{1}{p^{r(r+2u+1)/2}\,(p)_r}.$$

Example 5.4. Finally, assume that $m = 2$, which should apply if the p^2rd but no higher roots of unity are present in the base field. For $u = 0$, the value of $P_{2,p}^{(0)}(G)$ is given in Theorem 3.4(c). The general formulae for $u \geq 1$ seem to get quite messy, therefore we only give some example values. When $u = 1$ we find

$$P_{2,p}^{(1)}(\mathbb{Z}/p^k\mathbb{Z}) = \frac{(p^2)_u(p)_\infty}{(p)_u(p^2)_\infty} \cdot \frac{(p)_{r+u}\, p^{\binom{r}{2}}}{(p)_u|\mathbb{Z}/p^k\mathbb{Z}|^u\, |\mathrm{Aut}(\mathbb{Z}/p^k\mathbb{Z})|}$$

(for this calculation we have to sum over groups of types $\mathbb{Z}/p^\alpha\mathbb{Z}\times\mathbb{Z}/p^\beta\mathbb{Z}$ with $\alpha \geq k \geq \beta$), while for the smallest non-cyclic p-group the result is

$$P_{2,p}^{(1)}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) = \frac{(p)_\infty}{(p^2)_\infty} \cdot \frac{p^3+p^2-1}{p^7(p-1)}.$$

From the previous result we obtain

$$P_{2,p}^{(2)}(1) = \frac{(p^4)_1(p)_\infty}{(p)_1(p^2)_\infty}$$

for the trivial group at $u = 2$.

One might expect that the case $\mathcal{O} \neq \mathbb{Z}$ can be treated with similar methods as those presented above. The main problem seems to be to find a suitable adaptation of the concept of u-probability to the case of $\mathfrak{p}$-torsion modules. The obvious approach does not seem to yield results which are in agreement with computational data from [13, 14].

References

[1] J. D. Achter, The distribution of class groups of function fields. J. Pure and Appl. Algebra **204** (2006), 316–333.

[2] ———, Results of Cohen–Lenstra type for quadratic function fields. In: *Computational arithmetic geometry*, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, 1–7.

[3] M. Adam, On the distribution of eigenspaces in classical groups over finite rings and the Cohen–Lenstra heuristic. Dissertation, TU Kaiserslautern, 2014.

[4] ———, On the distribution of eigenspaces in classical groups over finite rings. Linear Algebra Appl. **443** (2014), 50–65.

[5] M. Bhargava, The density of discriminants of quartic rings and fields. Ann. of Math. (2) **162** (2005), 1031–1063.

[6] H. Cohen, H. W. Lenstra Jr., Heuristics on class groups of number fields. In: *Number theory, Noordwijkerhout 1983* (Noordwijkerhout, 1983). Springer, Berlin, 1984, 33–62.

[7] H. Cohen, J. Martinet, Étude heuristique des groupes de classes des corps de nombres. J. reine angew. Math. **404** (1990), 39–76.

[8] ———, Heuristics on class groups: some good primes are not too good. Math. Comp. **63** (1994), 329–334.

[9] J. S. Ellenberg, A. Venkatesh, C. Westerland, *Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields.* arXiv:0912.0325 (2009).

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

[11] E. Friedman, L. C. Washington, On the distribution of divisor class groups of curves over a finite field. In: *Théorie des nombres* (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, 227–239.

[12] J. Lengler, The Cohen–Lenstra heuristic: methodology and results. J. Algebra **323** (2010), 2960–2976.

[13] G. Malle, Cohen–Lenstra heuristic and roots of unity. J. Number Theory **128** (2008), 2823–2835.

[14] ______, On the distribution of class groups of number fields. Experiment. Math. **19** (2010), 465–474.

FB Mathematik, TU Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany.
E-mail address: adam@mathematik.uni-kl.de
E-mail address: malle@mathematik.uni-kl.de