MATHEMATICS OF COMPUTATION
Volume 74, Number 250, Pages 937–947
S 0025-5718(04)01725-9
Article electronically published on October 27, 2004

p-CLASS GROUPS OF CERTAIN EXTENSIONS OF DEGREE p

CHRISTIAN WITTMANN

Abstract. Let p be an odd prime number. In this article we study the distribution of p-class groups of cyclic number fields of degree p, and of cyclic extensions of degree p of an imaginary quadratic field whose class number is coprime to p. We formulate a heuristic principle predicting the distribution of the p-class groups as Galois modules, which is analogous to the Cohen-Lenstra heuristics concerning the prime-to-p-part of the class group, although in our case we have to fix the number of primes that ramify in the extensions considered. Using results of Gerth we are able to prove part of this conjecture. Furthermore, we present some numerical evidence for the conjecture.

1. Introduction

Let p be an odd prime number throughout this paper. If $K/\mathbb{Q}$ is a cyclic number field of degree p, the Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$ acts on the class group $\mathcal{Cl}(K)$. Since the norm element $\phi = 1 + \sigma + \cdots + \sigma^{p-1}$ annihilates the class group and $\mathbb{Z}[\sigma]/(\phi) \cong \mathbb{Z}[\omega]$, we see that $\mathcal{Cl}(K)$ is a $\mathbb{Z}[\omega]$-module, where ω is a primitive pth root of unity. Furthermore, the class group decomposes in a natural way into $\mathcal{Cl}(K) = \mathcal{Cl}(K)_p \oplus \mathcal{Cl}(K)_{\neq p}$, where $\mathcal{Cl}(K)_p$ is the p-Sylow subgroup, and $\mathcal{Cl}(K)_{\neq p}$ is the prime-to-p-part of the class group.

The goal of this paper is to describe the distribution of the p-class group $\mathcal{Cl}(K)_p$ as K varies over all cyclic number fields of degree p. The corresponding problem for $\mathcal{Cl}(K)_{\neq p}$ was investigated by Cohen and Lenstra and led to their famous heuristic principle (cf. [3]). According to this conjecture, for a given $\mathbb{Z}[\omega]$-module M the ratio of number fields K satisfying $\mathcal{Cl}(K)_{\neq p} \cong_{\mathbb{Z}[\omega]} M$ among all cyclic number fields of degree p is proportional to $|\mathrm{Aut}_{\mathbb{Z}[\omega]}(M)|^{-1}|M|^{-1}$. This conjecture is still unproved, but supported by numerical verifications. However, the p-part had to be excluded in their heuristics, the reason being that it is determined by genus theory to some extent. More precisely, the cardinality of $\mathcal{Cl}(K)_p$ increases as the number of primes that ramify in K increases.

The main idea in formulating an analogous conjecture for the p-part is to fix the number of primes that ramify in the extension $K/\mathbb{Q}$. Note that $\mathcal{Cl}(K)_p$ can be regarded as a $\mathbb{Z}_p[\omega]$-module, where $\mathbb{Z}_p$ is the ring of p-adic integers. Now (a special case of) our conjecture can be stated as follows: Let $t \geq 1$ be an integer and M_0 be an arbitrary finite $\mathbb{Z}_p[\omega]$-module with $|M_0/(1-\omega)M_0| = p^{t-1}$. Then the ratio of number fields K such that $\mathcal{Cl}(K)_p \cong_{\mathbb{Z}_p[\omega]} M_0$ among all cyclic number fields of

Received by the editor March 21, 2003 and, in revised form, March 27, 2004.
2000 *Mathematics Subject Classification.* Primary 11R29, 11R33, 11Y40.
Key words and phrases. Class groups, Galois modules, Cohen-Lenstra heuristics, numerical verifications.

degree p with exactly t ramified primes is proportional to $|\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M_0)|^{-1}|M_0|^{-1}$. Using genus theory we are able to prove part of this conjecture. In addition, we will relate our conjecture to a conjecture of Gerth, and we will present results of numerical verifications that are in good accordance with the predictions. We remark that the above results and the conjecture carry over to the case of cyclic extensions K/F of degree p of a fixed imaginary quadratic base field F whose class number is coprime to p and such that F does not contain the pth roots of unity.

In addition to the notation introduced so far, we always let $q = p^{-1}$, and $(q)_m = \prod_{i=1}^{m}(1-q^i)$ for $m \in \mathbb{N}\cup\{\infty\}$ (note that the product converges for $m = \infty$ because of $0 < q < 1$).

This paper grew out of my doctoral thesis, and I am grateful to my advisor Prof. C. Greither for various hints and fruitful discussions.

2. Cohen-Lenstra sums

In this section we will compute some infinite sums, similar to those occurring in Cohen-Lenstra heuristics. We fix a discrete valuation ring S. Let J be its maximal ideal, and suppose that the residue class field of S is $\mathbb{F}_p$. In what follows we will investigate sums of the form

$$\sum_{\substack{M \\ |M/JM|=p^h}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u},$$

where $h, u \in \mathbb{N}$ and M runs through all finite S-modules, of course up to isomorphism. Furthermore, we will also deal with refinements of these sums (i.e., with additional restrictions imposed on the modules M).

We start with a lemma (for a proof see [3, Prop. 3.1]). By $s_n^S(M)$ we denote the number of surjective S-homomorphisms $S^n \to M$. Recall that $q = p^{-1}$.

Lemma 2.1. *Let M be a finite S-module. Then*

$$|\{U \subseteq S^n \mid U \text{ submodule with } S^n/U \cong M\}| = s_n^S(M)|\mathrm{Aut}_S(M)|^{-1}$$

and

$$s_n^S(M) = |M|^n \frac{(q)_n}{(q)_{n-\nu}},$$

where $\nu = \dim_{\mathbb{F}_p}(M/JM)$ is the minimal number of generators of M.

Theorem 2.2. *Let $h, u \in \mathbb{N}$. Then*

$$\sum_{\substack{M \\ |M/JM|=p^h}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u} = \frac{q^{h(h+u)}(q)_u}{(q)_h(q)_{h+u}}.$$

Proof. This follows from [3, Th. 6.1(ii)]. □

Theorem 2.3. *Let M_0 be a finite S-module, and let $h_0 \in \mathbb{N}$ with $|M_0/JM_0| = p^{h_0}$. Let $h, u \in \mathbb{N}$ with $h \geq h_0$. Then*

$$\sum_{\substack{M \\ |M/JM|=p^h \\ JM\cong M_0}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u} = \frac{q^{h(h+u)}}{(q)_{h-h_0}}|\mathrm{Aut}_S(M_0)|^{-1}|M_0|^{-u}.$$

Proof. If M is a finite S-module, then $|M/JM| = p^h$ if and only if $M \cong S^h/U$ for a submodule $U \subseteq J^h$ of finite index. Therefore,

$$\sum_{\substack{M \\ |M/JM|=p^h \\ JM \cong M_0}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u} = \sum_{\substack{U \subseteq J^h \\ J^h/U \cong M_0}} \frac{|\mathrm{Aut}_S(S^h/U)|^{-1}|S^h/U|^{-u}}{|\{U' \subseteq J^h \mid S^h/U' \cong S^h/U\}|}$$

$$= \sum_{\substack{U \subseteq J^h \\ J^h/U \cong M_0}} \frac{[S^h : U]^{-u}}{s_h^S(S^h/U)}$$

by Lemma 2.1, and consequently,

$$\begin{aligned}
\sum_{\substack{M \\ |M/JM|=p^h \\ JM \cong M_0}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u} &= \frac{1}{(q)_h} \sum_{\substack{U \subseteq J^h \\ J^h/U \cong M_0}} [S^h : U]^{-(h+u)} \\
&= \frac{q^{h(h+u)}}{(q)_h}|M_0|^{-(h+u)}|\{U \subseteq J^h \mid J^h/U \cong M_0\}| \\
&= \frac{q^{h(h+u)}}{(q)_h}|M_0|^{-(h+u)}s_h^S(M_0)|\mathrm{Aut}_S(M_0)|^{-1} \\
&= \frac{q^{h(h+u)}}{(q)_{h-h_0}}|\mathrm{Aut}_S(M_0)|^{-1}|M_0|^{-u}.
\end{aligned}$$

□

Corollary 2.4. *Let $h, u, r \in \mathbb{N}$ with $r \leq h$. Then*

$$\sum_{\substack{M \\ |M/JM|=p^h \\ |JM/J^2M|=p^r}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u} = \frac{q^{h(h+u)}q^{r(r+u)}(q)_u}{(q)_{h-r}(q)_r(q)_{r+u}}.$$

Proof. This follows from the above theorems:

$$\begin{aligned}
\sum_{\substack{M \\ |M/JM|=p^h \\ |JM/J^2M|=p^r}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u} &= \sum_{\substack{M_0 \\ |M_0/JM_0|=p^r}} \sum_{\substack{M \\ |M/JM|=p^h \\ JM \cong M_0}} |\mathrm{Aut}_S(M)|^{-1}|M|^{-u} \\
&= \frac{q^{h(h+u)}}{(q)_{h-r}} \sum_{\substack{M_0 \\ |M_0/JM_0|=p^r}} |\mathrm{Aut}_S(M_0)|^{-1}|M_0|^{-u} \\
&= \frac{q^{h(h+u)}}{(q)_{h-r}} \frac{q^{r(r+u)}(q)_u}{(q)_r(q)_{r+u}}.
\end{aligned}$$

□

3. Galois module structure of p-class groups

Let $K/\mathbb{Q}$ be a cyclic number field of degree p, put $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ and let σ be a generator of Δ. We will present some results describing the structure of the p-part $\mathcal{C}\ell(K)_p$ of the class group as a Galois module over Δ, i.e., as a module over the discrete valuation ring $\mathbb{Z}_p[\omega]$. We note that we will always use the letter σ to denote the action of ω on $\mathcal{C}\ell(K)_p$ since σ corresponds to ω under the isomorphism $\mathbb{Z}[\Delta]/(\phi) \cong \mathbb{Z}[\omega]$.

The isomorphism type of $\mathcal{C}\ell(K)_p$ is determined by the cardinalities of the quotients

$$\mathcal{C}\ell(K)_p^{(\sigma-1)^{i-1}}/\mathcal{C}\ell(K)_p^{(\sigma-1)^i}$$

for $i \geq 1$. These quotients are $\mathbb{F}_p$-vector spaces, since $\mathbb{Z}_p[\omega]/(\omega-1) \cong \mathbb{F}_p$. By Chevalley's Theorem (cf. [10, Sec. 13, Lemma 4.1]) the cardinality of the first quotient is

$$|\mathcal{C}\ell(K)_p/\mathcal{C}\ell(K)_p^{\sigma-1}| = |\mathcal{C}\ell(K)_p^{\Delta}| = p^{t-1},$$

where $t \geq 1$ is the number of rational primes that ramify in K.

The cardinalities of $\mathcal{C}\ell(K)_p^{(\sigma-1)^{i-1}}/\mathcal{C}\ell(K)_p^{(\sigma-1)^i}$ for $i \geq 2$ are investigated in [6], although their calculation becomes rather complicated. We will only deal with the case $i = 2$ here; that is, we compute the $\mathbb{F}_p$-dimension of

$$\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2},$$

the so-called $(\sigma-1)^2$-rank of $\mathcal{C}\ell(K)_p$. The idea, which goes back to Rédei (cf. [12]) in a related situation, is to connect the above dimension to the rank of a certain matrix over $\mathbb{F}_p$. See also [7], [8].

From now on let $p_1, \ldots, p_t$ be the prime numbers that ramify in K, and suppose that $p \notin \{p_1, \ldots, p_t\}$ (in other words, $K/\mathbb{Q}$ is tamely ramified). This implies that $p_i \equiv 1 \bmod p$ for all $i = 1, \ldots, t$. The extension $K(\omega)/\mathbb{Q}(\omega)$ is a Kummer extension; hence there exists an element $\alpha \in \mathbb{Q}(\omega)$ such that

$$K(\omega) = \mathbb{Q}(\omega, \sqrt[p]{\alpha}).$$

Let $\mathfrak{p}_i$ be an arbitrary prime ideal $\subseteq \mathbb{Z}[\omega]$ over p_i (note that p_i splits completely in $\mathbb{Q}(\omega)$), and let $\nu_i := v_{\mathfrak{p}_i}(\alpha) \not\equiv 0 \bmod p$ for $i = 1, \ldots, t$. Since we can replace α by $\alpha^2, \alpha^3, \ldots, \alpha^{p-1}$ without changing our field, we will assume $\nu_1 = 1$.

We remark that there is a bijection between the cyclic number fields K of degree p such that $p_1, \ldots, p_t$ are the primes that ramify in K, and the $(t-1)$-tuples $(\nu_2, \ldots, \nu_t)$ of integers $1 \leq \nu_i \leq p-1$. This means that there are exactly $(p-1)^{t-1}$ cyclic number fields K of degree p with discriminant $\operatorname{disc}(K) = (p_1 \cdots p_t)^{p-1}$.

The following theorem states a formula for the $(\sigma-1)^2$-rank of $\mathcal{C}\ell(K)_p$. This requires some basic knowledge of Hilbert symbols, as in [11, Ch. V, §3].

Theorem 3.1. *Let K be as above, and define the matrix $A = (a_{ij}) \in \mathbb{F}_p^{t\times t}$ via the Hilbert symbols*

$$\left(\frac{p_j, \alpha}{\mathfrak{p}_i}\right) = \omega^{a_{ij}}.$$

Then the following formula holds:

$$\dim_{\mathbb{F}_p}(\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}) = t - 1 - \operatorname{rk}(A).$$

Note that the product formula for Hilbert symbols implies that the sum of the entries in each column is zero. Furthermore, there is an explicit formula for the Hilbert symbols (cf. [11, Ch. V, Prop. 3.4]) which reads

$$\left(\frac{p_j, \alpha}{\mathfrak{p}_i}\right) \equiv (p_j^{-v_{\mathfrak{p}_i}(\alpha)})^{(p_i-1)/p} \bmod p_i$$

if $i \neq j$.

Now fix $p_1, \ldots, p_t$ as above, and consider the following problem. As K varies over all $(p-1)^{t-1}$ cyclic number fields of degree p such that exactly $p_1, \ldots, p_t$ ramify

in K, which values do occur as $\dim(\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2})$? To this end we will construct a matrix $M = M_{\nu_2,\ldots,\nu_t} \in \mathbb{F}_p^{t\times t}$ such that with $(\nu_2,\ldots,\nu_t) \in \mathbb{F}_p^*\times\cdots\times\mathbb{F}_p^*$,

$$t - 1 - \mathrm{rk}(M_{\nu_2,\ldots,\nu_t})$$

runs through the values $\dim(\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2})$ for all fields K under consideration.

Fix $i \in \{1,\ldots,t\}$ for a moment, and let $\xi_i \not\equiv 1 \bmod p_i$ be a solution of the congruence

$$X^p \equiv 1 \bmod p_i. \tag{1}$$

Then $\{1,\xi_i,\ldots,\xi_i^{p-1}\}$ is the set of all solutions. Define $m'_{ij} \in \mathbb{F}_p$ for $j \neq i$ by

$$\xi_i^{m'_{ij}} \equiv p_j^{(p_i-1)/p} \bmod p_i.$$

Now we put

$$m_{ij} := \nu_i \cdot m'_{ij} \quad \text{if } j \neq i,$$

where we still set $\nu_1 = 1$. If we had chosen a different nontrivial solution η_i of the congruence (1), we would have $\eta_i = \xi_i^k$ for some $1 \leq k \leq p-1$. Therefore, the row vector $(m_{i1},\ldots,m_{i\,i-1},m_{i\,i+1},\ldots,m_{it})$ is uniquely determined up to multiplication by an element of $\mathbb{F}_p^*$. Finally, we define the diagonal entries of the matrix M by

$$m_{jj} := -\sum_{i\neq j} m_{ij}.$$

Thus we get a matrix $M = (m_{ij}) \in \mathrm{M}_t(\mathbb{F}_p)$ whose entries depend on $\nu_2,\ldots,\nu_t$, such that for each choice of $\nu_2,\ldots,\nu_t$, the rank of $M_{\nu_2,\ldots,\nu_t}$ corresponds to the $(\sigma-1)^2$-rank of the p-class group of a number field K as above, according to Theorem 3.1.

Corollary 3.2. *Let $p_1,\ldots,p_t$ be distinct prime numbers satisfying $p_i \equiv 1 \bmod p$. Let $\mathcal{K}$ be the set of all cyclic number fields of degree p such that exactly $p_1,\ldots,p_t$ ramify in K. Then there is a bijection between the set $\mathcal{K}$ and the set of $(t-1)$-tuples $(\nu_2,\ldots,\nu_t) \in \mathbb{F}_p^*\times\cdots\times\mathbb{F}_p^*$ such that if $K \in \mathcal{K}$ and $(\nu_2,\ldots,\nu_t)$ correspond to each other, the relation*

$$\dim_{\mathbb{F}_p}(\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}) = t - 1 - \mathrm{rk}(M_{\nu_2,\ldots,\nu_t})$$

holds.

4. Heuristic principle for p-class groups

In this section we will present our heuristic principle for the p-part of the class group, considered as a $\mathbb{Z}_p[\omega]$-module.

Let $t \geq 1$, and denote by $\mathfrak{K}_t$ the set of all cyclic number fields K of degree p (up to isomorphism), such that t rational primes ramify in K. Let Ω_t denote a set of representatives of the isomorphism classes of all finite $\mathbb{Z}_p[\omega]$-modules. If we set

$$C_t = \frac{q^{t(t-1)}(q)_1}{(q)_t(q)_{t-1}},$$

the map $M \mapsto |\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M)|^{-1}|M|^{-1}\,C_t^{-1}$ defines a probability measure on Ω_t, according to Theorem 2.2.

Conjecture 4.1. *Let $f : \Omega_t \to \mathbb{R}_+$ be an arbitrary function. Then the following formula holds:*

$$\lim_{x\to\infty} \frac{\sum_{K\in\mathfrak{K}_t,\ \mathrm{disc}(K)\le x} f(\mathcal{C}\ell(K)_p)}{|\{K\in\mathfrak{K}_t \mid \mathrm{disc}(K)\le x\}|} = \frac{\sum_{M\in\Omega_t} f(M)|\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M)|^{-1}|M|^{-1}}{C_t},$$

which means that the limit on the left-hand side exists if and only if the sum on the right-hand side converges, and in that case both values coincide. In particular, if f is the characteristic function of some element $M_0 \in \Omega_t$, we write $\mathrm{Prob}_t(\mathcal{C}\ell(K)_p \cong M_0)$ *for the limit on the left-hand side, and the formula reads*

$$\mathrm{Prob}_t(\mathcal{C}\ell(K)_p \cong M_0) = \frac{|\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M_0)|^{-1}|M_0|^{-1}}{C_t}. \tag{2}$$

In what follows we will support this conjecture. First we will prove a direct consequence concerning the $(\sigma-1)^2$-rank of the p-class group, using the results of section 3; cf. Theorem 4.3. In addition, we will relate our conjecture to results of Gerth that deal with the case $t\to\infty$, loosely speaking. Finally, we will also present some numerical evidence.

We remark that it suffices to consider a smaller family of number fields without affecting the statement of the conjecture. More precisely, we may suppose that the prime p is unramified in K, since it is clear that

$$|\{K\in\mathfrak{K}_t \mid \mathrm{disc}(K)\le x,\ p\,|\,\mathrm{disc}(K)\}| = o\left(|\{K\in\mathfrak{K}_t \mid \mathrm{disc}(K)\le x\}|\right)$$

as $x\to\infty$.

Now we will prove part of the conjecture. Let $0\le r\le t-1$ and put

$$\mathrm{Prob}_t\left(|\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}| = p^r\right) :=$$
$$\lim_{x\to\infty} \frac{|\{K\in\mathfrak{K}_t \mid \mathrm{disc}(K)\le x,\ |\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}| = p^r\}|}{|\{K\in\mathfrak{K}_t \mid \mathrm{disc}(K)\le x\}|}.$$

This is the ratio of fields $K\in\mathfrak{K}_t$ whose $(\sigma-1)^2$-rank equals r. Define

$$f:\Omega_t\to\mathbb{R}_+,\quad f(M) := \begin{cases} 1\,, & |(\omega-1)M/(\omega-1)^2M| = p^r,\\ 0\,, & \text{otherwise.}\end{cases}$$

Then it follows from Conjecture 4.1 and the sum formula in Corollary 2.4 that

$$\begin{aligned}\mathrm{Prob}_t&\left(|\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}| = p^r\right)\\ &= \sum_{\substack{M_0\in\Omega_t\\ |(\omega-1)M_0/(\omega-1)^2M_0| = p^r}} \mathrm{Prob}_t(\mathcal{C}\ell(K)_p\cong M_0)\\ &= \frac{q^{t(t-1)}q^{r(r+1)}(q)_1}{(q)_{t-1-r}(q)_r(q)_{r+1}}\cdot\frac{(q)_t(q)_{t-1}}{q^{t(t-1)}(q)_1}\\ &= \frac{q^{r(r+1)}(q)_t(q)_{t-1}}{(q)_r(q)_{t-1-r}(q)_{r+1}}.\end{aligned}$$

We will prove in the next theorem that this is indeed the case.

Lemma 4.2. *Let $k,m,n\in\mathbb{N}$ with $k\le\min\{m,n\}$. Then*

$$p^{(n+m-k)k}\frac{(q)_n(q)_m}{(q)_{n-k}(q)_{m-k}(q)_k}$$

equals the number of matrices in $\mathbb{F}_p^{m\times n}$ of rank k.

See [5, Th. 2] for a proof.

Theorem 4.3. *Let $0 \le r \le t-1$. Then we have*

$$\mathrm{Prob}_t\left(|\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}| = p^r\right) = \frac{q^{r(r+1)}(q)_t(q)_{t-1}}{(q)_r(q)_{t-1-r}(q)_{r+1}}.$$

Proof. We assume that $p \nmid \mathrm{disc}(K)$ for all fields K. By Theorem 3.1 those fields satisfy

$$|\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}| = p^{t-1-\mathrm{rk}(A)}$$

where $A = A(K) \in \mathbb{F}_p^{t\times t}$ is defined via Hilbert symbols. Furthermore, this matrix has the property that the entries in each column add up to zero. In [8] the following asymptotic formula as $x \to \infty$ is derived:

$$|\{K \in \mathfrak{K}_t \mid \mathrm{disc}(K) \le x \text{ and } A(K) = M\}| \sim \frac{1}{p^{t(t-1)}}|\{K \in \mathfrak{K}_t \mid \mathrm{disc}(K) \le x\}|,$$

using the fact that the Hilbert symbols are equidistributed (cf. [7]). Here $M \in \mathbb{F}_p^{t\times t}$ is any (fixed) matrix such that the sum of the entries in each column is zero. Thus we get

$$\begin{aligned}\mathrm{Prob}_t\left(|\mathcal{C}\ell(K)_p^{\sigma-1}/\mathcal{C}\ell(K)_p^{(\sigma-1)^2}| = p^r\right) &= \frac{|\{A \in \mathbb{F}_p^{(t-1)\times t} \mid \mathrm{rk}(A) = t-1-r\}|}{p^{t(t-1)}}\\ &= \frac{q^{r(r+1)}(q)_t(q)_{t-1}}{(q)_r(q)_{t-1-r}(q)_{r+1}},\end{aligned}$$

by Lemma 4.2, and the proof is complete. □

It is crucial to fix the number t of ramified primes in Conjecture 4.1, since by Chevalley's Theorem we have $|\mathcal{C}\ell(K)_p/\mathcal{C}\ell(K)_p^{\sigma-1}| = p^{t-1}$; thus the set of cyclic number fields of degree p, having a prescribed p-class group, has density zero among all cyclic number fields of degree p. However, using ideas of Gerth it is possible to formulate an analogous conjecture closer to the original Cohen-Lenstra heuristics. One has to study the distribution of the submodules $\mathcal{C}\ell(K)_p^{\sigma-1}$ instead of the full p-class group.

We put $\mathfrak{K} = \bigcup_{t\ge 1}\mathfrak{K}_t$. Let M_0 be a finite $\mathbb{Z}_p[\omega]$-module. We want to deduce the value of

$$\mathrm{Prob}(\mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0) := \lim_{x\to\infty}\frac{|\{K \in \mathfrak{K} \mid \mathrm{disc}(K) \le x,\ \mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0\}|}{|\{K \in \mathfrak{K} \mid \mathrm{disc}(K) \le x\}|}$$

from Conjecture 4.1, under an additional assumption (stated in the next lemma). We define $\mathrm{Prob}_t(\mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0)$ in the obvious way, by restricting ourselves to the fields in $\mathfrak{K}_t$.

Lemma 4.4. *Put*

$$r(x,t') := \frac{\sum_{t=1}^{t'}|\{K \in \mathfrak{K}_t \mid \mathrm{disc}(K) \le x,\ \mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0\}|}{\sum_{t=1}^{t'}|\{K \in \mathfrak{K}_t \mid \mathrm{disc}(K) \le x\}|},$$

and assume that the limits $\lim_{x\to\infty}\lim_{t'\to\infty} r(x,t')$ and $\lim_{t'\to\infty}\lim_{x\to\infty} r(x,t')$ exist and are equal. Then

$$\mathrm{Prob}(\mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0) = \lim_{t'\to\infty}\mathrm{Prob}_{t'}(\mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0).$$

Proof. The assertion follows easily from the fact that

$$|\{K \in \mathfrak{K}_t \mid \mathrm{disc}(K) \le x\}| = o\left(|\{K \in \mathfrak{K}_{t'} \mid \mathrm{disc}(K) \le x\}|\right) \quad (x \to \infty)$$

for all $t < t'$. □

Applying Conjecture 4.1 with

$$f : \Omega_t \to \mathbb{R}_+, \quad f(M) := \begin{cases} 1\,, & (\omega-1)M \cong M_0, \\ 0\,, & \text{otherwise} \end{cases}$$

yields:

$$\begin{aligned} \mathrm{Prob}_{t'}(\mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0) &= \sum_{\substack{|M/(\omega-1)M| = p^{t'} \\ (\omega-1)M \cong M_0}} \mathrm{Prob}_{t'}(\mathcal{C}\ell(K)_p \cong M) \\ &= \sum_{\substack{|M/(\omega-1)M| = p^{t'} \\ (\omega-1)M \cong M_0}} \frac{(q)_{t'}(q)_{t'-1}}{q^{t'(t'-1)}(q)_1} |\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M)|^{-1} |M|^{-1} \\ &\to \frac{(q)_\infty}{(q)_1} |\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M_0)|^{-1} |M_0|^{-1} \end{aligned}$$

as $t' \to \infty$, using Theorem 2.3. Now Conjecture 4.1, together with the assumption made in the preceding lemma, yields the following conjecture (independent of t) which is already in [8] (though between the lines).

Conjecture 4.5. *Let M_0 be a finite $\mathbb{Z}_p[\omega]$-module. Then*

$$\mathrm{Prob}(\mathcal{C}\ell(K)_p^{\sigma-1} \cong M_0) = \frac{|\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M_0)|^{-1} |M_0|^{-1}}{(q)_1 (q)_\infty^{-1}}.$$

Note that

$$\sum_{M_0} |\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M_0)|^{-1} |M_0|^{-1} = \frac{(q)_1}{(q)_\infty};$$

cf. [3, Sec. 6].

5. Numerical verifications

The goal of this section is to support Conjecture 4.1 by numerical results. To this end, we let $B > 0$ be a (sufficiently large) bound, and we generate the Galois module structure of the p-class group of all cyclic number fields K such that t prime numbers $p_1 < \cdots < p_t \le B$ satisfying $p_i \equiv 1 \bmod p$ ramify in K. This permits us to approximate the value $\mathrm{Prob}_t(\mathcal{C}\ell(K)_p \cong M_0)$ for a fixed module M_0, and to compare it with the predictions made by the conjecture. We will see that the agreement is rather satisfactory.

If $p_1 < \cdots < p_t$ are prime numbers as above, we have to find, first of all, defining polynomials for the set $\mathcal{K}$ of cyclic number fields of degree p, ramified exactly in $p_1, \ldots, p_t$. For $p \ge 5$ this can be done as in [2, Sec. 5.3] (by adjoining a primitive pth root of unity ω to the base field $\mathbb{Q}$ and using Kummer theory); see, in particular, Alg. 5.3.17. For $p = 3$ there is a well-known result yielding defining equations for the 2^{t-1} cyclic cubic fields in $\mathcal{K}$; see, for example, [1, Th. 4.6.4].

Now that one has defining equations for the fields $K \in \mathcal{K}$, one could of course compute all class groups $\mathcal{C}\ell(K)$ using [1, Alg. 6.5.9] and, in addition, derive the Galois module structure of their p-parts, i.e. $\mathcal{C}\ell(K)_p$ as $\mathbb{Z}_p[\omega]$-module, by investigating how σ acts on $\mathcal{C}\ell(K)_p$. However, there is a much more efficient way. The

crucial point is the following. By Corollary 3.2, it is easy to a priori calculate the number of fields in $\mathcal{K}$ with $(\sigma-1)^2$-rank equal to zero: we only have to construct the matrix $M = M_{\nu_2,\ldots,\nu_t}$, and we have to count the number of choices $(\nu_2,\ldots,\nu_t)$ such that this matrix has rank $t-1$. As soon as we have found all $K \in \mathcal{K}$ with nontrivial $(\sigma-1)^2$-rank, we know that

$$\mathcal{C}\ell(K)_p \cong (\mathbb{Z}_p[\omega]/(1-\omega))^{t-1}$$

for the remaining fields in $\mathcal{K}$. According to Theorem 4.3, the ratio of fields with trivial $(\sigma-1)^2$-rank among all cyclic number fields of degree p with t ramified primes equals

$$\frac{(q)_t}{(q)_1} > \frac{(q)_\infty}{(q)_1} \geq \prod_{i=2}^{\infty}(1-(\tfrac{1}{3})^i) \approx 0.84018912;$$

that is, "most" fields have trivial $(\sigma-1)^2$-rank.

The algorithm described above can be used to check how the p-class groups are distributed among the finite $\mathbb{Z}_p[\omega]$-modules M_0 with $|M_0/(1-\omega)M_0| = p^{t-1}$. These statistics can be compared with the ratios

$$\frac{(q)_{t-1}(q)_t}{q^{t(t-1)}(q)_1}\ |\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M_0)|^{-1}|M_0|^{-1}$$

predicted by Conjecture 4.1. For this purpose we need a formula for the number of $\mathbb{Z}_p[\omega]$-automorphisms of M_0. Write $M_0 \cong \bigoplus_{i=1}^{d}(\mathbb{Z}_p[\omega]/(1-\omega)^{u_i})^{k_i}$ with $d \in \mathbb{N}$, $1 \leq u_1 < \cdots < u_d$ and $k_1 + \cdots + k_d = t-1$. Then

$$|\mathrm{Aut}_{\mathbb{Z}_p[\omega]}(M_0)| = (q)_{k_1}\cdots(q)_{k_d}\cdot p^{(t-1)\sum_i k_i u_i - \sum_{i<j} k_i k_j (u_j-u_i)},$$

which can be seen from Lemma 2.1 together with [4, Th. 2.11].

We will now present some results of the numerical verifications in the cases $p=3$ and $t=2,3,4$. We have restricted ourselves to the case of cubic number fields, since many class groups have to be computed in order to get significant amounts of data. These class group computations are very time-consuming, in particular, if the degree of the number field increases. For all computations the PARI/GP package[1] has been used.

Notations. We use the following abbreviations (here ω is a third root of unity):

$$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3[\omega]} = [a_1,\ldots,a_n] \quad :\Longleftrightarrow \quad \mathcal{C}\ell(K)_3 \ \cong_{\mathbb{Z}_3[\omega]}\ \bigoplus_{i=1}^{n}\mathbb{Z}_3[\omega]/(1-\omega)^{a_i},$$

and if we are interested in the group structure:

$$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3} = [b_1,\ldots,b_m] \quad :\Longleftrightarrow \quad \mathcal{C}\ell(K)_3 \ \cong_{\mathbb{Z}_3}\ \bigoplus_{i=1}^{m}\mathbb{Z}/3^{b_i}\mathbb{Z}.$$

In the following tables, the first column contains the distinct $\mathbb{Z}_3[\omega]$-structures of the 3-class groups that occurred, and the second column contains the corresponding group structures. The third column indicates the observed ratio, while the last column indicates the ratio predicted by Conjecture 4.1. The entries in columns 3 and 4 are rounded to 8 decimals. Note that in each of the following tables, the ratio of number fields in the first row *must* (according to Theorem 4.3) converge to the predicted value, as the number of fields considered is increased. For

[1] `http://pari.math.u-bordeaux.fr`

all the relevant data concerning the number fields and the class groups used, see `http://www1.informatik.unibw-muenchen.de./Wittmann/tables.html` .

Case $p = 3$, $t = 2$.
Number of fields considered: 2510640.
Discriminant $(p_1p_2)^2$ with prime numbers $7 \le p_1 < p_2 \le 29389$.

$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3[\omega]}$	$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3}$	ratio	pred. ratio
[1]	[1]	0.88980101	0.88888889
[2]	[1, 1]	0.09746041	0.09876543
[3]	[2, 1]	0.01132221	0.01097394
[4]	[2, 2]	0.00124470	0.00121933
[5]	[3, 2]	0.00015255	0.00013548
[6]	[3, 3]	0.00001593	0.00001505
[7]	[4, 3]	0.00000279	0.00000167
[8]	[4, 4]	0.00000040	0.00000019

Case $p = 3$, $t = 3$.
Number of fields considered: 1013840.
Discriminant $(p_1p_2p_3)^2$ with prime numbers $7 \le p_1 < p_2 < p_3 \le 1531$.

$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3[\omega]}$	$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3}$	ratio	pred. ratio
[1, 1]	[1, 1]	0.85924998	0.85596708
[2, 1]	[1, 1, 1]	0.12351357	0.12680994
[3, 1]	[2, 1, 1]	0.01451314	0.01408999
[4, 1]	[2, 2, 1]	0.00162649	0.00156555
[2, 2]	[1, 1, 1, 1]	0.00071905	0.00117417
[5, 1]	[3, 2, 1]	0.00020220	0.00017395
[3, 2]	[2, 1, 1, 1]	0.00013118	0.00017395
[6, 1]	[3, 3, 1]	0.00002071	0.00001933
[4, 2]	[2, 2, 1, 1]	0.00001677	0.00001933
[5, 2]	[3, 2, 1, 1]	0.00000395	0.00000215
[7, 1]	[4, 3, 1]	0.00000197	0.00000215
[3, 3]	[2, 2, 1, 1]	0.00000099	0.00000161

Case $p = 3$, $t = 4$.
Number of fields considered: 163800.
Discriminant $(p_1p_2p_3p_4)^2$ with prime numbers $7 \le p_1 < p_2 < p_3 < p_4 \le 283$.

$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3[\omega]}$	$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3}$	ratio	pred. ratio
[1, 1, 1]	[1, 1, 1]	0.86090354	0.84539958
[2, 1, 1]	[1, 1, 1, 1]	0.12154457	0.13568141
[3, 1, 1]	[2, 1, 1, 1]	0.01440781	0.01507571
[4, 1, 1]	[2, 2, 1, 1]	0.00166667	0.00167508
[2, 2, 1]	[1, 1, 1, 1, 1]	0.00105617	0.00167508
[5, 1, 1]	[3, 2, 1, 1]	0.00017705	0.00018612
[3, 2, 1]	[2, 1, 1, 1, 1]	0.00015873	0.00024816
[6, 1, 1]	[3, 3, 1, 1]	0.00004884	0.00002068
[4, 2, 1]	[2, 2, 1, 1, 1]	0.00003053	0.00002757
[3, 3, 1]	[2, 2, 1, 1, 1]	0.00000611	0.00000230

6. Imaginary quadratic base fields

Let F be an imaginary quadratic number field such that $p \nmid h_F$, where h_F is the class number of F, and such that the pth roots of unity are not contained in F (in other words, $F \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$).

Now all the results of this paper remain valid if we consider cyclic extensions K/F of degree p (instead of cyclic number fields K of degree p), since again $\mathcal{C}\ell(K)_p$ is a $\mathbb{Z}_p[\omega]$-module. In this situation we fix the number of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ of F that ramify in K, and we assume that no $\mathfrak{p}_i$ divides p, which implies that $N(\mathfrak{p}_i) \equiv 1 \bmod p$. The obvious modifications of the results and the conjectures

in section 4 are left to the reader (compare with [9], and with [4] for the usual Cohen-Lenstra heuristics in this case).

We conclude with some numerical results for cyclic cubic extensions K of $F = \mathbb{Q}(i)$ such that two prime ideals of F ramify in K. Note that we can assume that the prime ideals of F that ramify in K have inertia degree 1 (the other extensions do not contribute to the limit of the conjecture).

Case $F = \mathbb{Q}(i)$ (base field), $p = 3$, $t = 2$.
Number of fields considered: 205656.
Relative discriminant of the extension fields $K/\mathbb{Q}(i)$:
$\mathfrak{d}_{K/\mathbb{Q}(i)} = (\mathfrak{p}_1\mathfrak{p}_2)^2$ with prime ideals $\mathfrak{p}_1 \neq \mathfrak{p}_2$ of F of degree 1 with
$13 \leq N(\mathfrak{p}_1) \leq N(\mathfrak{p}_2) \leq 7417$.

$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3[\omega]}$	$(\mathcal{C}\ell(K)_3)_{\mathbb{Z}_3}$	ratio	pred. ratio
[1]	[1]	0.89220835	0.88888889
[2]	[1, 1]	0.09194966	0.09876543
[3]	[2, 1]	0.01106216	0.01097394
[4]	[2, 2]	0.00120590	0.00121933
[5]	[3, 2]	0.00019450	0.00013548
[6]	[3, 3]	0.00000972	0.00001505
[?]	[?]	0.00336970	0.00000000

Note that here the fields K are of degree 6 over $\mathbb{Q}$. There were some fields (contained in the last row of the table) for which the computation of the 3-class number or of a relative defining equation failed. In these cases, the $(\sigma - 1)^2$-rank of the 3-class group must have been > 0.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1991. MR1228206 (94i:11105)

[2] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer, 2000. MR1728313 (2000k:11144)

[3] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, Number Theory Noordwijkerhout 1983, LNM **1068**, Springer, 1984. MR0756082 (85j:11144)

[4] H. Cohen and J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39–76. MR1037430 (91k:11097)

[5] S.D. Fisher and M.N. Alexander, *Matrices over a finite field*, Amer. Math. Monthly **73** (1966), 639–641.

[6] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l I, II*, Ann. Inst. Fourier **23**,3 (1973), 1–48, **23**,4 (1973), 45–64. MR0360519 (50:12967)

[7] F. Gerth III, *Counting certain number fields with prescribed l-class numbers*, J. Reine Angew. Math. **337** (1982), 195–207. MR0676052 (84c:12002)

[8] F. Gerth III, *Densities for ranks of certain parts of p-class groups*, Proc. Amer. Math. Soc. **99** (1987), 1–8. MR0866419 (88b:11067)

[9] F. Gerth III, *On p-class groups of cyclic extensions of prime degree p of quadratic fields*, Mathematika **36** (1989), 89–102. MR1014203 (90i:11126)

[10] S. Lang, *Cyclotomic Fields I and II*, Springer, 1990. MR1029028 (91c:11001)

[11] J. Neukirch, *Algebraic Number Theory*, Springer, 1999. MR1697859 (2000m:11104)

[12] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **171** (1935), 55–60.

Universität der Bundeswehr München, Fakultät für Informatik, Institut für Theoretische Informatik und Mathematik, 85577 Neubiberg, Germany

E-mail address: wittmann@informatik.unibw-muenchen.de