Tuomas Hakkarainen

On the Computation of the Class Numbers of Real Abelian Fields

Turku Centre *for* Computer Science

TUCS Dissertations

No 87, April 2007

On the Computation of the Class Numbers of Real Abelian Fields

by

Tuomas Hakkarainen

To be presented, with the permission of the Faculty of Mathematics and Natural Sciences of the University of Turku, for public criticism in Auditorium XXI of the University on May 18th, 2007, at 12 noon

University of Turku
Department of Mathematics
FI-20014 Turku, Finland

2007

Supervisor

Professor Tauno Metsänkylä
Department of Mathematics
University of Turku
FI-20014 Turku
Finland

Reviewers

Professor Radan Kučera
Institute of Mathematics
University of Brno
CZ-66295 Brno
Czech Republic

Professor Horst-Günter Zimmer
Fachrichtung Mathematik
Universität des Saarlandes
D-66041 Saarbrücken
Germany

Opponent

Professor Günter Lettl
Institut für Mathematik und Wissenschaftliches Rechnen
Karl-Franzens-Universität Graz
A-8010 Graz
Austria

ISBN 978-952-12-1881-1
ISSN 1239-1883
Painosalama Oy
Turku, Finland
2007

Acknowledgements

I wish to express my sincere gratitude to my supervisor, Professor Tauno Metsänkylä, for his continuous support during this work. Without his excellent guidance and broad knowledge, this thesis would not have been possible.

I am very grateful to Professors Radan Kučera and Horst-Günter Zimmer for reviewing the thesis manuscript and for their invaluable suggestions and remarks.

I thank the Department of Mathematics and Turku Centre of Computer Science TUCS for providing excellent working conditions, and all my friends and colleagues for creating a pleasant atmosphere and for the scientific as well as not-so-scientific discussions.

Finally, I would like to thank my family and all who have enriched my life during the studies and research.

Turku
April 2007 Tuomas Hakkarainen

Contents

Introduction **5**

1 Elementary notions **7**
1.1 The representations of an abelian group . . . 7
1.2 Dirichlet characters . . . 8
1.3 Abelian fields . . . 8
1.4 The group algebra $\mathbf{Q}[G]$ . . . 9

2 The unit group and the class number **13**
2.1 The decomposition of the unit group . . . 13
2.2 χ-units . . . 14
2.3 Complete submodules of units . . . 15
2.4 Regulators . . . 16
2.5 Cyclotomic χ-units . . . 18
2.6 Cyclotomic units of K . . . 19
2.7 χ-class numbers . . . 20

3 A condition for the class number divisibility **23**
3.1 Leopoldt's condition . . . 23
3.2 Divisibility of the p-adic regulator . . . 24
3.3 The method of Schwarz . . . 29
3.4 Examples . . . 31

4 Computation of the class number **35**
4.1 Outline of the algorithm . . . 35
4.2 Search for units of order p . . . 36
4.3 Verification of the p-divisibility . . . 38
4.4 Higher powers of p . . . 39
4.5 An example of the calculation . . . 42
4.6 Discriminant bounds . . . 44

5 Heuristics **47**
5.1 Heuristics for the class number 47
5.2 Heuristics for the p-adic regulator 50

6 Other methods **53**
6.1 A connection with Yoshino's method 53
6.2 p-Adic methods 56

7 Conclusion and open problems **59**

8 Tables **61**

Bibliography **81**

Introduction

The class number is a basic object in algebraic number theory, extensively studied since the 19th century. Yet, little is known of its values in general. In this thesis we study the computation of the class numbers of real abelian fields.

To define the class number h_F of an algebraic number field F, we first recall that the integral elements of F form a ring. The prime ideals of this ring generate a free abelian group. The index of the subgroup generated by the principal ideals is finite and it is called the class number. One may consider it to measure the failure of unique factorization in the ring of integers.

There does not exist a practical method to compute h_F in general, but an efficient algorithm exists, for instance, for quadratic fields and for some other fields of very small degree. However, such a method is not known even for the family of abelian fields, i.e., the Galois extensions of the rationals with abelian Galois group.

The class number of an abelian field K splits in the form $h_K = h_K^+ h_K^-$, where h_K^- is in theory easy to compute and h_K^+ is the class number of the maximal real subfield of K. The latter is difficult to compute or even estimate due to its close relation to the unit group of K. The known upper bounds are exponential in the degree of K.

In his recent work [32] concerning real abelian fields of prime power conductor, R. Schoof predicted, using a heuristic assumption, that the class numbers of such fields are most likely small, compared to the known upper bounds. Schoof also presented and applied an efficient procedure to compute class number divisors. There are also other methods to check whether a prime divides the class number. Indeed, this is in principle a feasible task, while the actual difficulty lies in finding a practical upper bound.

Our aim in the present work is to find methods which can be applied to fields of any conductor. This is not straightforward, mainly since the structure of the unit group may be quite complicated. The approach is to apply some results of Leopoldt [17] on the decomposition of the unit group and the class number in order to design criterions for the class number divisibility. We computed a table of odd primes $p < 10000$ dividing the class numbers of real abelian fields of conductor at most 2000. The prime

2 and the primes dividing the degree of the field are excluded since they would require different techniques. We also present heuristic assumptions similar to Schoof's and predict that there are no primes $p > 10000$ dividing the class numbers of these fields.

Another objective of this work is the computation of the p-adic regulator $R_p(K)$ of a real abelian field K for an odd prime p. A direct computation is difficult since the p-adic regulator contains information of the unit group. However, the p-adic class number formula gives an explicit expression for the product $h_K R_p(K)$, which allows a computation of the values of $R_p(K)$ without knowing the generators of the unit group explicitly. We present a table of values of p-adic regulators and compare them with probabilities given by heuristic assumptions.

In Chapter 1 we give some background on representation theory. We also fix the notation for later use. In Chapter 2 we discuss the group theoretic decomposition of the class number, mostly following Leopoldt [17]. These chapters provide the foundation for the rest of the thesis.

In another work by Leopoldt [18], Kummer's classical results on the divisibility of the class numbers are generalized to all real abelian fields. The main result is that if an odd prime p divides the class number, then a certain rational product is divisible by p. Chapter 3 arises from the results of W. Schwarz [34], who applied the p-adic class number formula and found a simple computational criterion for the class number divisibility, which is equivalent to Leopoldt's criterion. First we present this computational criterion in a more general setting and discuss the computation of the p-adic regulator in this connection. We also show how the results of Leopoldt, described in Chapter 2, clarify Schwarz's criterion in the case of a composite conductor; from this we obtain the first part of our algorithm to compute the class number divisors.

Chapter 4 contains the most essential results of the work. We complete the algorithm for verifying the divisibility of the class number by a prime p. We also show how to determine whether some higher power of p divides h_K.

Chapter 5 is comprised of a heuristic study of both the class number and the p-adic regulator. The numerical results, obtained by using the method of the preceding chapters, are compared with the probabilities given by the heuristics.

In Chapter 6 we show that there exists a close connection between our method and a recent method of Yoshino [39]. Moreover, we give a short overview of recent p-adic methods. Chapter 7 is devoted to some open problems and Chapter 8 contains the computed tables and their explanations.

The article [13], which has been submitted for publication, partly contains the results of this thesis.

Chapter 1

Elementary notions

We begin by recalling some basics on abelian fields and rational group algebras. The reader should consult an algebra textbook for the most elementary definitions that will be left out.

1.1 The representations of an abelian group

We review some elementary facts and definitions from representation theory. Assume that L is a field of characteristic 0 and that G is a finite abelian group of order g. Recall that a representation of G is a homomorphism $\rho : G \to GL(V)$, where V is an L-vector space of finite dimension and $GL(V)$ is the general linear group on V. The dimension of V is called the *degree* of the representation ρ. We use the notation $\rho(s) = \rho_s$ for simplicity. To give a representation of G on V is the same as to give an $L[G]$-module V; the correspondence is provided by the formula $\rho_s(x) = x^s$ $(s \in G, x \in V)$ with $\rho : s \mapsto \rho_s$ a representation on V. We will here and hereafter use the exponent notation for the module operation. Two representations are called *isomorphic* if the corresponding $L[G]$-modules are isomorphic.

If V has nontrivial $L[G]$-submodules V_1, V_2 such that $V = V_1 \oplus V_2$, one calls V *reducible*. Otherwise, V is called *irreducible* or *simple*. Every $L[G]$-module has (up to isomorphism) a unique decomposition into simple $L[G]$-modules. Similarly a representation breaks up uniquely into irreducible representations.

For any representation ρ, the map $\chi_\rho : G \to L$, $\chi_\rho(s) = \mathrm{Tr}(\rho_s) = \mathrm{Tr}(A)$, where A is a matrix representing ρ_s, is called the *character* of ρ. We define the *degree* of χ_ρ to be equal to the degree of ρ. We may shortly call χ_ρ a character of G. Two representations are isomorphic if and only if their characters coincide.

For clarity, when the field L varies, we speak of L-representations, L-irreducibility, etc.

If $L = \mathbf{C}$, the irreducible characters of G (i.e., the characters corresponding to the irreducible representations) are all of degree 1. They form an abelian group $\widehat{G}$ of all the homomorphisms $\chi : G \to \mathbf{C}^\times$. We have (non-canonically) $G \simeq \widehat{G}$.

1.2 Dirichlet characters

We recall here some character theory shortly in order to specify the notation used.

When $G = (\mathbf{Z}/n\mathbf{Z})^\times$, the characters in $\widehat{G}$ have a simple description. Let $\chi \in \widehat{G}$. If $n \mid m$, then χ induces a character of $(\mathbf{Z}/m\mathbf{Z})^\times$ by composition with the projection $(\mathbf{Z}/m\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times$. In the same manner, χ may be induced from a character of $(\mathbf{Z}/n_1\mathbf{Z})^\times$ with $n_1 \mid n$. Since the maps are essentially the same, we choose n minimal in this sense; it is called the *conductor* of χ and denoted f_χ. For $\nu \in \mathbf{N}$, let $\zeta_\nu = e^{2\pi i/\nu}$ be a primitive νth root of unity. The values of χ are $\varphi(f_\chi)$th roots of unity, $\zeta^k_{\varphi(f_\chi)}$, where φ is Euler's phi function.

By defining $\chi(a) = \chi(\bar{a})$ for $\bar{a} = a + n\mathbf{Z} \in (\mathbf{Z}/n\mathbf{Z})^\times$ and $\chi(a) = 0$ for $(a, n) > 1$, we may consider characters of $(\mathbf{Z}/n\mathbf{Z})^\times$ as Dirichlet characters modulo n. We first recall the Dirichlet characters modulo an odd prime power p^s. Choose a primitive root r modulo p^2. This is a primitive root modulo p^s for any $s \in \mathbf{N}$. Define a homomorphism $(\mathbf{Z}/p^s\mathbf{Z})^\times \to \mathbf{C}^\times$ by $\chi_{p^s}(r) = \zeta_{\varphi(p^s)}$. All the Dirichlet characters modulo p^s are of the form $\chi^c_{p^s}$ with $0 \le c \le \varphi(p^s) - 1$. Those with $(c, p) = 1$ are of conductor p^s.

Denote by $\langle\alpha\rangle$ the cyclic group generated by α. For $p = 2$, we have $(\mathbf{Z}/2^s\mathbf{Z})^\times = \langle\overline{-1}\rangle \times \langle\bar{5}\rangle$. Let ω_4 modulo 4 be defined by $\omega_4(-1) = -1$. For $s \ge 3$, define χ_{2^s} modulo 2^s by $\chi_{2^s}(5) = \zeta_{2^{s-2}}$ and $\chi_{2^s}(-1) = 1$.

Let $n \in \mathbf{N}$. Since $(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/\frac{n}{2}\mathbf{Z})^\times$ for $n \equiv 2 \pmod 4$, we may assume $n \not\equiv 2 \pmod 4$. Let $n = p_1^{s_1} \cdots p_t^{s_t}$ be the prime decomposition of n. All the Dirichlet characters modulo n are of the form $\omega_4^{c_0}\chi^{c_1}_{p_1^{s_1}} \cdots \chi^{c_t}_{p_t^{s_t}}$ with $0 \le c_i \le d_i - 1$, where d_i is the order of the corresponding character, i.e., $d_i = \varphi(p_i^{s_i})$ for odd p_i and $d_i = 2^{s_i-2}$ for $p_i = 2, s_i \ge 3$. We have $d_0 = 2$ and, for odd n, $c_0 = 0$. The characters of conductor n are those satisfying for $i = 1, \ldots, t$ the condition $p_i \nmid c_i$ in the cases $s_i \ge 2$, $p_i \ne 2$ and $s_i \ge 3$, $p_i = 2$, and the condition $(p_i - 1) \nmid c_i$ in the case $s_i = 1$; for $4 \mid n, 8 \nmid n$, we must also have $c_0 = 1$.

1.3 Abelian fields

Let m be a natural number. The field $\mathbf{Q}(\zeta_m)$ is called the mth *cyclotomic* field. Its Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) = G_m \simeq (\mathbf{Z}/m\mathbf{Z})^\times$ consists of the automorphisms $\sigma_k : \zeta_m \mapsto \zeta_m^k$ with $k \in \mathbf{Z}, (k, m) = 1$.

Suppose that K is an abelian field, i.e., a finite extension of $\mathbf{Q}$ with abelian Galois group. By the Kronecker–Weber theorem [36], $K \subseteq \mathbf{Q}(\zeta_m)$ for some $m \in \mathbf{N}$. The smallest number f such that $K \subseteq \mathbf{Q}(\zeta_f)$ is called the *conductor* of K. The Galois group $\mathrm{Gal}(K/\mathbf{Q}) = G$ of K is isomorphic to the factor group G_f/H, where $H = \mathrm{Gal}(\mathbf{Q}(\zeta_f)/K)$. Thus an automorphism of K may be viewed as a restriction to K of an automorphism of G_f.

The character group $\widehat{G}$ of G is called the *character group* of K. There is an inclusion preserving bijection between the subgroups of $\widehat{G}$ and the subfields of K. A character of K may be regarded as a Dirichlet character modulo f since $\widehat{G_f/H} \simeq \{\chi \in \widehat{G}_f \mid \chi(h) = 1 \,\forall\, h \in H\}$.

Denote by g_χ the order of $\chi \in \widehat{G}$. We say that $\psi \in \widehat{G}$ is $\mathbf{Q}$-*conjugate* to χ if $\psi = \chi^k$ with $(k, g_\chi) = 1$, i.e., $\langle\psi\rangle = \langle\chi\rangle$. This is an equivalence relation; denote by $\widetilde{\chi}$ the $\mathbf{Q}$-conjugacy class of the character χ and by $\widetilde{G}$ the set of all $\mathbf{Q}$-conjugacy classes of $\widehat{G}$. We have $\widetilde{\chi} = \{\chi^k \mid (k, g_\chi) = 1\}$. The sums $\sum_{\psi\in\widetilde{\chi}} \psi$ are characters with values in $\mathbf{Q}$; in fact, we will see that they are exactly the $\mathbf{Q}$-irreducible characters of G.

Let f_χ, g_χ and $\mathrm{Ker}(\chi)$ be respectively the common conductor, order and kernel of the $\mathbf{Q}$-conjugates of χ. Denote by K_χ the subfield of K with character group $\langle\chi\rangle$. There is a one-to-one correspondence between the $\mathbf{Q}$-conjugacy classes of $\widehat{G}$ and the cyclic subfields of K, given by $\widetilde{\chi} \longleftrightarrow \langle\chi\rangle$; the cyclic field corresponding to $\widetilde{\chi}$ is K_χ. Its degree is g_χ, its conductor f_χ, and since $\mathrm{Ker}(\chi) = \mathrm{Gal}(K/K_\chi)$, we have $G/\mathrm{Ker}(\chi) \simeq \mathrm{Gal}(K_\chi/\mathbf{Q}) \simeq \langle\chi\rangle$. From this it also follows that if $\mathrm{Ker}(\psi) = \mathrm{Ker}(\chi)$, then ψ and χ are $\mathbf{Q}$-conjugate. We will write $G_\chi = \mathrm{Gal}(K_\chi/\mathbf{Q})$.

1.4 The group algebra $\mathbf{Q}[G]$

Let G be a finite abelian group. Here and hereafter we denote by g the order of G. Consider the group algebra $\mathbf{C}[G]$. For $\chi \in \widehat{G}$, an *orthogonal idempotent* of $\mathbf{C}[G]$ corresponding to χ is given by $e_\chi = \frac{1}{g}\sum_{\sigma\in G} \chi(\sigma^{-1})\sigma$. Thus the elements e_χ are characterized by the following two relations:

$$e_\chi^2 = e_\chi, \qquad e_\chi e_\psi = 0 \quad \text{if} \quad \chi \neq \psi.$$

It is easy to verify that $e_\chi\sigma = \chi(\sigma)e_\chi$ for any $\sigma \in G$. The set $\{e_\chi \mid \chi \in \widehat{G}\}$ is *full*, i.e., it satisfies $\sum_{\chi\in\widehat{G}} e_\chi = 1$.

Now we turn to the group algebra $\mathbf{Q}[G]$. The following proposition describes its structure; we follow [17, p. 9].

Proposition 1.1. *Let $e_{\widetilde{\chi}} = \sum_{\psi\in\widetilde{\chi}} e_\psi$. The set of $e_{\widetilde{\chi}}$ with $\widetilde{\chi}$ running through $\widetilde{G}$ is a full set of orthogonal idempotents of the algebra $\mathbf{Q}[G]$. There is a* *decomposition*

$$\mathbf{Q}[G] = \bigoplus_{\widetilde{\chi} \in \widetilde{G}} \mathbf{Q}[G] e_{\widetilde{\chi}} \tag{1.1}$$

into a direct sum of minimal ideals $\mathbf{Q}[G]e_{\widetilde{\chi}}$, *where* $\mathbf{Q}[G]e_{\widetilde{\chi}}$ *is a ring with unity element* $e_{\widetilde{\chi}}$ *and* $\mathbf{Q}[G]e_{\widetilde{\chi}} \simeq \mathbf{Q}(\zeta_{g_\chi})$.

Proof. For any $\sigma \in G$ and $\chi \in \widehat{G}$, $\sum_{\psi \in \widetilde{\chi}} \psi(\sigma) = \mathrm{Tr}_{\mathbf{Q}(\zeta_{g_\chi})/\mathbf{Q}}(\chi(\sigma)) \in \mathbf{Q}$. The elements $e_{\widetilde{\chi}} \in \mathbf{Q}[G]$ obviously form a full set of orthogonal idempotents. The algebra $\mathbf{Q}[G]$ thus admits the decomposition (1.1) into a direct sum of ideals generated by $e_{\widetilde{\chi}}$.

Extend χ by $\mathbf{Q}$-linearity to a ring homomorphism

$$\chi : \mathbf{Q}[G] \to \mathbf{Q}(\zeta_{g_\chi}), \quad \chi(\sum_{\sigma \in G} a_\sigma \sigma) = \sum_{\sigma \in G} a_\sigma \chi(\sigma).$$

This is surjective since there exists $\sigma \in G$ with $\chi(\sigma) = \zeta_{g_\chi}$.

Let $\sigma_0 \operatorname{Ker}(\chi)$ be a generator of the cyclic group $G/\operatorname{Ker}(\chi)$. We have

$$\chi(e_{\widetilde{\chi}}) = \frac{1}{g} \sum_{\sigma \in G} \sum_{(k, g_\chi)=1} \chi^k(\sigma^{-1})\chi(\sigma) = \frac{\#\operatorname{Ker}(\chi)}{g} \sum_{u=1}^{g_\chi} \sum_{(k, g_\chi)=1} \chi^k(\sigma_0^{-u})\chi(\sigma_0^u).$$

Changing the order of summation yields the inner sum $\sum_{u=1}^{g_\chi} \chi(\sigma_0)^{u(1-k)}$ which is equal to g_χ if $k = 1$ and 0 otherwise. It follows that $\chi(e_{\widetilde{\chi}}) = 1$, and hence that the restriction of χ to the ideal $\mathbf{Q}[G]e_{\widetilde{\chi}}$ is still surjective.

Since the $\mathbf{Q}$-conjugacy classes form a partition of $\widehat{G}$, we have

$$\dim_{\mathbf{Q}} \bigoplus_{\widetilde{\chi} \in \widetilde{G}} \mathbf{Q}(\zeta_{g_\chi}) = \sum_{\widetilde{\chi} \in \widetilde{G}} \varphi(g_\chi) = g = \dim_{\mathbf{Q}} \mathbf{Q}[G].$$

It follows that $\dim_{\mathbf{Q}} \mathbf{Q}[G]e_{\widetilde{\chi}} = \varphi(g_\chi)$ and that the restriction of χ is an isomorphism

$$\mathbf{Q}[G]e_{\widetilde{\chi}} \simeq \mathbf{Q}(\zeta_{g_\chi}).$$

In particular, the ideals $\mathbf{Q}[G]e_{\widetilde{\chi}}$ are fields, which proves their minimality. □

By the proposition, $\mathbf{Q}[G]e_{\widetilde{\chi}}$ is a simple $\mathbf{Q}[G]$-module. Its character is $\sum_{\psi \in \widetilde{\chi}} \psi = \mathrm{Tr}_{\mathbf{Q}(\zeta_{g_\chi})/\mathbf{Q}}(\chi)$.

In the following we briefly state some results of *orders*. See [17, p. 11]. Recall that an order in $\mathbf{Q}[G]$ is a subring R that is finitely generated over $\mathbf{Z}$ and satisfies $\mathbf{Q} \otimes_{\mathbf{Z}} R = \mathbf{Q}[G]$. It follows from the proposition above that the maximal order of $\mathbf{Q}[G]$ is $\mathcal{O}_G = \oplus_{\widetilde{\chi} \in \widetilde{G}} \mathbf{Z}[G]e_{\widetilde{\chi}}$. Indeed, we have $\mathbf{Z}[G]e_{\widetilde{\chi}} \simeq \mathbf{Z}[\zeta_{g_\chi}]$. Their isomorphism is described as follows (recall that $e_\chi \sigma = \chi(\sigma)e_\chi$): If σ is a generator of G_χ and $\tau \in G$, we may uniquely write $\tau = \sigma^k \tau'$ for some $0 \leq k < g_\chi$ and $\tau' \in \operatorname{Ker}(\chi)$. Associate τ with $\zeta_{g_\chi}^k$.

Another important order of $\mathbf{Q}[G]$ is the ring $\mathbf{Z}[G]$ whose index (as an additive subgroup) in $\mathcal{O}_G$ is given by $g^g = [\mathcal{O}_G : \mathbf{Z}[G]]^2 d(\mathcal{O}_G)$, where $d(\mathcal{O}_G) = \prod_{\widetilde{\chi}\in\widetilde{G}} d_{\widetilde{\chi}}$ and $d_{\widetilde{\chi}}$ is the absolute value of the discriminant of $\mathbf{Q}(\zeta_{g_\chi})$. An order whose index we will later need is $\mathcal{L} = \mathbf{Z}[G] + e_{\widetilde{1}}\mathbf{Z}[G]$, where $e_{\widetilde{1}} = \frac{1}{g}\sum_{\sigma\in G}\sigma$. We have

$$Q_G = [\mathcal{O}_G : \mathcal{L}] = [\mathcal{O}_G : \mathbf{Z}[G]]/g = \sqrt{\frac{g^{g-2}}{d(\mathcal{O}_G)}}. \tag{1.2}$$

Chapter 2

The unit group and the class number

In this chapter we split the unit group and the regulator of a real abelian field in terms of the rational idempotents and show how these decompositions allow to split the class number. This chapter contains a large part of the results of Leopoldt's thesis [17]. The reader may also find its French exposition [29] useful.

2.1 The decomposition of the unit group

From now on we assume K real; then $K \subseteq \mathbf{Q}(\zeta_f + \zeta_f^{-1})$ for some f. Let $G = \mathrm{Gal}(K/\mathbf{Q})$. Denote by E_K the unit group of K and let W be the torsion group of E_K. Since W consists of the roots of unity in K, we have $W = \{\pm 1\}$. Denote the class $\{\alpha, -\alpha\}$ by $\pm\alpha$. For $M \subset \mathbf{R}$ a $\mathbf{Z}[G]$-module containing -1, let us define a G-operation on $|M| = M/\{\pm 1\}$ by $(\pm\alpha)^\sigma = \pm\alpha^\sigma$. Then $|E_K|$ is a $\mathbf{Z}[G]$-module and (as an abelian group) of type $\mathbf{Z}^{g-1}$ by Dirichlet's Unit Theorem. On extension by $\mathbf{Q}$ we obtain a $\mathbf{Q}[G]$-module $|E_K|^{\mathbf{Q}} = \mathbf{Q} \otimes_{\mathbf{Z}} |E_K|$. The following proposition describes its structure. The proof follows that of Oriat [28]. For brevity, we will here and hereafter denote by $\sum'_{\widetilde{\chi}\in\widetilde{G}}$ a sum over $\widetilde{\chi} \in \widetilde{G}, \widetilde{\chi} \neq 1$. We also adopt the same notation for other similar operators.

Proposition 2.1. *There is a* $\mathbf{Q}[G]$*-module isomorphism*

$$|E_K|^{\mathbf{Q}} \simeq {\bigoplus_{\widetilde{\chi}\in\widetilde{G}}}' \mathbf{Q}[G] e_{\widetilde{\chi}}. \tag{2.1}$$

Proof. We will show that the characters of these $\mathbf{Q}[G]$-modules coincide. Let $\lambda : E_K \to \mathbf{R}^g$, $\lambda(\varepsilon) = (\ln |\varepsilon^\sigma|)_{\sigma\in G}$ be the logarithmic embedding of E_K. By Dirichlet's Unit Theorem, the kernel of λ is W and its image is a discrete subgroup of $\mathbf{R}^g$ of rank $g-1$ consisting of the elements $(x_\sigma)_{\sigma\in G}$ that satisfy $\sum_{\sigma\in G} x_\sigma = 0$.

Let U be the subgroup of $\mathbf{R}^g$ consisting of the elements $(a, a, \ldots, a)$, $a \in \mathbf{Z}$. The group $\mathrm{Im}(\lambda) \oplus U$ is a discrete subgroup of $\mathbf{R}^g$ of rank g. By defining a $\mathbf{Z}[G]$-module structure for $\mathbf{R}^g$ by $\tau(x_\sigma)_{\sigma\in G} = (x_{\tau\sigma})_{\sigma\in G}$, λ becomes a $\mathbf{Z}[G]$-homomorphism and U a trivial $\mathbf{Z}[G]$-submodule of $\mathbf{R}^g$. Let $\{e_1, e_2, \ldots, e_g\}$ be a $\mathbf{Z}$-basis of $\mathrm{Im}(\lambda) \oplus U$.

For $\sigma \in G$, let A_σ be the matrix defined by the action of σ on $\mathrm{Im}(\lambda) \oplus U$, $(e_1^\sigma, \ldots, e_g^\sigma) = (e_1, \ldots, e_g)A_\sigma$. We may as well consider this σ-action in $\mathbf{R}^g$ since $\{e_1, e_2, \ldots, e_g\}$ is also a basis of $\mathbf{R}^g$. The trace of A_σ is independent of the choice of the basis of $\mathbf{R}^g$. By choosing the canonical basis, we see that $\mathrm{Tr}(A_\sigma) = g$ if $\sigma = 1$ and 0 otherwise.

The map $\sigma \mapsto \mathrm{Tr}(A_\sigma)$ is the character of the $\mathbf{Q}[G]$-module

$$\mathbf{Q} \otimes_{\mathbf{Z}} (\mathrm{Im}(\lambda) \oplus U) = (\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{Im}(\lambda)) \oplus (\mathbf{Q} \otimes_{\mathbf{Z}} U).$$

Since the character of $\mathbf{Q} \otimes_{\mathbf{Z}} U$ is 1, we see that the character α of $\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{Im}(\lambda)$ is determined by

$$\alpha(\sigma) = g - 1 \quad \text{if} \quad \sigma = 1, \quad \alpha(\sigma) = -1 \quad \text{if} \quad \sigma \neq 1.$$

It follows, by known character relations, that $\alpha = \sum'_{\widetilde{\chi}\in\widetilde{G}} \widehat{\chi}$ with $\widehat{\chi} = \sum_{\psi\in\widetilde{\chi}} \psi$ is the character of $\mathbf{Q}[G]e_{\widetilde{\chi}}$. The claim follows. □

2.2 χ-units

We now construct simple submodules of units that correspond to the factorization (2.1). Denote by $N_{K/k}$ the norm map. We will call a $\mathbf{Z}[G]$-module M *simple* if $\mathbf{Q} \otimes_{\mathbf{Z}} M$ is simple. Recall that K_χ is the subfield of K whose character group is generated by $\chi \in \widehat{G}$.

Definition 2.1. Let ε be a real unit of $\mathbf{Q}(\zeta_{2f_\chi})$ satisfying $\varepsilon^2 \in K_\chi$. We call ε a *χ-unit* if $(\pm\varepsilon^2)^{e_{\widetilde{\chi}}} = \pm\varepsilon^2$.

In fact, we could replace $\mathbf{Q}(\zeta_{2f_\chi})$ in the above definition by any abelian field containing ε and having χ as a character. Indeed, if L_1 is an abelian field containing $K_\chi(\varepsilon)$ and G_1 and G denote their Galois groups, respectively, then the restriction homomorphism $\phi : \mathbf{Q}[G_1] \to \mathbf{Q}[G]$ gives $\phi(e^1_{\widetilde{\chi}}) = e_{\widetilde{\chi}}$ for $e^1_{\widetilde{\chi}}$ the idempotent of $\mathbf{Q}[G_1]$ corresponding to $\widetilde{\chi}$. Hence $(\pm\varepsilon^2)^{e_{\widetilde{\chi}}} = (\pm\varepsilon^2)^{e^1_{\widetilde{\chi}}}$.

There exists another characterization of χ-units given in the next proposition. The proof can be found in [17, p. 21]; it is based on a manipulation of the formulas of the idempotents $e_{\widetilde{\chi}}$.

Proposition 2.2. *A real unit ε is a χ-unit if and only if $\varepsilon^2 \in K_\chi$ and $N_{K_\chi/L}(\varepsilon^2) = 1$ for all proper subfields L of K_χ.*

A χ-unit is called *proper* if it belongs to K_χ. Denote respectively by E^0_χ and E_χ the groups of χ-units and proper χ-units (the notation differs from that used by Leopoldt). Both groups only depend on $\widetilde{\chi}$. Leopoldt [17, p. 29] shows that $[E^0_\chi : E_\chi]$ equals 1 or 2 and that $|E^0_\chi|$ and $|E_\chi|$ are isomorphic as $\mathbf{Z}[G_\chi]$-modules.

Let $|E_\chi|^{\mathbf{Q}} = \mathbf{Q} \otimes_{\mathbf{Z}} |E_\chi|$. Applying Proposition 2.1 with G_χ in place of G, we conclude (by the orthogonality) that $|E_\chi|^{\mathbf{Q}} \simeq \mathbf{Q}[G_\chi]e_{\widetilde{\chi}}$. It follows that $|E_\chi|$ is a simple $\mathbf{Z}[\zeta_{g_\chi}]$-module of $\mathbf{Z}$-rank $\varphi(g_\chi)$. Since $\mathbf{Z}[G]e_{\widetilde{\chi}} \simeq \mathbf{Z}[\zeta_{g_\chi}]$, $|E_\chi|$ may also be regarded as a $\mathbf{Z}[G]$-module.

2.3 Complete submodules of units

Recall that $\mathcal{O}_G = \oplus_{\widetilde{\chi} \in \widetilde{G}} \mathbf{Z}[G]e_{\widetilde{\chi}}$. We see that $\prod_{\widetilde{\chi} \in \widetilde{G}} |E_\chi|$ is an $\mathcal{O}_G$-module. But since $|E_K|$ is only a $\mathbf{Z}[G]$-module, its relationship to $\prod_{\widetilde{\chi}} |E_\chi|$ is not clear. This question will be answered in this section. We assume that M is a $\mathbf{Z}[G]$-module which as a group is free and finitely generated.

We begin with a definition. Let $\mathcal{O}_M = \{x \in \mathcal{O}_G \mid M^x \subseteq M\}$; this is an order of $\mathbf{Q}[G]$ that satisfies $\mathbf{Z}[G] \subseteq \mathcal{O}_M \subseteq \mathcal{O}_G$.

Definition 2.2. We call M *complete* if $\mathcal{O}_M = \mathcal{O}_G$.

Remark 2.1. We use here the notion of completeness following Oriat [28], while Leopoldt [17] defined completeness for lattices; the notions are essentially equal.

The following lemma describes some basic notions related to complete $\mathbf{Z}[G]$-modules.

Lemma 2.1. *The* $\mathbf{Z}[G]$*-module* $M^* = M^{\mathcal{O}_G}$ *is complete and contained in every complete* $\mathbf{Z}[G]$*-module containing* M*. There exists a complete submodule* M_* *of* M *that contains every complete submodule of* M*. The indices* $[M^* : M]$ *and* $[M : M_*]$ *are finite.*

Proof. The product of complete modules is still complete. Define M_* as the product of all complete submodules of M. The modules M^* and M_* obviously satisfy the inclusion conditions.

We have $(M^*)^g = M^{g\mathcal{O}_G} \subseteq M^{\mathbf{Z}[G]} \subseteq M$. This proves $[M^* : M]$ finite. Since $(M^*)^g$ is a complete submodule, $(M^*)^g \subseteq M_*$. Hence also $M^g \subseteq M_*$, thus $[M : M_*] < \infty$. □

Oriat calls M^* and M_* the *envelope* and the *kernel* of M, respectively.

We will shortly call a character of $\mathbf{Q} \otimes_{\mathbf{Z}} M$ a character of M. Let M be a simple $\mathbf{Z}[G]$-module with character $\sum_{\psi \in \widetilde{\chi}} \psi$; indeed, by Proposition 1.1, all $\mathbf{Q}$-irreducible characters of G are of this form. For any $\widetilde{\psi} \neq \widetilde{\chi}$, we have $M^{e_{\widetilde{\psi}}} = 1$ (since $(\mathbf{Q} \otimes M)^{e_{\widetilde{\psi}}} \simeq \mathbf{Q}[G]e_{\widetilde{\chi}}e_{\widetilde{\psi}} = 0$). It follows that $M = M^{e_{\widetilde{\chi}}}$, thus $M = M^*$. We have shown the following fact.

Lemma 2.2. *Every simple* $\mathbf{Z}[G]$*-module is complete.*

It would also be easy to prove that any complete $\mathbf{Z}[G]$-module is a direct sum of simple $\mathbf{Z}[G]$-modules (see [28]).

In the following we provide a complete submodule of units constructed from χ-units. This will clarify the relationship between E_χ and E_K.

Definition 2.3. Let $\widetilde{\chi} \in \widetilde{G}$. Define $E_\chi^K = E_K \cap E_\chi^0$ and $E^K = \prod'_{\widetilde{\chi}\in\widetilde{G}} E_\chi^K$. Let $Q_K = [E_K : E^K]$.

Proposition 2.3. *The product* $|E^K| = \prod'_{\widetilde{\chi}\in\widetilde{G}} |E_\chi^K|$ *is direct. The* $\mathbf{Z}[G]$*-module* $|E^K|$ *is the kernel of* $|E_K|$*. The index* Q_K *is finite and divides* g^{g-1}*.*

Proof. If $\varepsilon \in E_\chi^K$, then (by definition) we have $(\pm\varepsilon)^{e_{\widetilde{\chi}}} = \pm\varepsilon$ and $(\pm\varepsilon)^{e_{\widetilde{\psi}}} = 1$ for $\widetilde{\psi} \neq \widetilde{\chi}$. This proves the first claim.

Let H be a complete submodule of $|E_K|$. Define an $e_{\widetilde{\chi}}$-action on $\eta \in H$ by the action on the $\varepsilon \in E_K$ satisfying $\eta = \pm\varepsilon$. We have $H^{e_{\widetilde{\chi}}} \subseteq H \subseteq |E_K|$ and, by the definition of E_χ^0, $H^{e_{\widetilde{\chi}}} \subseteq |E_\chi^0|$. This shows that $H^{e_{\widetilde{\chi}}} \subseteq |E_\chi^K|$ for any $\widetilde{\chi}$, hence that $H \subseteq |E^K|$. By the proof of Lemma 2.1, we conclude that $|E_K|_* \subseteq |E^K|$. To show that $|E_K|_* = |E^K|$, we prove $|E^K|$ complete. Since $[E_\chi^0 : E_\chi] \leq 2$, $|E_\chi^K|$ is equal to $|E_\chi^0|$ or $|E_\chi|$. These are simple $\mathbf{Z}[G_\chi]$-modules, thus $|E_\chi^K|$ is a complete module; the same also holds when regarding $|E_\chi^K|$ as a $\mathbf{Z}[G]$-module. We conclude that $|E^K|$ is complete.

Since $|E_\chi^0|$ is of $\mathbf{Z}$-rank $\varphi(g_\chi)$, $|E^K|$ is of rank $g-1$. In the proof of Lemma 2.1 we showed $|E_K|^g \subseteq |E_K|_* = |E^K|$, thus $Q_K \mid g^{g-1}$. □

Remark 2.2. Leopoldt [17, p. 24] shows that Q_K divides the index Q_G defined in (1.2). In general, very little is known about the value of Q_K, but for instance for cyclic K of prime degree, $Q_K = Q_G = 1$.

Definition 2.4. Define $E_+^K = \prod'_{\widetilde{\chi}\in\widetilde{G}} E_\chi$ and $Q_K^+ = [E_K : E_+^K]$.

A similar argument as in Proposition 2.3 shows that $|E_+^K|$ is the direct product of the $|E_\chi|$ and that it is complete and contained in $|E^K|$. We have $Q_K^+ = 2^{q_K} Q_K$ with $q_K \in \mathbf{Z}_+$.

2.4 Regulators

As before, let K be a real abelian field. Recall the notion of *regulator* $R_K(H)$ of a subgroup $H \leq E_K/\{\pm 1\}$ of finite index; intuitively it is the volume of the body generated by a $\mathbf{Z}$-basis of H in the "logarithmic space". Let $\{\sigma_1, \sigma_2, \ldots, \sigma_g\}$ be the elements of G and let $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{g-1}\}$ be a set of generators of H. Then

$$R_K(H) = |\det(\ln|\varepsilon_i^{\sigma_j}|)|_{1\leq i,j\leq g-1}.$$

This is independent of the choice of the basis and the ordering of the σ_j. The regulator of $E_K/\{\pm 1\}$ is called the regulator of K and denoted R_K. We have (see [36, Lemma 4.15])

$$[|E_K| : H] = R_K(H)/R_K. \tag{2.2}$$

It is well known (cf. [36, Lemma 5.26]) that if $f : G \to \mathbf{R}$ is any function, we may write $\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G} = \prod_{\chi\in\widehat{G}}\sum_{\sigma\in G}\chi(\sigma)f(\sigma)$. This gives a clue on how to decompose the regulator through characters. We state the following definition.

Definition 2.5. Let $\alpha \in |E_K|^{\mathbf{Q}}$ and let χ be a nontrivial character of K. Define the *χ-regulator* of α in K as

$$R_\chi^K(\alpha) = \prod_{\psi\in\widetilde{\chi}}\sum_{\sigma\in G}\psi(\sigma^{-1})\ln|\alpha^\sigma|.$$

For $\varepsilon \in |E_\chi|^{\mathbf{Q}}$ and $u \in \mathbf{Z}[G_\chi]$, we see that

$$\sum_{\sigma\in G_\chi}\chi(\sigma^{-1})\ln|\varepsilon^{u\sigma}| = \chi(u)\sum_{\sigma\in G_\chi}\chi(\sigma^{-1})\ln|\varepsilon^\sigma|;$$

thus

$$R_\chi^{K_\chi}(\varepsilon^u) = N_{\mathbf{Q}(\zeta_{g_\chi})/\mathbf{Q}}(\chi(u))R_\chi^{K_\chi}(\varepsilon). \tag{2.3}$$

The notion of χ-regulator generalizes to any $\mathbf{Z}[G]$-module H that is finitely generated as a $\mathbf{Z}$-module and contained in $|E_K|^{\mathbf{Q}}$. If $H^{e_{\widetilde{\chi}}} = 1$, define $R_\chi^K(H) = 0$. Otherwise, let $\varepsilon \in H$ such that $\varepsilon^{e_{\widetilde{\chi}}} \neq 1$ and define an integral ideal $\mathfrak{h} \subseteq \mathbf{Q}[G]e_{\widetilde{\chi}}$ by its inverse $\mathfrak{h}^{-1} = \{u \in \mathbf{Q}[G]e_{\widetilde{\chi}} \mid \varepsilon^u \in H^{e_{\widetilde{\chi}}}\}$. Then the χ-regulator of H is defined as

$$R_\chi^K(H) = R_\chi^K(\varepsilon)/N_{\mathbf{Q}(\zeta_{g_\chi})/\mathbf{Q}}(\chi(\mathfrak{h})). \tag{2.4}$$

It is independent of the choice of ε (see [29, p. 19] for the proofs). If H is generated by the conjugates of ε, we see that $\mathfrak{h} = 1$, thus $R_\chi^K(H) = R_\chi^K(\varepsilon)$.

The above definitions allow to derive some properties of χ-regulators analogous to regulators. We state here only the results we need. They are proved in [17, pp. 31–35].

Proposition 2.4. *Let $H \subseteq |E_\chi|^{\mathbf{Q}}$ be a $\mathbf{Z}[G_\chi]$-module, finitely generated as a $\mathbf{Z}$-module. If H_1 is a submodule of H, we have*

$$[H : H_1] = R_\chi^K(H_1)/R_\chi^K(H).$$

Proposition 2.5. *Let $H \subseteq |E_K|^{\mathbf{Q}}$ be a $\mathbf{Z}[G]$-module, finitely generated as a $\mathbf{Z}$-module. The χ-regulator of H relates to the χ-regulator of $H^{e_{\widetilde{\chi}}}$ by the formula*

$$R_\chi^K(H) = [K : K_\chi]^{\varphi(g_\chi)}R_\chi^{K_\chi}(H^{e_{\widetilde{\chi}}}).$$

The following proposition describes the decomposition of the regulator into χ-parts.

Proposition 2.6. *Let H be a complete $\mathbf{Z}[G]$-submodule of $|E_K|$. The regulator of H admits the following decomposition:*

$$gQ_G R_K(H) = \prod_{\tilde{\chi}\in\tilde{G}}{}' R_\chi^K(H).$$

2.5 Cyclotomic χ-units

In the following we explicitly give a subgroup of E_χ of finite index.

Let χ be an even nontrivial character of conductor f_χ. Let A be the subgroup of $(\mathbf{Z}/f_\chi\mathbf{Z})^\times$ that corresponds to $\mathrm{Gal}(\mathbf{Q}(\zeta_{f_\chi})/K_\chi) = \mathrm{Ker}(\chi)$ and let $A^+ \subset \mathbf{Z}$ be a system of representatives of $A/\{\pm 1\}$. The cardinality of A^+ is $a_\chi = \varphi(f_\chi)/2g_\chi$. Define

$$\Theta_\chi = \prod_{a\in A^+}(\zeta_{2f_\chi}^a - \zeta_{2f_\chi}^{-a}) \in \mathbf{Q}(\zeta_{2f_\chi}), \quad \Lambda_\chi = \prod_{\ell\,|g_\chi}(1-\sigma^{g_\chi/\ell}) \in \mathbf{Z}[G_\chi], \quad (2.5)$$

where ℓ runs through all prime divisors of g_χ and σ is a fixed generator of G_χ. Denote by $\overline{\Lambda}_\chi$ the element obtained from Λ_χ by changing σ to $\overline{\sigma}$, an extension of σ in $K_\chi(\Theta_\chi)$.

Let $\Phi_n(x) = \prod_{(j,n)=1}(x-\zeta_n^j)$ be the nth cyclotomic polynomial.

Lemma 2.3. *We have $\Theta_\chi^2 \in K_\chi$. Moreover, $\Theta_\chi^{1-\overline{\sigma}}$ is a unit of K_χ.*

Proof. We see that $-(1-\zeta_{f_\chi}^a)(1-\zeta_{f_\chi}^{-a}) = (\zeta_{2f_\chi}^a - \zeta_{2f_\chi}^{-a})^2$; hence we have

$$\Theta_\chi^2 = (-1)^{a_\chi} N_{\mathbf{Q}(\zeta_{f_\chi})/K_\chi}(1-\zeta_{f_\chi}) \in K_\chi.$$

For $f_\chi = p^k$, a prime power, $\Phi_{f_\chi}(1) = p$; otherwise, $\Phi_{f_\chi}(1) = 1$. It follows that $1-\zeta_{f_\chi}$ is either a generator of the unique ramified prime ideal or a unit of $\mathbf{Q}(\zeta_{f_\chi})$, respectively. The norm of $1-\zeta_{f_\chi}$ has the same properties in K_χ. Thus $\Theta_\chi^{1-\overline{\sigma}}$ is in both cases a unit of $\mathbf{Q}(\zeta_{2f_\chi})$. Moreover, it belongs to K_χ. Indeed, if $\Theta_\chi \notin K_\chi$, then $K_\chi(\Theta_\chi) \subseteq \mathbf{Q}(\zeta_{2f_\chi})$ is a quadratic and abelian (hence normal) extension of K_χ and we have $K_\chi(\Theta_\chi) = K_\chi(\Theta_\chi^{\overline{\sigma}})$. By writing $\Theta_\chi^{\overline{\sigma}} = a + b\Theta_\chi$ with $a, b, \Theta_\chi^{2\overline{\sigma}} \in K_\chi$, we conclude that $a = 0$. □

Proposition 2.7. *The number $\eta = \Theta_\chi^{\overline{\Lambda}_\chi}$ is a proper χ-unit.*

Proof. By Lemma 2.3, η is a unit in K_χ and $\Theta_\chi^2 \in K_\chi$, hence we have $\eta^2 = \Theta_\chi^{2\overline{\Lambda}_\chi} = \Theta_\chi^{2\Lambda_\chi}$. In order to prove that $\eta \in E_\chi$, it thus suffices to show that $\Lambda_\chi e_{\widetilde{\chi}} = \Lambda_\chi$. Since $\sum_{\widetilde{\chi}\in\widetilde{G}} e_{\widetilde{\chi}} = 1$, it suffices to verify that $\Lambda_\chi e_{\widetilde{\psi}} = 0$ for all characters ψ of G_χ such that $\widetilde{\psi} \neq \widetilde{\chi}$.

When regarding χ and ψ as characters of K_χ, we find $\mathrm{Ker}(\chi) = 1$ and $\mathrm{Ker}(\psi) \neq \mathrm{Ker}(\chi)$. Thus there exists a prime number ℓ dividing $\#\,\mathrm{Ker}(\psi)$. We conclude $\sigma^{g_\chi/\ell} \in \mathrm{Ker}(\psi)$. It follows that $\sigma^{g_\chi/\ell} e_{\widetilde{\psi}} = e_{\widetilde{\psi}}$ and $\Lambda_\chi e_{\widetilde{\psi}} = 0$. $\square$

Definition 2.6. Denote by F_χ the subgroup of E_χ generated by -1 and the conjugates of η. This is called the group of *cyclotomic χ-units*.

We may define the element $\eta' = \Theta_\chi^{\Lambda_\chi}$ up to sign since its square is in K_χ. It follows that we may assume $|F_\chi| = \langle(\pm\eta)^\sigma \mid \sigma \in G_\chi\rangle$ with $\eta = \eta'$.

The group $|F_\chi|$ is a $\mathbf{Z}[G_\chi]$-module. Like $|E_\chi|$, it also admits a $\mathbf{Z}[\zeta_{g_\chi}]$-structure. Later we will show that $[|E_\chi| : |F_\chi|] = [E_\chi : F_\chi]$ is finite.

We prove that, unlike η, the module $|F_\chi|$ is independent of the choice of the generator σ of G_χ. Any factor of Λ_χ is of the form $1 - \tau$ with $\tau = \sigma^{g_\chi/\ell}$ and $\ell \mid g_\chi$ a prime. When we change the generator to any σ^j with $(j, g_\chi) = 1$, this becomes $1-\tau^j = (1-\tau)(1+\tau+\cdots+\tau^{j-1})$. Since the element $\sum_{0<i<j} x^i$ is invertible in $\mathbf{Z}[x]/\langle\Phi_{g_\chi}(x)\rangle \simeq \mathbf{Z}[\zeta_{g_\chi}]$, we conclude that the change of the generator of G_χ has no effect on the $\mathbf{Z}[\zeta_{g_\chi}]$-module $|F_\chi|$, but only on the choice of its generator $\pm\eta$. Consequently, $|F_\chi|$ only depends on $\widetilde{\chi}$.

2.6 Cyclotomic units of K

Define $F_K = \prod'_{\widetilde{\chi}\in\widetilde{G}} F_\chi$. This is called the group of *cyclotomic units of* K. We have $|F_K| = \prod'_{\widetilde{\chi}\in\widetilde{G}} |F_\chi|$ and this product is direct. Since $|E_\chi|$ is simple, the submodule $|F_\chi|$ is also simple or equal to 1 (it will be seen that it is 1 only for $\chi = 1$). Hence $|F_K|$ is a complete $\mathbf{Z}[G]$-module (cf. the proof of Proposition 2.3). We have $F_\chi = F_K^{e_{\widetilde{\chi}}}$.

Denote by Cl_K the class group of K, i.e., the finite abelian group of (nonzero) fractional ideals modulo principal fractional ideals of K. Let h_K be the order of the class group, the class number of K. We are ready to state a fundamental result due to Leopoldt.

Proposition 2.8. *The index of the group of cyclotomic units in the group of units is* $[E_K : F_K] = h_K Q_G$.

Proof. Write the class number formula in the form (cf. [14])

$$h_K R_K = \prod_{\chi\in\widehat{G}}' \sum_{\sigma \bmod \mathrm{Ker}(\chi)} \chi(\sigma^{-1}) \ln|\Theta_\chi^\sigma|,$$

where σ runs through a system of representatives of $G/\operatorname{Ker}(\chi)$ and Θ_χ^σ is defined up to sign. Since $G_\chi \simeq G/\operatorname{Ker}(\chi)$, we may write

$$h_K R_K = \prod_{\widetilde{\chi}\in\widetilde{G}}{}' R_\chi^{K_\chi}(\Theta_\chi).$$

By Propositions 2.6 and 2.5,

$$R_K(F_K) = g^{-1}Q_G^{-1}\prod_{\widetilde{\chi}\in\widetilde{G}}{}' R_\chi^K(F_K), \quad R_\chi^K(F_K) = (g/g_\chi)^{\varphi(g_\chi)}R_\chi^{K_\chi}(\eta).$$

From (2.3) it follows that $R_\chi^{K_\chi}(\eta) = N_{\mathbf{Q}(\zeta_{g_\chi})/\mathbf{Q}}(\chi(\Lambda_\chi))R_\chi^{K_\chi}(\Theta_\chi)$. Write shortly N for $N_{\mathbf{Q}(\zeta_{g_\chi})/\mathbf{Q}}$. In order to calculate $N(\chi(\Lambda_\chi))$, we first note $N(\chi(\Lambda_\chi)) = \prod_{\psi\in\widetilde{\chi}}\prod_{\ell|g_\chi}(\psi(1)-\psi(\sigma^{g_\chi/\ell}))$. Since $\psi(\sigma^{g_\chi/\ell})$ is a primitive ℓth root of unity, we obtain

$$N(\chi(\Lambda_\chi)) = \prod_{\ell\,|g_\chi} N(1-\zeta_\ell) = \prod_{\ell\,|g_\chi} \ell^{\varphi(g_\chi)/(\ell-1)} = g_\chi^{\varphi(g_\chi)}/d_{\widetilde{\chi}},$$

where $d_{\widetilde{\chi}}$ is the absolute value of the discriminant of $\mathbf{Q}(\zeta_{g_\chi})$.

Recall $\sum'_{\widetilde{\chi}\in\widetilde{G}}\varphi(g_\chi) = g-1$. Now by (2.2) and by the definition (1.2) of Q_G, we conclude

$$\begin{aligned}[E_K : F_K] = R_K(F_K)/R_K &= g^{-1}Q_G^{-1}h_K\prod_{\widetilde{\chi}\in\widetilde{G}}{}'(g/g_\chi)^{\varphi(g_\chi)}N(\chi(\Lambda_\chi)) \\ &= Q_G^{-1}h_K g^{g-2}\Big/\prod_{\widetilde{\chi}\in\widetilde{G}}{}' d_{\widetilde{\chi}} = Q_G h_K.\end{aligned}$$

□

2.7 χ-class numbers

Let χ be a nontrivial character of K. One defines the χ-*class number* as $h_\chi = [E_\chi : F_\chi]$. It only depends on $\widetilde{\chi}$. For $\chi = 1$, we set $h_1 = 1$.

Proposition 2.8 implies $[E_K : F_K] < \infty$. By Definition 2.4, we find

$$[E_K : F_K] = [E_K : E_+^K][E_+^K : F_K] = Q_K^+\prod_{\widetilde{\chi}\in\widetilde{G}} h_\chi.$$

It follows that h_χ is always finite. Thus $|F_\chi|$ is a nontrivial simple $\mathbf{Z}[G_\chi]$-module with character $\widetilde{\chi}$ for any $\chi \neq 1$. From Proposition 2.4 and Eq. (2.4), we conclude that h_χ is a norm of an integral ideal in $\mathbf{Q}(\zeta_{g_\chi})$. We state the results.

Proposition 2.9. *The class number h_K of a real abelian field K admits the decomposition*

$$h_K = \frac{Q_K^+}{Q_G} \prod_{\widetilde{\chi} \in \widetilde{G}} h_\chi. \tag{2.6}$$

The numbers $h_\chi = [E_\chi : F_\chi]$ are norms of some integral ideals of $\mathbf{Q}(\zeta_{g_\chi})$.

If p is a prime not dividing g, we have $g^{-1} \equiv a_k \pmod{p^k}$ for some $a_k \in \mathbf{Z}$ with $k = 1, 2, \ldots$. By defining $\alpha^{1/g} = \alpha^{a_k}$ for $\alpha \in \mathrm{Cl}_p$ of order p^k, we may split the p-primary part of Cl_K, i.e., the p-class group Cl_p of K, as a $\mathbf{Z}[G]$-module through the rational idempotents $e_{\widetilde{\chi}}$. We obtain the decomposition (see [17, p. 44])

$$\mathrm{Cl}_p = \mathrm{dir} \prod_{\widetilde{\chi}} \mathrm{Cl}_{\chi,p}, \tag{2.7}$$

where $\mathrm{Cl}_{\chi,p} = \mathrm{Cl}_p^{e_{\widetilde{\chi}}}$ and $\#\mathrm{Cl}_{\chi,p} = h_{\chi,p}$, the p-part of h_χ. The technique used to prove the independence of $(\pm\varepsilon^2)^{e_{\widetilde{\chi}}}$ of the choice of the field containing ε shows that the $\mathbf{Z}[\zeta_{g_\chi}]$-module $\mathrm{Cl}_{\chi,p}$ depends only on K_χ.

The set $\mathrm{Cl}_{\chi,p}$ can also be characterized as the group of ideal classes of order a power of p in K_χ satisfying the following condition: any ideal in the ideal class becomes principal under the relative norm map to any subfield $L \subsetneq K_\chi$ (see [18, p. 40]). Thus the values h_χ also provide structural information on the class group.

This brings us to the actual theme of the present study. The rest of our work will concentrate on the computation of the class number. We will construct an effective method to compute, for $p \nmid 2g$, the p-parts of the class numbers of real abelian fields of degree g. This will be based on the decomposition (2.6).

Remark 2.3. One may also decompose the p-class group through rational p-adic characters $\mathrm{Tr}_{\mathbf{Q}_p(\zeta_{g_\chi})/\mathbf{Q}_p}(\chi)$; this could allow computations as well. Some techniques stemming from this decomposition are briefly surveyed in Chapter 6.

Chapter 3

A condition for the class number divisibility

We give a p-adic condition for the class number divisibility. In this connection we also investigate the p-adic regulator.

3.1 Leopoldt's condition

Leopoldt [18] showed the following fact when proving his theorem about the class number divisibility referred to in the introduction. The proof is based on the decomposition (2.7) of the p-class group, the reflection theorem and Stickelberger theorem.

Lemma 3.1. *Let p be an odd prime dividing neither the conductor nor the degree of a real abelian field K and let χ be a character of K. If $\mathrm{Cl}_{\chi,p} \neq 1$, then*

$$\prod_{\psi \in \widetilde{\chi}} B_{p-1,\psi} \equiv 0 \pmod{p},$$

where $B_{k,\psi}$ is the kth generalized Bernoulli number associated to ψ.

Note that the above product over $\widetilde{\chi}$ is rational.

Later we will give an equivalent condition that allows practical computation, proved by W. Schwarz in his thesis [34, p. 54]. Leopoldt also obtained a result in the ramified case $p \mid f$, $p^2 \nmid f$, but we leave it out from this study for the sake of simplicity; in the computations we dealt with the case $p \mid f$ using another method.

Before stating Schwarz's condition, we derive a result in a more general setting. If we assume that the p-part of the class number is known, this will result in a method to treat the p-divisibility of the p-adic regulator without explicitly knowing the fundamental units, but only the class number.

3.2 Divisibility of the p-adic regulator

In order to investigate the p-adic regulator, one has to work in the p-adic numbers. We thus fix an embedding of K in the algebraic closure $\mathbf{\Omega}_p$ of the p-adic field $\mathbf{Q}_p$. The function v_p will denote the normalized (i.e., $v_p(p) = 1$) exponential valuation on $\mathbf{\Omega}_p$. For $\alpha, \beta \in \mathbf{\Omega}_p$, we may also denote the relation $v_p(\alpha - \beta) \geq k(\geq 1)$ by $\alpha \equiv \beta \pmod{p^k}$.

First recall that for $x \in \mathbf{\Omega}_p, v_p(x) > 0$, $\log_p(1 + x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}x^n}{n}$ defines the p-adic logarithm (extended as usual to all nonzero $x \in \mathbf{\Omega}_p$). Note that $v_p(\log_p(1+x)) = v_p(x)$ when $v_p(x) > 1/(p-1)$. Define the p-adic regulator by replacing all the entries $\ln|\varepsilon|$ in the definition of the ordinary regulator with $\log_p(\varepsilon)$. As this is a p-adic number, it makes sense to speak about its p-divisibility. We will assume $p \nmid 2f$; for $p \mid f$, the method is not sufficient, and the prime 2 is excluded since it was already excluded from the study of the class numbers.

Recall the *p-adic class number formula* [36, Thm. 5.24]:

$$\frac{2^{g-1} h_K R_p(K)}{\sqrt{d_K}} = \prod_{\chi \neq 1} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi),$$

where $R_p(K)$ is the p-adic regulator of K, d_K is the discriminant of K and $L_p(s, \chi)$ is the p-adic L-function associated to a Dirichlet character χ of K. The product extends over all nontrivial characters of K.

The following known lemma focuses on the part of the p-adic class number formula that deserves closer inspection in our work.

Lemma 3.2. *For any odd prime p not dividing the conductor f of K,*

$$v_p(h_K R_p'(K)) = v_p\Big(\prod_{\chi \neq 1} L_p(1, \chi)\Big), \tag{3.1}$$

where $R_p'(K) = R_p(K)/p^{g-1}$ is nonzero and p-integral.

Proof. Let $f(K)$ be the residue class degree and $g(K)$ the number of primes above p in K. As p is unramified in K, we have $g = f(K)g(K)$. The values $\chi(p)$ of the characters of K run through all $f(K)$th roots of unity, each with multiplicity $g(K)$ (see [36, p. 34]). Thus we may equate

$$\prod_{\chi \neq 1} \left(1 - \frac{\chi(p)}{p}\right) = \frac{1}{p^{g-1}(p-1)} \prod_{\chi \in \widehat{G}} (p - \chi(p)) = \frac{p^{1-g}(p^{f(K)} - 1)^{g(K)}}{p - 1}.$$

Since $p \nmid d_K$, the p-adic class number formula implies (3.1).

The nonvanishing of the p-adic regulator is well known. It remains to prove the p-integrality. This follows from the fact that $v_p(\log_p(\varepsilon)) \geq 1$ when

ε is a unit of $\mathbf{Q}(\zeta_f)$; indeed, for any integer $\alpha \in \mathbf{Q}_p(\zeta_f)$, we have $\alpha^{p^{f_p}} \equiv \alpha \pmod{p}$, where f_p is the residue class degree of $\mathbf{Q}_p(\zeta_f)$, i.e., the order of p modulo f, whence

$$\log_p(\varepsilon) = \frac{1}{p^{f_p}-1} \log_p(1 + (\varepsilon^{p^{f_p}-1} - 1)). \qquad \square$$

We will study the right hand side of (3.1). Recall [36, Thm. 5.18] that the p-adic L-function at $s=1$ has the value

$$L_p(1,\chi) = -\left(1 - \frac{\chi(p)}{p}\right) \frac{\tau(\chi)}{f_\chi} \sum_{a=1}^{f_\chi - 1} \overline{\chi}(a) \log_p(1-\zeta^a), \tag{3.2}$$

where χ is a nontrivial character of conductor f_χ, $\overline{\chi} = \chi^{-1}$, $\zeta = \zeta_{f_\chi}$ and $\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a)\zeta^a$ is the *Gauss sum*. For brevity, we will denote $f_\chi = f$.

In order to compute the p-adic value of the product of the class number and the p-adic regulator, we have to compute p-adic approximations modulo p^k, $k \geq 1$, of $L_p(1,\chi)$. We first approximate the p-adic logarithm; we will see later that it suffices to compute an approximation of $\log_p(1-\zeta^p)$. We will compute this modulo p^{k+1} since there is a p in the denominator in (3.2).

For any $n \in \mathbf{N}$, $v_p(\frac{x^n}{n}) = nv_p(x) - v_p(n)$ and $\min(v_p(n), v_p(n+1)) = 0$. Hence in order to compute $\log_p(1+x) \pmod{p^r}$, we must compute at least the first $r-1$ terms of the series defining $\log_p$. If $v_p(r+s) > s$ is satisfied for some $s \geq 0$, we also compute the $(r+s)$th term. In the range of our calculations we confronted this situation only in the form $v_p(r) > 0$. We will subsequently assume that it suffices to compute $r-1$ terms; one may easily manipulate the formulas to cover the other cases.

Let $d \in \mathbf{Z}$ be a multiple of f_p such that $d > k$. Then we may write

$$\begin{aligned}\log_p(1-\zeta^p) &= \frac{1}{p^d-1}\log_p(1 + ((1-\zeta^p)^{p^d-1} - 1)) \\ &\equiv \sum_{j=1}^{k} \frac{(-1)^j}{j}\big((1-\zeta^p)^{p^d-1} - 1\big)^j \pmod{p^{k+1}}.\end{aligned}$$

Any fth root of unity, say η, satisfies

$$\frac{1}{\eta^p - 1} = \frac{1}{f}\sum_{\nu=1}^{f-1} \nu\eta^{p\nu}. \tag{3.3}$$

The computation of $(\zeta^p - 1)^{p^d}$ may be performed by exponentiation by p of polynomials via the isomorphism $\mathbf{Z}[\zeta] \simeq \mathbf{Z}[x]/\langle\Phi_f(x)\rangle$, where Φ_f is the fth cyclotomic polynomial. In practice, it is more efficient to compute modulo $(x^f - 1, p^{k+1})$ and reduce the result modulo $\Phi_f(x)$. For large d, this becomes tedious, therefore we also present an alternative approach (which only depends on f_p and not on the choice of d).

By (3.3) and the binomial formula, we may write

$$(1-\zeta^p)^{p^d-1} = \frac{(\zeta^p-1)^{p^d}}{\zeta^p-1} = \frac{1}{f}\sum_{\nu=1}^{f-1}\nu\zeta^{p\nu}\sum_{i=0}^{p^d}\binom{p^d}{i}(-1)^{p^d-i}\zeta^{pi}. \tag{3.4}$$

We investigate residues of binomial coefficients. For $1 \le j \le p^d$, we have $\frac{j}{p^d}\binom{p^d}{j} = \prod_{i=1}^{j-1}\frac{p^d-i}{i}$ (define an empty product to be equal to 1), which is a p-adic unit. We conclude that there are exactly $\varphi(p^s)$ binomial coefficients satisfying $p^s \| \binom{p^d}{l}$ if $s < d$; they are $\binom{p^d}{mp^{d-s}}$ for $1 \le m < p^s$, $p \nmid m$. Note that the number $\varphi(p^k) = p^{k-1}(p-1)$ grows exponentially in k.

Example 3.1. Let $k = 2$. Then $(1-\zeta^p)^{p^d-1} - 1 \pmod{p^3}$ equals, by (3.4),

$$\frac{1}{f}\sum_{\nu=1}^{f-1}\nu\zeta^{p\nu}\left(\sum_{i=1}^{p-1}\binom{p^d}{ip^{d-1}}(-1)^{i-1}\zeta^i + \sum_{\substack{i=1\\(i,p)=1}}^{p^2-1}\binom{p^d}{ip^{d-2}}(-1)^{i-1}\zeta^{i/p}\right) \pmod{p^3}.$$

We used here the facts that $p^d \equiv 1 \pmod{f}$, $\frac{\zeta^{p^{d+1}}-1}{\zeta^p-1} = 1$ and that p is odd. The residues for the binomial coefficients may be computed as follows (assume $p \nmid i$ and $d > 2$):

$$\binom{p^d}{ip^{d-1}} = \frac{p}{i}\prod_{j=1}^{ip^{d-1}-1}\frac{p^d-j}{j} \equiv \frac{p}{i}(-1)^r\prod_{v_p(j)\ge d-1}\frac{p^d-j}{j} \equiv \frac{p}{i}\prod_{j=1}^{i-1}\frac{p-j}{j} \pmod{p^3},$$

where $r = (ip^{d-1}-1)-(i-1)$ is even. Thus $\binom{p^d}{ip^{d-1}} \equiv \binom{p}{i} \pmod{p^3}$. Moreover,

$$\binom{p^d}{ip^{d-2}} = \frac{p^2}{i}\prod_{j=1}^{ip^{d-2}-1}\frac{p^d-j}{j} \equiv \frac{p^2}{i}(-1)^s\prod_{v_p(j)\ge d}\frac{p^d-j}{j} \equiv \frac{p^2}{i}(-1)^s \pmod{p^3},$$

where $s = ip^{d-2}-1$. Thus $\binom{p^d}{ip^{d-2}} \equiv \frac{p^2}{i}(-1)^{i-1} \pmod{p^3}$.

The computation of the binomial coefficients modulo p^{k+1} for any k may be performed using the same ideas. Naturally, the residues are independent of the choice of d.

Assume that we have computed the coefficients $a_j^{'}$, $0 \le a_j^{'} \le p^{k+1}-1$, in the congruence $(1-\zeta^p)^{p^d-1} \equiv \sum_{j=0}^{\varphi(f)-1} a_j^{'}\zeta^j \pmod{p^{k+1}}$ for some $k \ge 1$ using either of the methods presented above. By the relation $\Phi_f(\zeta) = 0$, we may as well write $\sum_{j=0}^{\varphi(f)-1} a_j^{'}\zeta^j \equiv \sum_{j=1-\varphi(f)/2}^{\varphi(f)/2} a_j\zeta^j \pmod{p^{k+1}}$ for some a_j, $0 \le a_j \le p^{k+1}-1$.

We note that $(1-\zeta^p)^{p^d-1}$ is real; indeed, its complex conjugate equals $(-\zeta^{-p}(1-\zeta^p))^{p^d-1}$ and we have $p^d \equiv 1 \pmod f$ since d is a multiple of f_p. Since $\{1, \zeta^j+\zeta^{-j} \mid 0 < j < \frac{\varphi(f)}{2}\}$ is an integral basis of $\mathbf{Q}(\zeta+\zeta^{-1})/\mathbf{Q}$, it follows that the coefficients a_j satisfy $a_{\varphi(f)/2} = 0$ and $a_j = a_{-j}$ for any $j = 1, \ldots, \frac{\varphi(f)}{2} - 1$. Hence also the coefficients d_j, $0 \le d_j \le p^k - 1$, in $\frac{1}{p}\log_p(1-\zeta^p) \equiv \sum_{j=1-\varphi(f)/2}^{\varphi(f)/2} d_j\zeta^j \pmod{p^k}$ satisfy $d_{\varphi(f)/2} = 0$ and $d_j = d_{-j}$ for any $j = 1, \ldots, \frac{\varphi(f)}{2} - 1$.

We now obtain a formula for $L_p(1,\chi)$ as follows. Since $\sum_{a=1}^{f} \overline{\chi}(a)\zeta^{aj} = \chi(j)\tau(\overline{\chi})$, we may write, following [23],

$$\begin{aligned}\frac{1}{p}\sum_{a=1}^{f}\overline{\chi}(a)\log_p(1-\zeta^a) &= \frac{\overline{\chi}(p)}{p}\sum_{\substack{a=1\\(a,f)=1}}^{f}\overline{\chi}(a)\log_p(1-\zeta^{ap})\\ &\equiv \overline{\chi}(p)\sum_{j=1-\frac{\varphi(f)}{2}}^{\frac{\varphi(f)}{2}-1} d_j\sum_{a=1}^{f}\overline{\chi}(a)\zeta^{aj} = \overline{\chi}(p)\tau(\overline{\chi})\sum_{j=1-\frac{\varphi(f)}{2}}^{\frac{\varphi(f)}{2}-1} d_j\chi(j),\end{aligned}$$

where the congruence is modulo p^k.

By the relation $d_j = d_{-j}$ and by noting that $\chi(0) = 0$ and $\chi(-1) = 1$, we have

$$\sum_{j=1-\frac{\varphi(f)}{2}}^{\frac{\varphi(f)}{2}-1} d_j\chi(j) = 2\sum_{j=1}^{\frac{\varphi(f)}{2}-1} d_j\chi(j).$$

Since $\tau(\chi)\tau(\overline{\chi}) = f$, we conclude

$$\begin{aligned}L_p(1,\chi) &= -\left(1-\frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\overline{\chi}(a)\log_p(1-\zeta^a)\\ &\equiv -2\big(p-\chi(p)\big)\overline{\chi}(p)\sum_{j=1}^{\varphi(f)/2-1} d_j\chi(j) \pmod{p^k}.\end{aligned}$$

By Lemma 3.2, the following now holds:

$$p^k \mid h_K R_p^{'}(K) \iff p^k \mid \prod_{\chi\neq 1}\sum_{j=1}^{\varphi(f_\chi)/2-1} d_j\chi(j). \tag{3.5}$$

Note that the numbers d_j are invariants of the $\mathbf{Q}$-conjugacy class $\widetilde{\chi}$.

Hence the above product over the characters may be split into parts

$$\prod_{\psi\in\widetilde{\chi}} \sum_{j=1}^{\varphi(f_\chi)/2-1} d_j\psi(j) \in \mathbf{Z} \tag{3.6}$$

that may be computed individually. Once we have solved the p-divisibility of $h_K R_p(K)$, we thus know the p-divisibility of $h_L R_p(L)$ for any subfield L of K. The phenomenon is similar to that observed for the class numbers (cf. Eq. (2.6)). For the computation of the product, we suggest the following method from [5], in which the product is regarded as a norm of an element in the field $\mathbf{Q}(\zeta_{g_\chi})$. Indeed, the values of χ are g_χth roots of unity and the product runs through the $\mathbf{Q}$-conjugates χ^k, $(k, g_\chi) = 1$, of χ. We denote by $(ki)_n$ the least positive residue of ki modulo n.

Proposition 3.1 (Fee–Granville). *Let N be the norm of the element $\sum_{i=0}^{n-1} b_i\zeta_n^i \in \mathbf{Q}(\zeta_n)$ to $\mathbf{Q}$. If $t \in \mathbf{Z}$ is positive and satisfies $|N| < \Phi_n(t)/2$, then N is the least residue, in absolute value, of*

$$\prod_{\substack{k=1\\(k,n)=1}}^{n} \sum_{i=0}^{n-1} b_i t^{(ki)_n} \pmod{\Phi_n(t)}.$$

To get an upper bound for the norm, we simply use the triangle inequality and the fact that $|d_j| < p^k/2$.

To determine the p-exponent of $h_K R_p^{'}(K)$, we use the condition in (3.5) for increasing k until for some k the product over the characters is not divisible by p^k. Hence we will always first check the case $k = 1$. For larger k, the efficiency of the method is not so important; indeed, the computations show that in most cases $p \nmid h_K R_p^{'}(K)$.

In this connection we note that the product in (3.5) is a product of norms and that the p-divisibility of an absolute norm of an element in $\mathbf{Z}[\zeta_{g_\chi}]$ implies the divisibility by p^{f_p}, where f_p is the residue class degree, i.e., the order of p modulo g_χ. It follows that $p \mid \prod_{\psi\in\widetilde{\chi}} L_p(1,\psi)$ implies $p^{f_p} \mid h_K R_p^{'}(K)$. In the case $k = 1$ the divisibility of the product $\prod_{\psi\in\widetilde{\chi}} \sum d_j\psi(j)$ in (3.6) by p^{f_p} is, in fact, equivalent to $\sum d_j\psi(j) \equiv 0 \pmod{\mathcal{P}}$ with $\mathcal{P} \mid p$ some prime ideal of $\mathbf{Q}(\zeta_{g_\chi})$. Indeed, all the prime ideals are Galois conjugate. By computing the generators of all the ideals $\mathcal{P}$ above p by a known method, we may check the latter condition as well and thus avoid the computation of the norm.

For the computation of the numbers d_j and the product in the case $k = 1$, there is an efficient method, presented by Schwarz in his thesis [34], which we review in the following. We also refer to an article of Metsänkylä [23].

We found out for $2 < p < 100$ the p-adic values of the product of the class number and the p-adic regulator for any field K of prime conductor

$f < 2000$. We also computed these values for the fields of prime conductor $f < 10000$ for all the odd prime divisors of the class number divisors found in the tables in [16] and [32]. Using these class number tables (also included in our tables for $p \neq 2$; see Chapter 8), we may read from our tables the values for the p-adic regulators.

Remark 3.1. One could as well split the set of characters $\chi \neq 1$ into p-adic conjugacy classes. The product over such a class would then correspond to a norm in $\mathbf{Q}_p(\zeta_{g_\chi})$. By using the above ideas and by approximating suitably the p-adic integers involved, we might also compute the p-adic values of such a product.

3.3 The method of Schwarz

We explain here the method for the case $k = 1$, mostly following Schwarz [34]. The proofs are merely sketched, but they can be read independently of Schwarz's thesis. Denote by $[a]$ the integer part of $a > 0$. We begin with a lemma [34, pp. 45–46].

Lemma 3.3. *If χ is a character of conductor $f_\chi = f$ and order $g_\chi = n$ and $p \nmid 2f$ is a prime, then*

$$B_{p-1,\chi} \equiv -\chi(p) \sum_{i=1}^{f-1} \chi(i) \sum_{\nu=1}^{[\frac{pi}{f}]} \nu^{-1} f^{-1} \pmod{\mathcal{P}_\chi} \tag{3.7}$$

for a prime ideal $\mathcal{P}_\chi \,|\, p$ in $\mathbf{Z}[\zeta_n]$.

Proof. By using properties of p-adic L-functions $L_p(s,\chi)$ (cf. [36, pp. 57–61]), we have

$$B_{p-1,\chi} \equiv L_p(2-p,\chi) \equiv L_p(1,\chi) \pmod{p}.$$

Metsänkylä (see [23], Thm. 2 and its proof) shows that

$$L_p(1,\chi) \equiv -\sum_{i=1}^{f-1} b_i \chi(i) \pmod{p} \tag{3.8}$$

whenever b_i modulo p are rational integers satisfying

$$\lambda(\zeta) = \frac{(\zeta-1)^p - (\zeta^p - 1)}{p(\zeta^p - 1)} \equiv \sum_{i=1}^{f-1} b_i \zeta^i \pmod{p}. \tag{3.9}$$

This follows by using ideas presented in Section 3.2 and by noting that the congruence $\log_p(1-\zeta^p) \equiv 1 - \frac{(\zeta-1)^p}{\zeta^p - 1} \pmod{p^2}$ holds. The numbers b_i are not uniquely defined if f is not prime, but (3.8) holds for any such numbers. (By [34, p. 43], the number $\lambda(\zeta)$ modulo p equals the *Fermat quotient* of $\zeta^p - 1$.)

Let $a \in \mathbf{Z}$, $a \equiv p^{-1} \pmod{f}$. Since $\frac{1}{p}\binom{p}{k} \equiv \frac{(-1)^{k-1}}{k} \pmod{p}$, we may write

$$(1-\zeta)\lambda(\zeta^a) = -\frac{1}{p}\big((\zeta^a-1)^p - (\zeta-1)\big) \equiv \sum_{\mu=0}^{f-1} c_\mu \zeta^\mu \pmod{p}$$

with

$$c_\mu \equiv -\sum_{\substack{k=1 \\ ak\equiv\mu \pmod{f}}}^{p-1} k^{-1} \equiv \sum_{\nu=[\frac{p(\mu-1)}{f}]+1}^{[\frac{p\mu}{f}]} \nu^{-1} f^{-1} \pmod{p}.$$

Define the numbers b_i for all $i \in \mathbf{Z} \setminus f\mathbf{Z}$ by periodicity modulo f. We have

$$(1-\zeta)\lambda(\zeta^a) \equiv (1-\zeta)\sum_{i=1}^{f-1} b_{pi}\zeta^i \equiv \sum_{i=1}^{f-1}(b_{pi} - b_{p(i-1)})\zeta^i \pmod{p}.$$

Consequently, by choosing

$$b_{pi} \equiv \sum_{\nu=1}^{[\frac{pi}{f}]} \nu^{-1} f^{-1} \pmod{p},$$

we see that (3.9) is satisfied.

By the formula (3.8),

$$L_p(1,\chi) \equiv -\sum_{i=1}^{f-1} b_{pi}\chi(pi) \pmod{p}.$$

We conclude that the congruence (3.7) holds modulo p (in $\mathbf{\Omega}_p$). The claim follows since the numbers in (3.7) are p-integers in the field $\mathbf{Q}(\zeta_n)$. □

Proposition 3.2. *Let f be the conductor and n the order of χ. Let*

$$\lambda : (\mathbf{Z}/f\mathbf{Z})^\times \to \{0,\ldots,n-1\}$$

be defined by $\chi(i) = \zeta_n^{\lambda(i)}$. If the prime $p \nmid 2fn$ divides the χ-class number h_χ, then

$$\mathrm{GCD}_{\mathbf{F}_p[x]}\Bigg(\sum_{\substack{i=1 \\ (i,f)=1}}^{f-1} a_i x^{\lambda(i)}, \Phi_n(x)\Bigg) \neq \overline{1}, \tag{3.10}$$

where $a_i \equiv \sum_{\nu=1}^{[\frac{pi}{f}]} \nu^{-1} f^{-1} \pmod{p}$.

Proof. Assume $p \mid h_\chi$. By Lemma 3.1, $\prod_{\chi \in \widetilde{\chi}} B_{p-1,\chi} \equiv 0 \pmod{p}$. Hence it follows from (3.7) that

$$\prod_{\chi \in \widetilde{\chi}} \sum_{i=1}^{f-1} a_i \chi(i) \equiv 0 \pmod{p}.$$

Since the conjugates χ^σ of χ satisfy $\chi^\sigma(i) = \zeta_n^{k\lambda(i)}$ and the zeros of $\Phi_n(x)$ are ζ_n^k for $(k,n) = 1$, we have

$$\prod_{\chi \in \widetilde{\chi}} \sum_{\substack{i=1 \\ (i,f)=1}}^{f-1} a_i \chi(i) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n-1} \sum_{\substack{i=1 \\ (i,f)=1}}^{f-1} a_i \zeta_n^{k\lambda(i)} = \mathrm{Res}\Big(\Phi_n(x), \sum_{\substack{i=1 \\ (i,f)=1}}^{f-1} a_i x^{\lambda(i)}\Big),$$

where $\mathrm{Res}(\cdot,\cdot)$ denotes the resultant. Finally, p divides $\mathrm{Res}(f(x), g(x))$ if and only if $\mathrm{GCD}_{\mathbf{F}_p[x]}(f(x), g(x)) \neq \overline{1}$. The claim follows. $\square$

Remark 3.2. To check whether p^k divides $\mathrm{Res}(f(x), g(x))$ for $k > 1$ is not easy. Hence we have to use a slower method (such as that in Proposition 3.1) to check the condition (3.5) in the case $k > 1$.

The proof of the proposition is essentially found in Schwarz's thesis. But while he showed that such a result holds for a single $\mathbf{Q}$-conjugacy class, he did not relate it to Leopoldt's decomposition of the class number. After observing this relation, we arrive at the result we stated in the proposition; this is more transparent especially in the case of a composite conductor. In particular, Proposition 2.9 gives us the factor group E_χ/F_χ of units that is of order h_χ. This will be applied in Chapter 4 that deals with the computation of the χ-class numbers.

Schwarz also shows that the computational complexity of the method is $O(p + f_\chi + g_\chi^2)$. He used the method to produce, among others, a table of possible class number divisors $p < 100000$ for any real abelian field of conductor $f \leq 500$. This table also gives information on the p-adic regulators; indeed, if p is included in the table for some field K, it means that $v_p(h_K R_p'(K)) \geq 1$.

Remark 3.3. In many cases one could also use the method and the p-adic class number formula to check whether the class number is *not* divisible by a prime dividing the degree of the field. Indeed, if the condition (3.10) is not satisfied for any character of K, then (since $B_{p-1,\chi} \equiv L_p(1,\chi) \pmod{p}$) Lemma 3.2 implies $p \nmid h_K$.

3.4 Examples

There exist families of fields for which it is possible to compute the p-adic regulator in practice. We discuss some easy examples of such computations.

In these fields the fundamental units may be explicitly given by means of Gaussian periods. Hence we may compute the p-adic regulator directly from its definition. We also compute the v_p-value of the product $h_K R_p(K)$ using some previously presented method and in this way obtain the p-part of the class number. Note that the latter is not a new result; the computations of the class numbers of the fields in these families have previously been extended to very large conductors.

The easiest instances of these families of fields are the quadratic fields of the form $\mathbf{Q}(\sqrt{n^2+1})$ or $\mathbf{Q}(\sqrt{n^2+4})$ for any $n \in \mathbf{Z}$. Other known instances are the "simplest cubic fields" found by Shanks [35] and the families of certain fields of degrees 4, 5, 6 and 8 investigated, among others, by M.-N. Gras [8], [9] and Emma Lehmer [19]. In the table of class numbers of Schoof [32], all these fields are marked with an asterisk.

Recall that if $v_p(x) \geq 1$, then $v_p(\log_p(1+x)) = v_p(x)$ and also that $\log_p(\varepsilon) = \frac{1}{p^{f_p}-1}\log_p(1+(\varepsilon^{p^{f_p}-1}-1))$.

Example 3.2. Let $f = 3137 = 56^2+1$ and $p = 3$. The fundamental unit ε of $\mathbf{Q}(\sqrt{f})$ is found using a known method; it is $\varepsilon = 56+\sqrt{3137}$. We have

$$\varepsilon^8 - 1 = 12387712745834496 + 221173895291328\sqrt{3137} = a + b\sqrt{3137}.$$

Then

$$|R_3(\mathbf{Q}(\sqrt{3137}))|_3 = |\,\varepsilon^8-1|_3 = \sqrt{|N(\varepsilon^8-1)|_3} = \sqrt{|a^2-fb^2|_3} = \frac{1}{9}.$$

Using the method we introduced in Section 3.2, we find out that 3^3 divides the product $hR_3/3$, but 3^4 does not. Hence $3^2 \parallel h_{\mathbf{Q}(\sqrt{3137})}$. This agrees with Schoof's tables.

The method of Schwarz shows that the product $hR_5/5$ is not divisible by 5. Indeed, similar calculations as above show that the 5-adic regulator admits no nontrivial divisor 5. Hence it follows (independently of any class number tables) that $3^2 5^0 \parallel h_{\mathbf{Q}(\sqrt{3137})}$.

Example 3.3. It is known that every cyclic cubic field K can be constructed by adjoining to $\mathbf{Q}$ a zero of an irreducible polynomial

$$f_a(x) = x^3 - ax^2 - (a+3)x - 1,$$

where $a \in \mathbf{Q}$. The discriminant of f_a is $(a^2+3a+9)^2$. If we restrict ourselves to the case $a \in \mathbf{Z}, a^2+3a+9$ a prime, we obtain a family called the "simplest cubic fields". These were investigated by Shanks [35], who also computed the fundamental units for these fields. Denoting by θ a zero of f_a, it is easy to verify that the other zeros are $\theta' = -\frac{1}{1+\theta}$ and $\theta'' = -\frac{1}{1+\theta'}$. The Galois group of K is therefore cyclic and generated by $\sigma : \theta \mapsto -\frac{1}{1+\theta}$. In [35] it is shown that θ and $\theta+1$ form a system of fundamental units of K. It follows that the p-adic regulator equals

$$\begin{vmatrix} \log_p(\theta) & \log_p(-\frac{1}{1+\theta}) \\ \log_p(\theta+1) & \log_p(-\frac{1}{1+\theta}+1) \end{vmatrix} = \log_p^2(\theta) - \log_p(\theta)\log_p(1+\theta) + \log_p^2(1+\theta).$$

By calculating the first terms of the series expansion of this sum, we obtain $R_p(K)$ modulo a power of p.

Let $a = 11$. Then $K \subset \mathbf{Q}(\zeta_{163})$. We have

$$-\log_p(\alpha) \equiv \alpha^{p^3-1} - 1 \pmod{p^2}.$$

Let $p = 7$. Using the relation $f_a(\theta) = 0$, we obtain

$$\frac{\theta^{7^3-1}-1}{7} \equiv 2\theta^2 + 3\theta + 4 \pmod 7,$$
$$\frac{(\theta+1)^{7^3-1}-1}{7} \equiv 3\theta^2 + \theta - 1 \pmod 7.$$

Putting all together, we conclude that $R_7(K)/7^2$ is divisible by 7. The method in Section 3.2 shows that $h_K R_7(K)/7^2$ is divisible by 7 but not by 7^2. The above calculation thus indicates that $7 \nmid h_K$.

Let $a = 2$, so $K \subset \mathbf{Q}(\zeta_{19})$ and it is known that $h_K = 1$. Let $p = 7321$. Then

$$\frac{\theta^{7321^3-1}-1}{7321} \equiv 3536 + 63326\theta + 25222\theta^2 \pmod{7321},$$
$$\frac{(\theta+1)^{7321^3-1}-1}{7321} \equiv 1795 + 27\theta + 32722\theta^2 \pmod{7321}.$$

Thus

$$\frac{R_{7321}(K)}{7321^2} \equiv 7321 + 73210\theta \equiv 0 \pmod{7321}.$$

This shows that $7321 \mid \frac{R_{7321}(K)}{7321^2}$, but we do not know the exact value of the 7321-adic regulator; we would have to compute better approximations of the p-adic logarithms (cf. Example 3.1). This was not done since the calculations would have been too long to be practical, due to the large value of p.

Then let $p = 7309$. We have

$$\frac{\theta^{7309^3-1}-1}{7309} \equiv 2230 + 31118\theta + 11165\theta^2 \pmod{7309},$$
$$\frac{(\theta+1)^{7309^3-1}-1}{7309} \equiv 4006 + 28891\theta + 18610\theta^2 \pmod{7309}.$$

Consequently,

$$\frac{R_{7309}(K)}{7309^2} \equiv 1368 + 33810\theta + 8180\theta^2 \pmod{7309}.$$

The norm of this residue over $\mathbf{Q}_{7309}$ is -24918847123. This is not divisible by 7309, thus $7309 \nmid \frac{R_{7309}(K)}{7309^2}$.

We found out that $\frac{R_{7321}(K)}{7321^2} \equiv 0 \pmod{7321}$. As a curiosity, could the residue have been of the form $\sum a_i\theta^i \neq 0$ with absolute norm divisible by p? The answer is negative in this case; we have the well-known fact that if p does not divide the discriminant (722 for $f = 19$) of the power basis $\{1, \theta, \theta^2\}$ of K, then any integer $\alpha \in K$ has a basis representation $a_1 + a_2\theta + a_3\theta^2$ with $a_i \in \mathbf{Q}$ p-integral. Now choose $\beta = \frac{R_{7321}(K)}{7321^2}$ and note that $v_p(\beta) \geq 1$ implies that $\alpha = \beta/p$ is also an integer in K.

For the family of quintic fields of E. Lehmer, there exist results allowing an easy computation of the p-adic regulator modulo a power of p with a procedure similar to the one with cubic fields; see the article of Schoof and Washington [33] for such results. For the other families of fields, one may possibly obtain such results from the works cited.

Remark 3.4. The p-adic class number formula may be regarded as an interpretation of the "index formula" (cf. Proposition 2.4 and [36, p. 153]) for the p-adic regulators of the cyclotomic units and fundamental units. Thus by computing the p-adic regulator of the cyclotomic units via the methods presented in the examples, we obtain $v_p(h_K R_p(K))$. However, this is only a reformulation of the method in Section 3.2.

Chapter 4

Computation of the class number

4.1 Outline of the algorithm

To begin with, we give a framework of the algorithm for the computation of the p-part of the class number. As before, we omit the prime 2 and the primes dividing the degree g of the field K in question. For the prime 2, see, e.g., the article [16].

To check if a prime $p \nmid 2g$ divides the class number of K, it suffices to run the test for all $h_{\chi,p}$ separately, i.e., it is sufficient to study only cyclic fields K_χ and cyclic modules $|F_\chi|$ of cyclotomic units. When computing h_χ, we always choose $K = K_\chi$ and $g = g_\chi$. To find out the p-divisibility of the class number for all real abelian fields of conductor f, we compute $h_{\chi,p}$ for all the nontrivial $\mathbf{Q}$-conjugacy classes of the characters of $\mathbf{Q}(\zeta_f + \zeta_f^{-1})$.

The method consists of three parts. First we put an upper bound for the primes to be tested. For each prime below this bound, we use the method of Schwarz, i.e., check the condition (3.10), and we are left with a small number of primes that must be tested further; for all the other primes p, the χ-class number is not divisible by p. We have to assume here that $p \nmid f$; the primes dividing f will be checked in the second step of the algorithm.

The second step consists of a search for cyclotomic units that are pth powers in the unit group, extending an idea of van der Linden [20]. In this way we can eliminate most of the remaining primes; they do not divide h_χ.

Passing these tests is a necessary condition for the p-divisibility, and after them we have a strong belief that p could divide the χ-class number h_χ, but this is still not a proof. To verify the divisibility, we finally check whether the pth root of a unit found in the second step is in K_χ. We use a method presented in an article of G. and M.-N. Gras [10].

Moreover, we provide a method to check whether h_χ is divisible by a higher power of p. This is also based on ideas in [10].

We limited the search to the fields of conductor $f \leq 2000$ and to the primes $p < 10000$. In theory there could be larger primes dividing these class numbers, but we will see that the heuristics of Cohen and Lenstra [3] and the results of the computations (the largest prime factor found was 379) show this to be very unlikely.

4.2 Search for units of order p

In [20] van der Linden investigated the group E_K/C_K of units modulo (Hasse's) cyclotomic units in connection with class numbers. He introduced a computational method to show in some cases the indivisibility of the class number by a given prime. However, in the general case a similar use of the group E_K/C_K would be problematic since one may have to combine cyclotomic unit groups of subfields in order to obtain a subgroup of units of full rank (cf. [36, p. 150]), and this leads to a complicated module structure. We avoid this problem by applying a similar procedure to the groups E_χ/F_χ.

To check if the p-part of $h_\chi = [E_\chi : F_\chi]$ is nontrivial, we must analyze the group E_χ/F_χ. As noted before, $E_\chi/\{\pm 1\}$ and $F_\chi/\{\pm 1\}$ are $\mathbf{Z}[\zeta_{g_\chi}]$-modules. Recalling that $(\pm\varepsilon)^{e_{\tilde{\chi}}} = \pm\varepsilon$ for any $\varepsilon \in E_\chi$ and that $\mathbf{Z}[G_\chi]e_{\tilde{\chi}} \simeq \mathbf{Z}[\zeta_{g_\chi}]$, we may also regard $|E_\chi|$ and $|F_\chi|$ as $\mathbf{Z}[G_\chi]$-modules. Hence F_χ/F_χ^p admits an $\mathbf{F}_p[G_\chi]$-module structure, where $F_\chi^p = \{x^p \mid x \in F_\chi\}$.

The map $xF_\chi \mapsto x^p F_\chi^p$ defines an isomorphism

$$(E_\chi/F_\chi)_p \simeq (E_\chi^p \cap F_\chi)/F_\chi^p,$$

where $(E_\chi/F_\chi)_p$ is the p-elementary subgroup (the group of elements of order 1 or p). For the injectivity of the map, note that for any real numbers x, y and for odd p, $x^p = y^p$ only if $x = y$.

If $h_{\chi,p} \neq 1$, then the group $(E_\chi^p \cap F_\chi)/F_\chi^p$ is a nontrivial $\mathbf{F}_p[G_\chi]$-submodule of F_χ/F_χ^p. Hence it must contain a minimal submodule of F_χ/F_χ^p. Let this be F_i/F_χ^p; then we have $F_i \subseteq E_\chi^p$. On the other hand, if F_j/F_χ^p is any minimal submodule of F_χ/F_χ^p such that $F_j \subseteq E_\chi^p$, then F_j/F_χ^p is a submodule of $(E_\chi^p \cap F_\chi)/F_\chi^p$. Since the intersection of two different minimal submodules is zero, the p-exponent of h_χ is at least the number of minimal submodules F_i/F_χ^p satisfying $F_i \subseteq E_\chi^p$.

In order to prove that $h_{\chi,p} = 1$, it suffices to compute all the minimal submodules of F_χ/F_χ^p and to check that all of them contain elements that are not pth powers of units. This is not difficult since the minimal submodules are cyclic and easily determined by the following proposition and remark. Recall that the $\mathbf{Z}[G_\chi]$-module $|F_\chi|$ is generated by $\pm\eta = (\pm\Theta_\chi)^{\Lambda_\chi}$, where Θ_χ and Λ_χ are defined by (2.5). Note that, as for $|F_\chi|$ (see Section 2.5), we may assume that F_χ/F_χ^p is generated by $\eta = \eta' = \Theta_\chi^{\Lambda_\chi}$; this will also be assumed in general whenever the sign is inessential and p is odd.

Proposition 4.1. *Assume that* $p \equiv 1 \pmod{g_\chi}$. *The minimal* $\mathbf{F}_p[G_\chi]$-*submodules of* F_χ/F_χ^p *are* $\langle \eta^{\Phi_{g_\chi}(\sigma)/(\sigma - i)} \rangle$, *where* i *runs through all the zeros of* $\Phi_{g_\chi}(x) \pmod p$ *and* σ *is a generator of* G_χ.

Proof. Consider the $\mathbf{F}_p[G_\chi]$-homomorphism

$$\tau : \mathbf{F}_p[G_\chi] \to F_\chi/F_\chi^p, \quad \delta \mapsto \eta^\delta F_\chi^p.$$

It is obviously well-defined and surjective. Its kernel is an $\mathbf{F}_p[G_\chi]$-module, i.e., an ideal in the principal ideal ring $\mathbf{F}_p[G_\chi] \simeq \mathbf{F}_p[x]/\langle x^{g_\chi} - 1\rangle$. Since F_χ is of finite index in E_χ, the $\mathbf{Z}$-rank of $|F_\chi|$ is equal to $\varphi(g_\chi)$. Thus the $\mathbf{F}_p$-rank of F_χ/F_χ^p is $\varphi(g_\chi)$; indeed, a $\mathbf{Z}$-basis $\{x_1, \ldots, x_k\}$ of $|F_\chi|$ induces an $\mathbf{F}_p$-basis $\{x_1 F_\chi^p, \ldots, x_k F_\chi^p\}$ of F_χ/F_χ^p.

Since Θ_χ^2 is an element of K_χ, we conclude $\Theta_\chi^{\sigma^{g_\chi}-1} = \pm 1$. The known relation $x^m - 1 = \prod_{d|m} \Phi_d(x)$ implies that $\sigma^{g_\chi} - 1 = \prod_{d|g_\chi} \Phi_d(\sigma)$. It follows that Λ_χ is divisible by all the $\Phi_d(\sigma)$ with $d \neq g_\chi$, whence $\eta^{\Phi_{g_\chi}(\sigma)} = \pm 1$. Consequently, the kernel $\mathrm{Ker}(\tau) \supseteq \langle \Phi_{g_\chi}(\sigma)\rangle$. The rank argument then implies that, in fact, these sets are equal.

We have proved the isomorphism

$$F_\chi/F_\chi^p \simeq \mathbf{F}_p[G_\chi]/\langle \Phi_{g_\chi}(\sigma)\rangle. \tag{4.1}$$

By the assumption on p, the cyclotomic polynomial $\Phi_{g_\chi}(x)$ factors completely modulo p and we have the evident $\mathbf{F}_p[G_\chi]$-isomorphisms

$$\mathbf{F}_p[G_\chi]/\langle \Phi_{g_\chi}(\sigma)\rangle \simeq \mathbf{F}_p[x]/\langle x^{g_\chi} - 1, \Phi_{g_\chi}(x)\rangle \simeq \mathbf{F}_p[x]/\langle \Phi_{g_\chi}(x)\rangle \simeq \mathbf{F}_p^{\varphi(g_\chi)}.$$

The minimal submodules of $\mathbf{F}_p^{\varphi(g_\chi)}$ are $\langle (1, 0, \ldots, 0)\rangle, \ldots, \langle (0, \ldots, 0, 1)\rangle$. By the above isomorphism, they correspond to the modules $\langle \Phi_{g_\chi}(\sigma)/(\sigma - i)\rangle$ in $\mathbf{F}_p[G_\chi]/\langle \Phi_{g_\chi}(\sigma)\rangle$, where $\sigma - i$ runs through the factors of $\Phi_{g_\chi}(\sigma) \pmod p$. The claim follows. $\square$

Remark 4.1. The proposition generalizes to all odd primes p not dividing g_χ. Indeed, choose the smallest $f_p \geq 1$ such that $p^{f_p} \equiv 1 \pmod{g_\chi}$. The g_χth cyclotomic polynomial factors over $\mathbf{F}_p$ into $\varphi(g_\chi)/f_p$ distinct polynomials $f_i(x)$ of degree f_p; hence $\mathbf{F}_p[G_\chi]/\langle \Phi_{g_\chi}(\sigma)\rangle \simeq (\mathrm{GF}(p^{f_p}))^{\varphi(g_\chi)/f_p}$. Then the minimal submodules of F_χ/F_χ^p are $\langle \eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}\rangle$.

It is also important to note that if a prime p of order f_p modulo g_χ divides h_χ, then also p^{f_p} divides h_χ. This follows from the fact, stated in Proposition 2.9, that h_χ is a norm of an integral ideal.

Remark 4.2. In particular, let $g_\chi = p^\nu$ be an odd prime power. The unique minimal ideal of $\mathbf{F}_p[x]/\langle (x-1)^{\varphi(p^\nu)}\rangle \simeq \mathbf{F}_p[\zeta_{p^\nu}]$ is $\langle (x-1)^{\varphi(p^\nu)-1}\rangle$. More generally, if $g_\chi = np^\nu$ with $(n,p)=1$, we have $\Phi_{g_\chi} = \Phi_n^{\varphi(p^\nu)}$ in $\mathbf{F}_p[x]$, where Φ_n factors into $\varphi(n)/f_p$ distinct polynomials of degree f_p, where f_p is the order of p modulo n. Hence we might also compute the prime divisors of h_χ that divide g_χ. This was not done since the difficulty of computing such factors of the class number h_K lies in computing the index Q_K^+ (see Chapter 7).

By the above considerations, to examine if $F_i \subseteq E_\chi^p$, it suffices to check whether $\eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ is the pth power of some $\varepsilon \in E_\chi$. We explain how this will be done, following [20]. Later we will also need the fact that $\varepsilon \notin F_\chi$; this follows from the nontriviality of F_i/F_χ^p.

Choose a prime $q \equiv 1 \pmod{2pf_\chi}$ and some $b \in \mathbf{Z}$ satisfying the conditions $b^{2f_\chi} \equiv 1 \pmod{q}$, $b \not\equiv 1 \pmod{q}$. Then $\zeta_{2f_\chi} \equiv b \pmod{\mathcal{Q}}$ for some prime ideal $\mathcal{Q}$ above q in $\mathbf{Q}(\zeta_{2f_\chi})$. By writing $\eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ as a rational function $r(\zeta_{2f_\chi})$, we examine whether

$$r(b)^{\frac{q-1}{p}} \equiv 1 \pmod{q}. \tag{4.2}$$

Indeed, this must hold if $r(\zeta_{2f_\chi}) = \varepsilon^p$. If the congruence holds, we choose another pair (q,b) and repeat the test; if the congruence condition is not satisfied for some pair, we conclude that $F_i \not\subseteq E_\chi^p$. If for every submodule F_i there exists a pair (q,b) not satisfying the congruence, we have the result $p \nmid h_\chi$. Otherwise, if there is a prime p and a submodule F_i which pass the congruence test for many pairs, this gives strong evidence that p would divide the class number. But since this process involves uncertainty, we still have to apply another method.

Remark 4.3. Instead of ζ_{2f_χ}, we may actually use f_χth roots of unity in the above computations. Indeed, by Lemma 2.3, $\Theta_\chi^{\sigma-1}$ (defined up to sign) belongs to K_χ, hence it may always be written as a rational function of ζ_{f_χ}.

4.3 Verification of the p-divisibility

For some $\alpha = \eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ satisfying (4.2) for many pairs (q,b), we want to verify that α is a pth power in E_χ. This is equivalent to showing that $\sqrt[p]{\alpha}$ is an element of K_χ. As a unit of K_χ, the element α has g_χ conjugates in K_χ. We calculate an approximation of α and its conjugates α^σ as real numbers by noting that

$$\frac{\zeta_{2f}^a - \zeta_{2f}^{-a}}{\zeta_{2f} - \zeta_{2f}^{-1}} = \frac{\sin(a\pi/f)}{\sin(\pi/f)}.$$

If the polynomial $m_p(x) = \prod_\sigma (x - \sqrt[p]{\alpha^\sigma})$ has integral coefficients, then α is a pth power; this is the minimum polynomial of $\sqrt[p]{\alpha}$. Then also $\sqrt[p]{\alpha^\sigma} = \sqrt[p]{\alpha}^{\,\sigma}$ and $\sqrt[p]{\alpha} \in K_\chi$. But since we have used only approximations, this is still not a proof.

Denote by $\widetilde{m}_p$ the polynomial that we have computed in this way to approximate m_p. If some coefficient of $\widetilde{m}_p$ is not close to an integer, this shows that α is not a pth power, given that the precision in the computations is adequate. Otherwise, if all the coefficients of $\widetilde{m}_p$ are very close to integers, we round off the coefficients to obtain the supposed minimum polynomial $m_p(x) \in \mathbf{Z}[x]$. We then check whether $m_p(x) \mid m(x^p)$, where $m(x)$ is the minimum polynomial of α. If this holds, it finally proves that m_p is the minimum polynomial of $\sqrt[p]{\alpha}$ and that $\sqrt[p]{\alpha}$ is an element of K_χ.

Since we actually compute α in F_χ/F_χ^p, note that we may minimize modulo p the absolute values of the coefficients of $\Phi_{g_\chi}(x)/f_i(x) \in \mathbf{Z}[x]$ in order to prevent coefficient explosion.

Remark 4.4. We were able to use this method in all the cases confronted in the computations, despite the fact that the coefficients of the minimum polynomials were sometimes huge. We note here that G. Gras and S. Jeannin [11] refined this method and showed that to prove an element to be a pth power, it essentially suffices to compute the approximations of the pth roots of the conjugates and to check that their sum is sufficiently close to an integer.

Remark 4.5. One may avoid computations involving minimum polynomials also using the following method (cf. [1]). First compute an integral basis $\{v_i \mid 1 \leq i \leq g_\chi\}$ of K_χ and the representation of $\alpha = \sum_i x_i v_i$ in this basis. If we claim that α is a pth power of a unit, we should be able to calculate the basis representation of the pth root $\sqrt[p]{\alpha} = \sum_i y_i v_i$ with some $y_i \in \mathbf{Z}$.

To solve the y_i, compute for any $\sigma \in G_\chi$ an approximate value of $\sqrt[p]{\alpha^\sigma}$ and write $\sqrt[p]{\alpha^\sigma} = \sum_i y_i v_i^\sigma$. We have g_χ equations and g_χ coefficients y_i to solve, hence we may compute all the y_i. They should be very close to integers if the precision is adequate; round them off to the nearest integers. Finally check whether $(\sum_i y_i v_i)^p = \sum_i x_i v_i$. If we cannot find $y_i \in \mathbf{Z}$ satisfying this relation, the claim seems to be false, which in turn should be verified using the method in Section 4.2.

4.4 Higher powers of p

Suppose that using the preceding method we have found a prime p with $p \mid h_\chi$. We want to check whether h_χ is divisible by a higher power of p. G. and M.-N. Gras [10] introduced a method with which this verification is in principle possible. Our approach earlier in this chapter was reminiscent of their procedure (see Remark 4.7), so it would be natural to assume that similar ideas could be applied in our case as well.

The following lemma describes the correspondence we found between our and Gras's approach. By combining this result with our method as shown later in this section, we are able to check all the cases with $p \equiv 1 \pmod{g_\chi}$ encountered in the computations.

Lemma 4.1. *Let $n \geq 2$ and assume $p \equiv 1 \pmod{n}$. Let $k \in \mathbf{Z}$ be a zero of $\Phi_n(x)$ modulo p. We have*

$$\frac{\Phi_n(\zeta_n)}{\zeta_n - k} \equiv \pm \frac{N(\zeta_n - k)}{\zeta_n - k} \pmod{p\mathbf{Z}[\zeta_n]},$$

where $N(\gamma)$ denotes the absolute norm of $\gamma \in \mathbf{Z}[\zeta_n]$.

Proof. By the assumption on p, all the zeros of $\Phi_n(x) \pmod{p}$ are of the form k^j, where $(j,n) = 1$. Thus the prime ideals of $\mathbf{Z}[\zeta_n]$ above p are $\mathcal{P}_j = \langle p, \zeta_n - k^j \rangle$, $(j,n) = 1$ (see [36, p. 15]). Write the claim in the form

$$\prod_{\substack{j=2 \\ (j,n)=1}}^{n} (\zeta_n - k^j) \equiv \pm \prod_{\substack{j=2 \\ (j,n)=1}}^{n} (\zeta_n^j - k) \pmod{p\mathbf{Z}[\zeta_n]}.$$

Since $\zeta_n \equiv k \pmod{\mathcal{P}_1}$, this congruence holds modulo $\mathcal{P}_1$. Moreover, since the automorphisms $\zeta_n \mapsto \zeta_n^j, (j,n) = 1$, permute the prime ideals, we see that both products contain a factor divisible by $\mathcal{P}_i$ for any $i \neq 1$. $\square$

Assume $p \mid h_\chi$ and $p \equiv 1 \pmod{g_\chi}$ and let σ be a fixed generator of G_χ. Let $N(\sigma - k) = \prod_{j=1,(j,g_\chi)=1}^{g_\chi} (\sigma^j - k) \in \mathbf{Z}[G_\chi]$. By the isomorphism $\mathbf{Z}[\zeta_{g_\chi}] \simeq \mathbf{Z}[G_\chi]/\langle \Phi_{g_\chi}(\sigma) \rangle$ and the lemma, we write in $\mathbf{Z}[G_\chi]$

$$\frac{\Phi_{g_\chi}(\sigma)}{\sigma - k} \equiv \pm \frac{N(\sigma - k)}{\sigma - k} \pmod{p, \Phi_{g_\chi}(\sigma)}. \tag{4.3}$$

Hence the isomorphism (4.1) implies that $\eta^{\Phi_{g_\chi}(\sigma)/(\sigma - k)}$ is a pth power in E_χ only if $\eta^{N(\sigma-k)/(\sigma-k)}$ is a pth power in E_χ. We know by elementary algebraic number theory that $N_{\mathbf{Q}(\zeta_{g_\chi})/\mathbf{Q}}(\zeta_{g_\chi} - k) = pm \in p\mathbf{Z}$ with $p \nmid m$ (if $p \mid m$, change k to some $k + tp$ until $p \nmid m$; in principle there could be some rare special cases where this might not be possible, but we did not meet any such cases in the practical computations). Hence $N(\sigma - k) \equiv pm \pmod{\Phi_{g_\chi}(\sigma)}$ and we have $\eta^{pm/(\sigma-k)} = \varepsilon^p$ for some $\varepsilon \in E_\chi \setminus F_\chi$ (see the paragraph after Remark 4.2). From this it follows that $\varepsilon^{\sigma - k} = \eta^m$.

Let $F'_\chi = \langle -1, \varepsilon^\tau \mid \tau \in G_\chi \rangle$. Then $|F'_\chi|$ is a $\mathbf{Z}[G_\chi]$-module. Since $\varepsilon \notin F_\chi$, but $\varepsilon^p \in F_\chi$ and $\varepsilon^\sigma = \varepsilon^k \eta^m$, we have $[F_\chi F'_\chi : F_\chi] = p$. On the other hand, $p \nmid [F_\chi F'_\chi : F'_\chi]$ since $\eta^m \in F'_\chi$ and F'_χ is closed under σ-conjugation. From

$p \,|\, [F_\chi F_\chi' : F_\chi^m]$, we thus deduce $[F_\chi' : F_\chi^m] = pu$ with some $u \in \mathbf{Z}, p \nmid u$. Finally, since $[E_\chi : F_\chi^m] = [E_\chi : F_\chi][F_\chi : F_\chi^m] < \infty$, we conclude that $[E_\chi : F_\chi'] < \infty$ and that the p-exponent of $[E_\chi : F_\chi']$ is equal to the p-exponent of h_χ/p. Look at the diagram below.

$$\begin{tikzcd}
& E_\chi \arrow[d, dash] & \\
& F_\chi F_\chi' \arrow[dl, dash, "p"'] \arrow[dr, dash] & \\
F_\chi \arrow[dr, dash] & & F_\chi' \arrow[dl, dash, "pu"] \\
& F_\chi^m &
\end{tikzcd}$$

Now we run the verification procedure (see Sections 4.2 and 4.3) using F_χ' in place of F_χ. To see that Proposition 4.1 holds with ε in place of η, observe that $|F_\chi'|$ is cyclic of $\mathbf{Z}$-rank $\varphi(g_\chi)$ and that $\varepsilon^{\Phi_{g_\chi}(\sigma)} = \pm 1$; the latter holds since $\varepsilon^p \in F_\chi$. We thus check whether $\varepsilon^{\Phi_{g_\chi}(\sigma)/(\sigma-j)}$ is a pth power for any j satisfying $\Phi_{g_\chi}(j) \equiv 0 \pmod p$. By (4.3), this is equivalent to checking whether $\varepsilon^{N(\sigma-j)/(\sigma-j)}$ is a pth power. We may compute $\varepsilon = \sqrt[p]{\eta^{N(\sigma-j)/(\sigma-j)}}$ and its conjugates ε^{σ^k} with a sufficient precision. It follows that we may compute an approximation of any conjugate of $\varepsilon^{\Phi_{g_\chi}(\sigma)/(\sigma-j)}$.

In fact, one knows a priori that it suffices to check only those minimal submodules of $F_\chi'/F_\chi'^p$ that correspond to the minimal submodules of F_χ/F_χ^p found to contain pth powers. Indeed, assume

$$\varepsilon \in E_\chi \setminus F_\chi, \quad \varepsilon^p = \eta^{N(\sigma-i)/(\sigma-i)}; \quad \rho \in E_\chi \setminus F_\chi', \quad \rho^p = \varepsilon^{N(\sigma-j)/(\sigma-j)},$$

where $i \neq j$. Let ε_1 be the real number defined by $\varepsilon_1^p = \eta^{N(\sigma-j)/(\sigma-j)}$. If $N(\sigma - i) = pm_1$ with $p \nmid m_1$, we have $\eta^{m_1} = \varepsilon^{\sigma-i}$, so $\varepsilon_1^{m_1} = \rho^{\sigma-i} \in E_\chi$. Since trivially $\varepsilon_1^p \in E_\chi$ and $(p, m_1) = 1$, we conclude $\varepsilon_1 \in E_\chi$.

This method seems to fail for $p \not\equiv 1 \pmod{g_\chi}$. Indeed, our algorithm in Section 4.2 only gives us pth powers explicitly, although we know by the theory that there also exist p^{f_p}th powers, where f_p is the residue class degree. Nevertheless, if we find that $p \,|\, h_\chi$, we may check whether the number $\varepsilon \in \mathbf{R}$ satisfying $\varepsilon^{p^{f_p}} = \eta^{N(f_i(\sigma))/f_i(\sigma)}$ belongs to $E_\chi \setminus F_\chi$ for some i. In this way we may still find a p^{f_p}th power in E_χ, but whether this happens remains theoretically unproven since there is no result similar to (4.3). In the computations this was possible in all the cases we confronted; indeed, the results in [10] give evidence that this should always be the case. Choose again $\langle -1, \varepsilon^{\tau} \mid \tau \in G_{\chi}\rangle = F_{\chi}^{'}$. A similar reasoning as above shows that the p-exponent of $[E_{\chi} : F_{\chi}^{'}]$ is equal to the p-exponent of h_{χ}/p^{f_p}. Finally, using our algorithm (with $F_{\chi}^{'}$ in place of F_{χ}), we can check whether $p \mid (h_{\chi}/p^{f_p})$.

In this way we were able to verify that among the fields of conductor at most 2000 there are only the following two cases in which h_{χ} contains p^{f_p} more than once (both with $f_p = 1$). The 17-class number of a 16-degree field of conductor 1921 is 17^3 and the 3-class number of the quadratic field of prime conductor 1129 is 3^2. The latter is also found in Schoof's table [32]. Additionally, we verified that all the other higher powers of p found in his table could also be determined with our method.

Remark 4.6. If a practical upper bound for h_K was known and $Q_K = Q_G$ (for instance, if K is cyclic of prime degree), then also the fundamental units of K might be computed with this method. Indeed, by successively applying the procedure for any $\widetilde{\chi}$ and for any p below the bound for h_K, it would be possible to find an element ε for which $[E_{\chi} : \langle -1, \varepsilon^{\tau} \mid \tau \in G_{\chi}\rangle] = 1$.

Remark 4.7. G. and M.-N. Gras [10] computed class numbers of abelian fields of small degree using a method quite similar to our method of finding pth powers. They also used Leopoldt's condition similar to Schwarz's method to limit the number of possible divisors. The tables [7] and [8] were computed using this method. The aim in [10] was to compute class numbers of real abelian fields using explicit upper bounds that are practical only in small degree fields; hence the efficiency of the algorithm was not as crucial as in our computations. On the other hand, the efficiency might be improved using first the congruence method as in Section 4.2 (see (4.2)). Gras's method essentially consists of a search of units of $E_{\chi}^{\mathcal{P}}$ belonging to F_{χ}, where $\mathcal{P}$ is a prime ideal of $\mathbf{Z}[\zeta_{g_{\chi}}]$ above p; this amounts to searching for units of the form $(\eta^{N(f_i(\sigma))/f_i(\sigma)})^{1/p^{f_p}}$ with $\mathcal{P} = \langle p, f_i(\zeta_{g_{\chi}})\rangle$. This suggests that our method could similarly be generalized to search (by the isomorphism $\mathbf{Z}[\zeta_{g_{\chi}}] \simeq \mathbf{Z}[G_{\chi}]/\langle \Phi_{g_{\chi}}(\sigma)\rangle$) for $\mathcal{P}$th powers in E_{χ}. This would settle more naturally the case of a larger residue class degree. One possibility would be to investigate the group $(E_{\chi}/F_{\chi})_{\mathcal{P}}$ (the $\mathcal{P}$-part will be defined in Chapter 5).

4.5 An example of the calculation

The following example shows how the calculations were done. We choose $K = \mathbf{Q}(\zeta_f + \zeta_f^{-1})$ with $f = 1261 = 13 \cdot 97$. There are 47 real cyclic fields of conductor f corresponding to the nontrivial $\mathbf{Q}$-conjugacy classes of characters of K.

We run for any χ-class number the first step of the method by checking whether the condition (3.10) holds. All the necessary information for the computation may be gathered from the knowledge of the corresponding $\mathbf{Q}$-conjugacy class $\widetilde{\chi}$. This is the lengthy part of the calculation since we check all the primes $2 < p < 10000$, $p \nmid f$, for all the 47 different h_χ. We find out that there are in total 68 primes (counted with multiplicity) that satisfy (3.10) for some h_χ, of which 10 primes divide g_χ. We continue to the second step only with the primes not dividing g_χ (the 10 discarded primes of course would also contain some information of the class number divisibility, but they would require another method; cf. Remark 4.2). Usually the number of primes satisfying (3.10) was found to be proportional to the number of different h_χ.

In the second step we check all the remaining 58 cases. We also check for all different h_χ the primes 13 and 97 dividing f. There are a total of 152 pairs (h_χ, p) to check. For instance, we have the prime candidate 2689 in the field of degree 96 corresponding to the character $\chi = \chi_{13}^1 \chi_{97}^9$. Since $2689 \equiv 1 \pmod{96}$, there are 96 minimal submodules corresponding to the various $\alpha_i = \eta^{\Phi_{96}(\sigma)/(\sigma - i)}$. We choose a pair (q, b) and check the congruence (4.2). For instance, the pair $(74598239, 46979)$ is appropriate. For this pair, the congruence (4.2) is not satisfied for any α_i, thus $2689 \nmid h_\chi$. All the primes are checked similarly; we can handle all the primes not dividing the class number in this way. An example of a prime dividing the class number is given in the following.

Let $p = 97$ and $\chi = \chi_{13}^2 \chi_{97}^{10}$. We compute 10 pairs (q, b) and notice that (4.2) is always satisfied for the minimal submodule corresponding to $f_i(\sigma) = \sigma + 48$ (the specific minimal submodule depends on the choice of the generator σ of G_χ; we had σ defined by $\zeta_f \mapsto \zeta_f^{19}$). We move on to the third step and compute a real approximation of $\eta^{\Phi_{96}(\sigma)/(\sigma+48)}$ and its conjugates. Its minimum polynomial has huge coefficients, thus it is first important to reduce the coefficients of $\Phi_{96}(\sigma)/(\sigma + 48) \in \mathbf{F}_{97}[G_\chi]$. Choosing the coefficients with the smallest absolute value modulo p seems to be adequate; denote by α the element thus obtained. The precision we needed in this case was over 5000 digits in order to be able to compute the minimum polynomial $m(x)$ of α. The choice of the coefficients of α was probably not ideal. Nevertheless, this was still possible to handle with computer. The minimum polynomial $m_p(x)$ of $\sqrt[p]{\alpha}$ was computed in the same manner; it had much smaller coefficients, the largest with 54 digits. Finally we checked that $m_p(x)$ divides $m(x^p)$. Moreover, we used the method of higher powers of p to verify that $p^2 \nmid h_\chi$.

There were altogether three pairs (h_χ, p) with p not dividing f (indeed, with $p = 5$ or 7; see Table 1) for which we could not find any pairs (q, b) failing to satisfy (4.2). They were all verified to be actual class number divisors using the method in Section 4.3.

The computing time of all the above was approximately one hour using Mathematica 4.1 [38] on an AMD Athlon 2000+.

4.6 Discriminant bounds

As explained before, our class number tables do not give rigorous results: in theory there could exist huge prime factors not found in the tables. This question will be discussed in Chapter 5, but first we review a method that allows rigorous computation in the case of a small conductor.

In this kind of computation one needs for the class number an upper bound that is both rigorous and practical, i.e., not too large. Such bounds are provided for fields of small conductor by Odlyzko's discriminant bounds. Using them, van der Linden [20] (extending previous similar computations by Masley [21]) was able to compute (assuming GRH, the generalized Riemann hypothesis, in some cases) the class numbers of a large collection of real abelian fields of conductor at most 200. For prime conductors, the calculations were extended to all the fields of conductor at most 163. The table we computed (supplemented by the table of Schwarz [34]) allows to extend these calculations somewhat; indeed, we may verify all the class numbers whose upper bounds lie below 100000.

The argument is as follows (see [21]): A. Odlyzko [26] computed a table of pairs (A, E) such that for any totally real field K of degree n and discriminant d_K and for any $x \geq n$, $d_K^{1/n} \geq Ae^{-E/x}$. Using this fact, Masley proved that $d_K^{1/n} < Ae^{-E/x}$ implies $h_K < x/n$. By designing conditions for the p-divisibility, one was then able to rule out all the primes not dividing the class number. Typical for these conditions was that each of them would only apply to some of the primes p below the bound, but by combining the results from different conditions one could in some cases exclude all the primes below the bound and arrive at the conclusion that $h_K = 1$. The prime 2 was always handled separately. All the odd class number divisors confronted could be verified using genus theory; this is practical only in some special cases for primes dividing the degree, hence it was left out of our study. For the remaining primes that could not be handled using any of these conditions, van der Linden used the condition we modified in Section 4.2 and, with the aid of a computer, arrived to his conclusions.

We add here some results that follow from our computations. Under GRH, Odlyzko obtained pairs (A, E) that lead to better bounds; this is why some of the results of van der Linden only hold under GRH. Assuming GRH and comparing the pairs to the class number bound 100000 of the tables of Schwarz, we find that the upper bounds seem to be practical for A up to a bound close to 185. Indeed, for $A = 185.592$ we have $E = 70185$ in the table

[26], and this usually leads to upper bounds below 100000; but $E = 158820$ for $A = 188.628$, and this is too large for us. In general, the values for E in the table increase with A.

The condition $d_K^{1/n} < 185$ is satisfied for all the fields of prime conductor $f \le 193$. For composite conductors $f < 300$ excluding 287, 289 and 299 and for most of the even conductors $f < 400$, this condition is satisfied for the field $K = \mathbf{Q}(\zeta_f + \zeta_f^{-1})$. It would be easy to prove (see [21]) that $d_L^{1/n_L} \le d_K^{1/n_K}$ for any subfield $L \subseteq K$; hence the upper bounds for K hold also for the class numbers of its subfields. By (2.6), we see that the class number of any subfield of K may be divisible only by primes dividing either the degree of K or h_K.

We conclude that, under GRH, for any real abelian field of the above mentioned conductors, the class number factors in our table certainly give the exact class number part coprime to 2 and the degree of the field. In particular, there are six fields $\mathbf{Q}(\zeta_f + \zeta_f^{-1})$ of prime conductor $f > 163$, namely with $f = 167, 173, 179, 181, 191, 193$. The field of conductor 191 has class number part (coprime to 2 and the degree of the field) equal to 11, and this is the only nontrivial class number factor found among these fields.

Chapter 5

Heuristics

In this chapter we will compare the computed tables of class numbers and p-adic regulators with heuristic predictions.

5.1 Heuristics for the class number

Schoof [32] showed, based on a speculative extension of the Cohen–Lenstra heuristics [3], that the class numbers of real abelian fields of prime conductor are most likely relatively small. The same holds for prime power conductors; see Buhler et al. [2]. We see from Chapter 2 how to treat class groups of fields of any conductor. It would be natural to assume that the predictions given by Schoof on the size of the class groups hold in our case as well. We will show that this is indeed the case.

Cohen and Lenstra give conjectural heuristic assumptions on the properties of finite modules over direct products of Dedekind domains. In particular, the assumptions apply to the modules over the (unique) maximal order of the group ring $\mathbf{Q}[G]/\langle\sum_{\sigma\in G}\sigma\rangle$ with G abelian. Their examples include probabilities for properties of the class groups of quadratic fields and real abelian fields. The p-parts of the class groups with p dividing the degree had to be excluded; recently Wittmann [37] presented heuristics for such primes in some special cases.

To apply the heuristics, one should originally have a large collection of fields of varying conductor and fixed degree. Since our computations are limited to the fields of conductor at most 2000 and of varying degree, the situation is different. But as is mentioned in [2] and [32], the heuristics and the computed results *together* support the conjecture that the class groups of real abelian fields are usually very small.

We assume for the rest of the section that $p \nmid \#G$. The decomposition (2.7) allows us to define the p-class groups as modules over $\bigoplus_{\widetilde{\chi}\neq\widetilde{1}}\mathbf{Z}[\zeta_{g_\chi}]$; since $\mathrm{Cl}_{1,p} = 1$ for the trivial character $1 = \chi_0$, we may drop the corresponding part from the direct sum. Since the above sum is isomorphic to the maximal order of the group ring $\mathbf{Q}[G]/\langle\sum_{\sigma\in G}\sigma\rangle = \mathbf{Q}[G]/e_1\mathbf{Q}[G]$, the heuristics may be applied in our case.

For a finite module A over a Dedekind domain R, there is a decomposition $A = \bigoplus_{\mathcal{P}} A_{\mathcal{P}}$, where the sum is taken over the prime ideals $\mathcal{P}$ of R and $A_{\mathcal{P}} = \{a \in A \mid \mathrm{Ann}_R a \text{ is a power of } \mathcal{P}\}$ (see [6]). Only finitely many $A_{\mathcal{P}} \neq 0$. Now by [3, Example 5.10], assuming the heuristics, the probability that $A_{\mathcal{P}} = 0$ is equal to $\prod_{k=2}^{\infty}(1 - N\mathcal{P}^{-k})$, where the norm $N\mathcal{P} = \#(A/\mathcal{P})$. The probabilities for the different $\mathcal{P}$ will be assumed independent.

Let us show how to apply the above probability in our case. Note first that the prime ideals of $\bigoplus_{\widetilde{\chi}\neq\widetilde{1}}\mathbf{Z}[\zeta_{g_\chi}]$ are of the form $\bigoplus_{\widetilde{\chi}\neq\widetilde{1},\widetilde{\psi}}\mathbf{Z}[\zeta_{g_\chi}] \oplus \mathcal{P}$, where $\widetilde{\psi}$ is any nontrivial $\mathbf{Q}$-conjugacy class of characters and $\mathcal{P}$ runs through the prime ideals of $\mathbf{Z}[\zeta_{g_\psi}]$. Their norms are equal to the norms of $\mathcal{P}$. There are $\varphi(g_\chi)/f_p$ prime ideals of $\mathbf{Z}[\zeta_{g_\chi}]$ above any unramified prime p. Their common norm is p^{f_p}, where f_p is the order of p modulo g_χ. The number of different $\mathbf{Z}[\zeta_{g_\chi}]$ in the decomposition of the rational group ring of a real cyclotomic field is equal to the number of $\mathbf{Q}$-conjugacy classes. Their number might be calculated, for instance, by the following result by Perlis and Walker [31]: If G is a finite abelian group of order g, we have $\mathbf{Q}[G] \simeq \bigoplus_{d|g}\frac{n_d}{\varphi(d)}\mathbf{Q}(\zeta_d)$, where n_d is the number of elements of order d in G.

The probability that the class group is trivial (excluding the primes dividing $2g_\chi$) is therefore

$$P(\mathrm{Cl}=1) = \prod_{\widetilde{\chi}}\prod_{p\in\mathbf{P}'}\prod_{\mathcal{P}|p}P(\mathrm{Cl}_{\chi,\mathcal{P}}=1) = \prod_{\widetilde{\chi}}\prod_{p\in\mathbf{P}'}\Big(\prod_{k\geq 2}(1-p^{-f_pk})\Big)^{\varphi(g_\chi)/f_p},$$

where $\mathbf{P}'$ denotes the set of all prime numbers $p \nmid 2g_\chi$. Having computed all the p-parts of the class groups for $2 < p < 10000$, we assume $p > 10000$. Then by taking the logarithm and using the estimates

$$-\ln\left(1-\frac{1}{p^{f_pk}}\right) < \frac{1+10^{-8}}{p^{f_pk}} \quad (k\geq 2), \quad \sum_{k\geq 2}p^{-f_pk} = \frac{1}{p^{f_p}(p^{f_p}-1)} \leq \frac{1+10^{-4}}{p^{2f_p}},$$

we obtain

$$-\ln\big(P(\mathrm{Cl}_{\chi,p} = 1\,\forall\, p > 10^4)\big) < 1.00011\varphi(g_\chi)\sum_{p>10^4}\frac{1}{f_pp^{2f_p}}.$$

The series is dominated by the terms with $f_p = 1$, i.e., $p \equiv 1 \pmod{g_\chi}$; the remainder is smaller than $\sum_{p>10^4}p^{-4} < 10^{-13}$ (the estimate is computed via the "prime zeta function" (5.1)). By the prime number theorem for arithmetic progressions, the number of primes $p < n$ satisfying $p \equiv 1 \pmod{g_\chi}$

equals approximately $\#\{p \in \mathbf{P} \mid p < n\}/\varphi(g_\chi)$ for large n. Thus with many different g_χ we have, at least on average,

$$\sum_{p>10^4} \frac{1}{f_p p^{2f_p}} < 10^{-13} + \sum_{\substack{p>10^4 \\ p\equiv 1 \pmod{g_\chi}}} p^{-2} \approx \frac{1}{\varphi(g_\chi)} \sum_{p>10^4} p^{-2}.$$

We assumed that 10^{-13} is insignificant; this holds, when the numbers g_χ are of the magnitude we confronted in the computations. The series over primes may be approximated from its expression in terms of values $\zeta(m)$ of the Riemann zeta function, $m \geq 2$. Indeed, we have

$$\sum_{p\in\mathbf{P}} \frac{1}{p^m} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \ln \zeta(km) \tag{5.1}$$

as the Möbius inversion of the logarithm of the Euler product for $\zeta(m)$ (see, e.g., [4]). This gives $\sum_{p\in\mathbf{P}} p^{-2} \approx 0.452247$. Consequently, we obtain $\sum_{p<10^4} p^{-2} \approx 0.452238$. It follows that

$$P(\mathrm{Cl}_{\chi,p} = 1\,\forall\, p > 10^4) \approx 0.999990.$$

It is interesting to note that this estimate does not depend on g_χ.

We computed all the (χ, p)-parts of the class groups for $2 < p < 10000$, $p \nmid g_\chi$, $f_\chi \leq 2000$. For $f_\chi \leq 500$, we even went up to the bound $p < 100000$ utilizing Schwarz's tables [34]. For any fixed p, there are a total of 9339 different $\mathbf{Z}[\zeta_{g_\chi}]$-modules $\mathrm{Cl}_{\chi,p}$ for $500 < f_\chi \leq 2000$ (1679 for $f_\chi \leq 500$). When substituting this information in the above formulas, one obtains from the heuristics that the predicted number of occurrences of nontrivial class group parts $\mathrm{Cl}_{\chi,p}$ (dropping out from the study all the primes dividing $2g_\chi$) for the fields of conductor $f_\chi \leq 2000$ would be approximately 443, and that the class number would not contain larger primes for $500 < f_\chi \leq 2000$ with probability $\approx 91\%$ (for $f_\chi \leq 500$ with $\approx 99\%$). We might exclude from the calculation all the class group parts corresponding to the fields of small degree since there exist extensive tables for them; then the above probability for $500 < f_\chi \leq 2000$ rises to at least 93%. Given that all the computations have produced only relatively small prime divisors compared to the degree of the field, we find it reasonable to believe that the found class number divisors are, in fact, all the primes dividing h_χ for any $f_\chi \leq 2000$, excluding the primes dividing $2g_\chi$.

We found 231 nontrivial χ-parts of class groups, which is less than the expected number 443, but which is still of the same order of magnitude when compared to the number of all the χ-parts. This supports the belief, stated by Schoof [32], that the heuristics would slightly overestimate the chance of a nontrivial class group when the conductor is relatively small.

5.2 Heuristics for the p-adic regulator

We recall that to check whether $v_p(h_K R_p(K)/p^{g-1}) > 0$, Schwarz introduced the condition (3.10), where one checks if a given cyclotomic polynomial is relatively prime modulo p to the polynomial $\sum_i a_i x^{\lambda(i)}$. By assuming the coefficients of this polynomial random and calculating the probability for (3.10) to hold, Schwarz presented heuristics that correspond quite well to his computed results.

When generalizing this condition to higher p-powers (see Section 3.2), we saw that one is led to a condition involving a norm of a character sum corresponding to $L_p(1,\chi)$ modulo p^k. Indeed, we restricted the study to a single $\mathbf{Q}$-conjugacy class of characters at a time and checked if

$$p^k \mid \prod_{\psi\in\widetilde{\chi}} \sum_{j=1}^{\varphi(f_\chi)/2-1} d_j \psi(j) \tag{5.2}$$

holds for some $k \geq 1$. This product equals the norm of a sum of g_χth roots of unity.

Let us assume that this sum $\sum_{i\leq g_\chi} c_i \zeta_{g_\chi}^i \in \mathbf{Z}[\zeta_{g_\chi}]$ is random. If $\mathcal{P}$ is any prime ideal of $\mathbf{Z}[\zeta_{g_\chi}]$ above p and we suppose the residue of the sum modulo $\mathcal{P}^k$ to be random, the probability that this residue is zero is $1/N(\mathcal{P}^k) = p^{-f_p k}$, where f_p is the residue class degree. If we also assume that the probabilities for different $\mathcal{P}$ above p are independent, then the probability that the residue is nonzero for all prime ideals above p is equal to $(1-p^{-f_p k})^{\varphi(g_\chi)/f_p}$. Since the residue may be zero for many different prime ideals above p, we continue as follows.

Let $\mathcal{P}_i$, $i = 1,\ldots,n$ with $n = \varphi(g_\chi)/f_p$, be the prime ideals above p and denote by $v_{\mathcal{P}_i}$ the function that counts the multiplicity of the occurrence of $\mathcal{P}_i$ in the prime decomposition of the sum $\sum_{i\leq g_\chi} c_i \zeta_{g_\chi}^i$. For a random $\alpha \in \mathbf{Z}[\zeta_{g_\chi}]$ and for any i and $k \geq 0$, we have

$$P(v_{\mathcal{P}_i}(\alpha)=k) = P(v_{\mathcal{P}_i}(\alpha)\geq k)P(v_{\mathcal{P}_i}(\alpha)<k+1 \mid v_{\mathcal{P}_i}(\alpha)\geq k) = p^{-f_p k}(1-p^{-f_p}).$$

Hence, for instance (defining $\binom{n}{i} = 0$ for $n < i$),

$$\begin{aligned} P\Big(\sum_{i=1}^{n} v_{\mathcal{P}_i}(\alpha) = 3\Big) &= nP\big(v_{\mathcal{P}_i}(\alpha) = 3,\ v_{\mathcal{P}_j}(\alpha) = 0\ \forall\ j \neq i\big) \\ &+ \tbinom{n}{2}P\big(v_{\mathcal{P}_i}(\alpha) = 2,\ v_{\mathcal{P}_j}(\alpha) = 1,\ v_{\mathcal{P}_k}(\alpha) = 0\ \forall\ k \neq i,j\big) \\ &+ \tbinom{n}{3}P\big(v_{\mathcal{P}_i}(\alpha) = v_{\mathcal{P}_j}(\alpha) = v_{\mathcal{P}_k}(\alpha) = 1,\ v_{\mathcal{P}_\ell}(\alpha) = 0\ \forall\ \ell \neq i,j,k\big) \\ &= (1-p^{-f_p})^n p^{-3f_p}\Big(\tbinom{n}{1} + 2\tbinom{n}{2} + \tbinom{n}{3}\Big). \end{aligned}$$

This shows that the probability for (5.2) to hold in the case $k = 4$ would be equal to

$$P\Big(\sum_i^n v_{\mathcal{P}_i}(\alpha) \geq 4\Big) = 1 - \sum_{j=0}^{3} P\Big(\sum_i^n v_{\mathcal{P}_i}(\alpha) = j\Big)$$
$$= 1 - \big(1 - p^{-f_p}\big)^n \big(1 + np^{-f_p} + \big(n + \tbinom{n}{2}\big)p^{-2f_p} + \big(n + 2\tbinom{n}{2} + \tbinom{n}{3}\big)p^{-3f_p}\big).$$

All the probabilities are deduced similarly; we only needed the cases $k \leq 6$ (for $g_\chi > 2$ only the cases $k \leq 4$) in the computations. We computed for all the primes $p < 100$, $p \nmid 2g_\chi$, a table of probabilities for (5.2) to hold for any of the above k and for any $\mathbf{Q}$-conjugacy class of characters (see Tables 1 and 2 in Chapter 8).

It can be seen from Tables 4 and 5 that different $\mathbf{Q}$-conjugacy classes with $p \mid g_\chi$ seem to be dependent, hence we dropped them from this heuristic study. In fact, Schwarz proved the following result (see [34, p. 40]) which in many cases describes such a dependence. For any field K of degree $p^\mu, p \nmid \mu$, and of conductor f not divisible by p, denote by $G(p)$ and H respectively the p-primary subgroup of G and the group of elements of G of order prime to p and by L and $K(p)$ their fixed fields. Then $v_p(h_K R_p^{'}(K)) = 0$ if and only if the following four conditions are satisfied: $v_p(h_L R_p^{'}(L)) = 0$, $K(p)$ has prime power conductor ℓ^ν with $\ell \neq p$, $\ell \not\equiv 1 \pmod{p^2}$ and ℓ does not split in L. We note that with minor changes a similar result would hold when restricted to $\mathbf{Q}$-conjugacy classes, but a generalization to higher p-powers such as in Section 3.2 is not straightforward (if at all possible).

Chapter 6

Other methods

We will briefly survey some other recent methods for checking the p-divisibility of the class numbers of real abelian fields. We will leave out the technical details involved in the methods and rather study the basic ideas. It is interesting to compare them with the techniques introduced in this work; in particular, it would probably be possible to generalize the methods limited to prime power conductors.

6.1 A connection with Yoshino's method

Let q be an odd prime. Yoshino investigates in his work [39] prime divisors of the class numbers of $\mathbf{Q}(\zeta_q + \zeta_q^{-1})$ and its subfields. The method is restricted to prime conductors (generalized to prime powers in [16]), but probably one could use Leopoldt's results to extend them to composite conductors.

Yoshino first gives a necessary condition for an odd prime $p \neq q$ to divide the class number h_K of $K = \mathbf{Q}(\zeta_q + \zeta_q^{-1})$ (he also has results concerning the prime 2). This condition is checked in practice by computing the $\mathbf{F}_p$-rank of a certain matrix. He also shows a reduction method that allows dealing with class numbers of subfields of K and finally finds a condition that is sufficient for the class number divisibility.

The idea is to investigate the group of units of K modulo an explicitly given subgroup of full rank. Yoshino lets this group be Hasse's cyclotomic units C_K. Since q is a prime, this group has a simple structure and is of index h_K in E_K by a well-known theorem [36, Thm. 8.2].

We give the definition of C_K (one should compare this with the definition of F_K in Section 2.6). First fix a primitive root r modulo q. The group C_K is a cyclic $\mathbf{Z}[G]$-module generated by $e_0 = (\zeta - \zeta^{-1})^{\sigma - 1}$, where $\zeta_q = \zeta$ and $\sigma : \zeta \mapsto \zeta^r$ is a generator of $G = \mathrm{Gal}(K/\mathbf{Q}) \simeq (\mathbf{Z}/q\mathbf{Z})^\times/\{\pm 1\}$. As a $\mathbf{Z}$-module, C_K is generated by the elements -1 and $e_i = e_0^{\sigma^i}, i = 0, \dots, n-1$ with $n = (q-1)/2$. One may prove (see [36]) that $\prod_{i=0}^{n-1} e_i = -1$ is the only nontrivial relation between the e_i, hence exactly $n-1$ of the e_i are independent.

The rank computations were later in [16] replaced by more efficient polynomial computations. This amounts to checking whether a certain polynomial is nontrivial. The polynomial is obtained by polynomial gcd computations very similar to what was done by Schwarz, i.e., similar to the first step in our algorithm. If the polynomial is found to be nontrivial, one computes its factorization in $\mathbf{Z}[x]$ and checks by a congruence condition if any factors are irrelevant for the class number divisibility. The calculations resemble our second step. If the polynomial obtained in the second step is still nontrivial, then the class number divisibility is finally verified using a technique corresponding to our third step.

We will show that there really is a connection between these methods. For simplicity, we do not deal with the subfields of K, but by following the reduction method in [16], one should be able to generalize the correspondence of the methods accordingly. We begin by presenting some definitions and results given in [39]. Let

$$E_U^{(p)} = \{\eta \in C_K \mid \alpha^p \equiv \eta \pmod{p^2} \text{ for some integer } \alpha \in K\}.$$

This group is called the *primary units*; the notion originally stems from the classical work of Kummer. Intuitively, the elements of $E_U^{(p)}$ are those cyclotomic units that have a possibility to be pth powers of units in view of the beginning of their p-adic expansions. If p divides the class number h_K, then p also divides $\#(E_U^{(p)}/C_K^p)$; indeed, then there exists a unit $\varepsilon \in E_K \setminus C_K$ such that $\varepsilon^p \in C_K$, and we see that $\varepsilon^p C_K^p$ generates a cyclic subgroup of order p in $E_U^{(p)}/C_K^p$.

Define $\alpha \in \mathbf{Z}[\zeta]$ such that $(\zeta - \zeta^{-1})^p = \zeta^p - \zeta^{-p} + p\alpha$ and let

$$\beta = -\frac{\alpha}{(\zeta-\zeta^{-1})^p} + \frac{(\zeta^p - \zeta^{-p})\alpha^\sigma}{(\zeta-\zeta^{-1})^p(\zeta^{pr} - \zeta^{-pr})} \in K.$$

These elements are used to prove the following equivalence; see [39] for its simple proof. If $\xi = \prod_{i=0}^{n-1} e_i^{x_i}$ is any cyclotomic unit, then

$$\xi \in E_U^{(p)} \Longleftrightarrow \sum_{j=0}^{n-1} x_j \beta^{\sigma^j} \equiv 0 \pmod{p}. \tag{6.1}$$

Note that the congruence can be understood p-adically; the elements involved are p-integral.

By a result of Kummer on the rationality of a certain sum of roots of unity, the congruence condition in (6.1) implies rational congruences $\sum_{j=0}^{n-1} x_j c_{i,j} \equiv 0 \pmod{p}$ for every $0 \le i \le n-1$ (see [39]). This may be written as

$$M(x_0, \ldots, x_{n-1})^T \equiv \mathbf{0} \pmod{p}$$

with $M = (c_{i,j})_{0\le i,j\le n-1}$. The dimension of its solution space $\mathcal{M}$ equals n subtracted by the $\mathbf{F}_p$-rank of M. Let $\mathcal{N} = \{(a,\dots,a) \mid a \in \mathbf{F}_p\}$. It is now easy to see that $\mathcal{M}/\mathcal{N}$ contains a subgroup isomorphic to $E_U^{(p)}/C_K^p$. Hence it suffices first to analyze the more explicitly given group $\mathcal{M}/\mathcal{N}$ in order to study class number divisibility.

Now we will show that when proceeding differently from (6.1), we arrive at a condition similar to the first step of our method. We begin with a lemma.

Lemma 6.1. *Let $p \neq q$. The p-adic regulator of C_K equals*

$$R_p(C_K) = \pm \det\big(\log_p(1-\zeta^{2pr^{i+j+1}}) - \log_p(1-\zeta^{2pr^{i+j}})\big),$$

where $0 \le i,j \le n-1$ and we omit one freely chosen value for both i and j.

Proof. The elements

$$\xi_i = \frac{(\zeta^{-1/2}(1-\zeta))^{\sigma^{i+1}}}{(\zeta^{-1/2}(1-\zeta))^{\sigma^i}} \quad (i = 0,\dots,n-2)$$

with -1 also generate C_K as a $\mathbf{Z}$-module (see [36, Lemma 8.1]). By the definition, $R_p(C_K) = \det(\log_p(\xi_i^{\tau_j}))_{0\le i,j\le n-2}$ modulo sign, where τ_j runs through all but one (freely chosen) element of G. Since this is independent of the choice of basis, we may substitute ζ by ζ^{2p} in the definition of ξ_i. By noting that $\log_p(\zeta) = 0$, we write

$$R_p(C_K) = \pm \det\big(\log_p((1-\zeta^{2p})^{\sigma^{i+j+1}}) - \log_p((1-\zeta^{2p})^{\sigma^{i+j}})\big),$$

where $0 \le i,j \le n-2$. Since the rows in the determinant are different permutations of $\log_p(\xi_i)$ modulo sign (recall that $\prod \xi_i = -1$), we may express $R_p(C_K)$ as above, omitting one freely chosen value for both i and j. $\square$

Proposition 6.1. *Let $K = \mathbf{Q}(\zeta_q + \zeta_q^{-1})$ and $p \neq q$. Then*

$$p \mid \#(E_U^{(p)}/C_K^p) \Longleftrightarrow v_p(h_K R_p(K)/p^n) > 0.$$

Proof. We first note that $\alpha = \lambda(\zeta^2)(\zeta^p - \zeta^{-p})$, where λ is defined in (3.9). By using the congruence $\zeta^p - \zeta^{-p} \equiv (\zeta - \zeta^{-1})^p \pmod p$, we obtain from this $\beta \equiv \lambda(\zeta^2)^\sigma - \lambda(\zeta^2) \pmod p$.

The proof of (3.8) rests essentially on the fact that $-\frac{1}{p}\log_p(1-\zeta^{ap}) \equiv \lambda(\zeta^a) \pmod p$ for every a prime to q (see [23]). We obtain

$$\beta \equiv -\frac{1}{p}\big(\log_p(1-\zeta^{2pr}) - \log_p(1-\zeta^{2p})\big) \pmod p. \tag{6.2}$$

Our observation is that the condition in (6.1) is invariant under σ-operation, i.e.,

$$\xi \in E_U^{(p)} \Longleftrightarrow \sum_{j=0}^{n-1} x_j \beta^{\sigma^{i+j}} \equiv 0 \pmod{p} \text{ for any } 0 \leq i \leq n-1.$$

The right hand side is equivalent to the condition $M_1(x_0, \ldots, x_{n-1})^T \equiv \mathbf{0} \pmod{p}$, where $M_1 = (\beta^{\sigma^{i+j}})_{0 \leq i,j \leq n-1}$ (with $\sigma^n = 1$). Denote by $\mathcal{M}_1$ its solution space. We have $\mathcal{N} \subseteq \mathcal{M}_1$ by (6.2). The $\mathbf{F}_p$-dimension of $\mathcal{M}_1/\mathcal{N}$ then equals $n - 1 - \mathrm{rank}_{\mathbf{F}_p} M_1$. By elementary linear algebra, the rank of M_1 equals s if all the $(s+1)$-minors of M_1 are equal to zero, but an s-minor is nonzero. But any $(n-1)$-minor of M_1 equals $R_p(C_K)/p^n$ modulo p by Lemma 6.1. Finally, by the p-adic version of (2.2) (see [36, p. 153]), $R_p(C_K)$ equals $h_K R_p(K)$. □

Remark 6.1. The group $\mathcal{M}_1/\mathcal{N}$ is a subgroup of $\mathcal{M}/\mathcal{N}$. However, the computations we carried out using Yoshino's criterion and Schwarz's method suggest that, in fact, the condition $\dim_{\mathbf{F}_p} \mathcal{M}/\mathcal{N} > 0$ would be equivalent to $v_p(h_K R_p(K)/p^n) > 0$, hence $E_U^{(p)}/C_K^p \simeq \mathcal{M}/\mathcal{N}$.

6.2 p-Adic methods

We noted in Chapter 2 that one may as well decompose the p-class group by means of the rational p-adic characters. This decomposition also corresponds to the p-adic decomposition of the unit group modulo cyclotomic units. Indeed, let χ be a nontrivial character of an abelian field K and let K_χ be the fixed field of $\mathrm{Ker}(\chi)$ as before. Let p be a prime not dividing g_χ and $\mathrm{Cl}_{\chi,p} = \mathrm{Cl}_p^{e_{\widetilde{\chi}}}$, where Cl_p is the p-class group of K and $e_{\widetilde{\chi}}$ is the idempotent corresponding to the rational p-adic character $\widehat{\chi} = \mathrm{Tr}_{\mathbf{Q}_p(\zeta_{g_\chi})/\mathbf{Q}_p}(\chi)$. Define $E_{\chi,p} = (E \otimes_{\mathbf{Z}} \mathbf{Z}_p)^{e_{\widetilde{\chi}}}$ and let $F_{\chi,p}$ be a $\mathbf{Z}_p[\zeta_{g_\chi}]$-module generated by $N_{\mathbf{Q}(\zeta_{f_\chi})/K_\chi}(\zeta_{f_\chi} - 1)^{e_{\widetilde{\chi}}}$.

As a consequence of Iwasawa's Main Conjecture (proved by Mazur and Wiles [22]), the equality $\# \mathrm{Cl}_{\chi,p} = \#(E_{\chi,p}/F_{\chi,p})$ follows. This allows to design criterions for the p-divisibility of the class number in a similar manner as was done in our work; additional work has to be done in appropriate truncation of the p-adic elements involved. Since the p-adic decomposition of the class group is a refinement of the rational decomposition, one would hope to obtain more precise results.

One such method is given by Schoof [32]. He only studied the fields of prime conductor for simplicity. The Gras conjecture, i.e., that the Jordan–Hölder filtrations of the class group of $K = \mathbf{Q}(\zeta+\zeta^{-1})$ and the group E_K/C_K are isomorphic as $\mathbf{Z}_p[G]$-modules, is also a consequence of the Main Conjecture (see [12, Proposition 9]). Schoof's idea was to compute all the simple

Jordan–Hölder factors of the p-part of a module isomorphic to E_K/C_K. The underlying idea is similar; indeed, the Jordan–Hölder filtration of the unit group corresponds to the decomposition into simple modules $E_{\chi,p}$.

Another p-adic method is introduced in a recent article of Aoki and Fukuda [1]. They not only give means to check the p-divisibility of the class number, but also present a technique to compute the structure of the p-class group. This is based on a result of Kolyvagin–Rubin–Thaine that gives explicitly the annihilators of some specific ideals of K.

Chapter 7

Conclusion and open problems

In this thesis we have examined the computation of the class numbers of real abelian fields. We constructed an efficient algorithm to compute class number divisors. The computed results predict that the size of the class numbers shows statistical behaviour similar to the class numbers of fields of prime conductor.

For abelian extensions over imaginary quadratic fields, there exists an explicitly given group of units constructed using elliptic functions. These units have properties analogous to cyclotomic units and they have been applied in some works concerning the computation of the class numbers of such fields. In particular, there exist class number formulae for these fields; for instance, K. Nakamula [25] has constructed algorithms to compute the class numbers of some sextic fields. It would be interesting to study these fields in connection with our methods.

We mainly ignored the question of checking the class number divisibility for the primes p dividing the degree g of the field. There exists the well-known theorem from class field theory [36, Thm. 10.4] that if L/K is a Galois extension of degree a power of p such that at most one prime ramifies, then $p \mid h_L$ implies $p \mid h_K$. The conditions hold if such a field L is real and of prime power conductor. In Schoof's table [32] of class number divisors this means that p does not divide the class number of any such field unless p divides the class number of a subfield of degree not divisible by p. But in the case of a composite conductor this result is not applicable in general, and one may not hope for a simple generalization to the case where more than one prime ramify.

When approaching this question from Leopoldt's point of view, the difficulty would be to compute the index $Q_K^+ = [E_K : E_+^K]$. In some simplest special cases Q_K^+ is known, but in general its computation is hard. In principle this is possible since we explicitly know the $g-1$ elements (i.e., the cyclotomic units) that form a $\mathbf{Z}$-basis of F_K, we know how to check the divisibility of the h_χ and we also know (by the relation $Q_K \mid Q_G$) all the possible prime divisors of Q_K^+. Indeed, to check whether p divides Q_K^+, we first compute the p-exponent of $\prod_{\widetilde{\chi}} h_\chi = [E_+^K : F_K]$ using the method in Chapter 4 and obtain explicitly a module $F_K^{'}$ for which $[E_+^K : F_K^{'}]$ is prime to p. Then it suffices to check if any element of $F_K^{'}$ is a pth power in $E_K \backslash F_K^{'}$; we may use one of the methods given in Section 4.3. The number of tests is $(p^{g-1}-1)/(p-1)$ since we may reduce modulo pth powers, i.e., reduce the coefficients modulo p in the basis representation. If some element satisfies the condition, we add this element to the basis of $F_K^{'}$ and obtain a set of generators of a subgroup of index Q_K^+/p in E_K. This allows us to write any element of this subgroup as a linear combination of the generators, hence it suffices to do at most $(p^g-1)/(p-1)$ tests to check if $p^2 \mid Q_K^+$. These computations were not performed since the number of tests would be very large. Moreover, it would probably be necessary to compute the index Q_K^+ separately for each field, and one cannot use any cyclicity arguments in order to restrict the number of elements to be tested (cf. Section 4.2).

Chapter 8

Tables

In the first table we present all the prime divisors $p < 10000$ of the class numbers of the real abelian fields of composite conductor $500 < f \leq 2000$ and the prime divisors $p < 100000$ for $f \leq 500$, excluding the prime 2 and the primes dividing the degree of the field. The first column indicates the conductor f_χ of K_χ. A character defining the field K_χ is written in the second column. The representatives of the $\mathbf{Q}$-conjugacy classes of characters were chosen as in [34].

The third column gives the degree g_χ of K_χ and the last column shows the prime divisor p of the χ-class number h_χ. We did not encounter any h_χ having more than one prime divisor. The occasional exponent of p is the residue class degree of p modulo g_χ, except for one case. This is a field of conductor 1921 for which we found two different submodules containing 17th powers. The search for higher p-powers showed that the class number is exactly divisible by 17^3. We computed, using PARI [30], that the 17-class group is of type $\mathbf{Z}/17^2\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}$. Note that 17 divides 1921. In general, the case where p divides the conductor seems to occur very often; indeed, 54 of the 182 entries of the table are of this form, including the two largest class number divisors found. For the fields of prime power conductor, recall that Vandiver's conjecture (verified up to a very large conductor) states that such primes never divide the class numbers.

For any real field K of conductor f, one may read the p-part of h_K for any $p < 10000$, $p \nmid 2[K : \mathbf{Q}]$, by combining the entries of the table (together with Schoof's table of the fields of prime conductor in [32]) for all cyclic subfields K_χ of K of conductor $f_\chi \mid f$. The p-class structure is given by (2.7).

For example, take the field $K = \mathbf{Q}(\zeta_f + \zeta_f^{-1})$ with $f = 1304 = 8 \cdot 163$. Our table gives for h_K twice the prime factor 19 coming from the fields with conductor f and $f/2 = 652$ (both of degree 18). By (2.7), the 19-class group is of type $\mathbf{Z}/19\mathbf{Z} \times \mathbf{Z}/19\mathbf{Z}$. In addition, there is a prime factor

3 coming from a quadratic subfield with conductor f. Since 3 divides the degree $324 = 4 \cdot 81$ of K, the 3-class group of K remains unknown; in fact, it could be possible that $3 \nmid h_K$. Since the class number of $\mathbf{Q}(\zeta_8 + \zeta_8^{-1})$ is 1 and that of $\mathbf{Q}(\zeta_{163} + \zeta_{163}^{-1})$ is 4 (see [20]), we find that all the other possible odd prime factors of h_K must be larger than 10000.

The results in Table 1 were checked to agree with the tables of real cyclic fields of degree at most 6 (cf. [27], [7], [8], [15], [24]). All the class number divisors of the fields of degree at most 20 were also confirmed with PARI. The results in the case of a prime conductor (omitted from this table since they are found in the other tables for $p \neq 2$) were found to agree with the tables of Schoof [32] and Koyama and Yoshino [16].

Tables 2 and 3 contain the results of the heuristic computation described in Section 5.2. For comparison, we also gathered the corresponding data from Table 4. The instances in Table 4 with v_p equal to $k > 1$ are included in these tables for any $k, k-1, \ldots, 1$. Table 2 contains all the instances with $p \equiv 1 \pmod{g_\chi}$ and Table 3 all the others. In Table 3 we assume $k = 1$ unless otherwise stated. In the column "found" we combined all the instances in Table 4 with g_χ dividing $p^{f_p} - 1$. In the column "exp" we computed a weighted probability for (5.2) to hold for fixed p and k. For example, let $p = 11$, $f_p = 1$ and $k = 1$. There are in total 255 different $\mathbf{Q}$-conjugacy classes of characters of conductor $f_\chi \leq 2000$ of order $g_\chi \mid p-1$, of which 147 are with $g_\chi = 2$, 73 with $g_\chi = 5$ and 35 with $g_\chi = 10$. Table 4 shows that p divides the product of the L_p-functions in 41 instances, hence the value in "found" is $41/255 \approx 0.161$. The value in "exp" is equal to $(147 \cdot 0.091 + 73 \cdot 0.317 + 35 \cdot 0.317)/255 \approx 0.187$.

This prediction corresponds quite well to the actual results, at least on average. Schwarz also found this in the case $k = 1$ by a heuristic principle equivalent to ours. However, note that in the tables one can find many examples of $\mathbf{Q}$-conjugacy classes of common conductor for which some p seems to occur unexpectedly often; hence it may be too simplistic to assume the $\mathbf{Q}$-conjugacy classes independent. It also seems that the nontrivial p-divisibility of the p-adic regulator occurs slightly more often in the cases where the class number is divisible by p; but note that the amount of such data is very small in our tables.

The computations of the p-adic regulators were not extended to the case of a composite conductor, but it would be natural to assume that the statistics would show a similar behaviour.

Table 4 shows for any odd prime conductor $f = f_\chi < 2000$ all the odd prime numbers $p < 100$, $p \nmid f$, and the representatives of the $\mathbf{Q}$-conjugacy classes of characters $\widetilde{\chi}$ of $\mathbf{Q}(\zeta_f + \zeta_f^{-1})$ for which $v_p(\prod_{\chi \in \widetilde{\chi}} L_p(1,\chi)) > 0$. This condition was checked using (3.10). In addition, we list the exact v_p-values in all these cases, obtained using the condition (3.5). For any real field K of prime conductor f and degree g, the p-adic exponential value of

$h_K R_p(K)/p^{g-1}$ can be read from the table by summing up all the values that correspond to the **Q**-conjugacy classes of characters of K. For clarity, we also list the degree g_χ of K_χ so that the summation would be simpler for a given field K. Indeed, sum up all the v_p-values for which g_χ divides the degree of K.

For a prime p, there may be several different conjugacy classes satisfying the condition in (3.10); they are separated by a comma in the table. If the line corresponding to some conductor is empty, there are no conjugacy classes of this conductor satisfying the condition (3.10) for any $2 < p < 100$. If there is the symbol $+^s$ for some $s \in \mathbf{N}$ (or simply $+$, meaning $+^1$) in the table, it indicates that $p^s \,|\, h_{K_\chi}$ by Schoof's table (to compute the p-part of the class number of K_χ, sum up also the p-divisors coming from the subfields). The asterisk $*$ in turn indicates that K_χ belongs to the family in which the fundamental units are known (see Section 3.4), thus the p-adic regulator may be computed independently of the class number. The bounds 2000 and 100 for f and p were arbitrarily chosen.

For example, let K be the real abelian field of conductor 1483 and degree 39. We may read from the table that

$$v_p(h_K R_p(K)/p^{g-1}) = \begin{cases} 0 & \text{for } p = 3, \\ 2 & \text{for } p = 5, \\ 1 & \text{for } p = 7, \\ 1+2=3 & \text{for } p = 13, \\ 1 & \text{for } p = 79, \\ 0 & \text{for other } 2 < p < 100. \end{cases} \tag{8.1}$$

Since 13 divides the degree, but does not divide the class number of the subfield of K of degree 3, it follows from [36, Thm. 10.4] that $13 \nmid h_K$ (cf. Chapter 7). Moreover, we know from the tables and Remark 3.3 that $3 \nmid h_K$. Since there are no symbols $+$ for these entries in the table, the other primes in (8.1) do not divide the class number either. Hence all the above values are v_p-values of the corresponding p-adic regulators.

Table 5 gives $h_K R_p(K)/p^{g-1}$ for those odd primes p that are class number divisors for some field of prime conductor $f < 10000$ by Schoof's table [32]. We have omitted the primes for which the information is already found in Table 4. For example, choose $f_\chi = 4993$. The prime 5 divides the class number of the field of degree 4 by Schoof's table; this is indicated by $+$. For the fields of degrees 2 and 24, the v_5-values in the table come from the 5-adic regulator. For the latter field, recall that the value must be divisible by 2 since it is the residue class degree of 5 modulo 24.

Table 1. The computed prime divisors of class numbers.

f_χ	χ	g_χ	p
212	$\omega_4^1\chi_{53}^{13}$	4	5
316	$\omega_4^1\chi_{79}^{39}$	2	3
321	$\chi_3^1\chi_{107}^{53}$	2	3
427	$\chi_7^3\chi_{61}^{15}$	4	5
469	$\chi_7^3\chi_{67}^{33}$	2	3
473	$\chi_{11}^5\chi_{43}^{21}$	2	3
481	$\chi_{13}^2\chi_{37}^4$	18	19
551	$\chi_{19}^9\chi_{29}^7$	4	5
556	$\omega_4^1\chi_{139}^{23}$	6	7
568	$\chi_8^1\chi_{71}^{14}$	10	11
	$\omega_4^1\chi_8^1\chi_{71}^{35}$	2	3
629	$\chi_{17}^8\chi_{37}^2$	18	19
	$\chi_{17}^4\chi_{37}^{18}$	4	5
651	$\chi_3^1\chi_7^3\chi_{31}^6$	10	11
652	$\omega_4^1\chi_{163}^9$	18	19
676	$\omega_4^1\chi_{169}^3$	52	53
692	$\omega_4^1\chi_{173}^{43}$	4	5
697	$\chi_{17}^8\chi_{41}^{20}$	2	3
703	$\chi_{19}^9\chi_{37}^1$	36	37
	$\chi_{19}^3\chi_{37}^9$	12	13
728	$\chi_8^1\chi_7^3\chi_{13}^3$	4	5
753	$\chi_3^1\chi_{251}^{25}$	10	11
756	$\omega_4^1\chi_{27}^2\chi_7^1$	18	19
763	$\chi_7^3\chi_{109}^9$	12	13
779	$\chi_{19}^9\chi_{41}^1$	40	41
785	$\chi_5^2\chi_{157}^{78}$	2	3
793	$\chi_{13}^1\chi_{61}^{55}$	12	37
808	$\omega_4^1\chi_8^1\chi_{101}^{25}$	4	5
817	$\chi_{19}^9\chi_{43}^{21}$	2	5
819	$\chi_9^1\chi_7^1\chi_{13}^2$	6	7
832	$\omega_4^1\chi_{64}^1\chi_{13}^3$	16	7^2
869	$\chi_{11}^5\chi_{79}^1$	78	79
889	$\chi_7^3\chi_{127}^{21}$	6	7
892	$\omega_4^1\chi_{223}^{111}$	2	3
916	$\omega_4^1\chi_{229}^{57}$	4	5
923	$\chi_{13}^3\chi_{71}^7$	20	61
928	$\omega_4^1\chi_{32}^1\chi_{29}^7$	8	17
935	$\chi_5^1\chi_{11}^5\chi_{17}^4$	4	5
940	$\omega_4^1\chi_5^2\chi_{47}^{23}$	2	3
944	$\omega_4^1\chi_{16}^1\chi_{59}^{29}$	4	5
976	$\omega_4^1\chi_{16}^1\chi_{61}^{15}$	4	5
980	$\omega_4^1\chi_5^1\chi_{49}^6$	28	29
985	$\chi_5^2\chi_{197}^{98}$	2	3
988	$\omega_4^1\chi_{13}^2\chi_{19}^3$	6	7
993	$\chi_3^1\chi_{331}^{165}$	2	3
999	$\chi_{27}^2\chi_{37}^{16}$	9	37

f_χ	χ	g_χ	p
1016	$\omega_4^1\chi_8^1\chi_{127}^{63}$	2	3
1025	$\chi_{25}^1\chi_{41}^7$	40	41
1036	$\omega_4^1\chi_7^2\chi_{37}^5$	36	73
1048	$\chi_8^1\chi_{131}^{26}$	10	11
1080	$\chi_8^1\chi_{27}^1\chi_5^1$	36	37
1101	$\chi_3^1\chi_{367}^{183}$	2	3
1105	$\chi_5^1\chi_{13}^9\chi_{17}^8$	4	5
1113	$\chi_3^1\chi_7^2\chi_{53}^{13}$	12	13
1116	$\omega_4^1\chi_9^2\chi_{31}^{25}$	6	7
1132	$\omega_4^1\chi_{283}^{47}$	6	7
1139	$\chi_{17}^2\chi_{67}^6$	88	89
1141	$\chi_7^2\chi_{163}^{36}$	9	19
1159	$\chi_{19}^2\chi_{61}^{10}$	18	73
1172	$\omega_4^1\chi_{293}^{73}$	4	13
1197	$\chi_9^2\chi_7^5\chi_{19}^{15}$	6	7
1207	$\chi_{17}^1\chi_{71}^{35}$	16	17
1211	$\chi_7^2\chi_{173}^{86}$	6	7
1235	$\chi_5^1\chi_{13}^4\chi_{19}^{15}$	12	13
	$\chi_5^2\chi_{13}^3\chi_{19}^9$	4	5
1241	$\chi_{17}^4\chi_{73}^{18}$	4	5
1243	$\chi_{11}^2\chi_{113}^{14}$	40	41
1257	$\chi_3^1\chi_{419}^{209}$	2	3
1261	$\chi_{13}^2\chi_{97}^{10}$	48	97
	$\chi_{13}^2\chi_{97}^{64}$	6	7
	$\chi_{13}^6\chi_{97}^{24}$	4	5
	$\chi_{13}^4\chi_{97}^{64}$	3	7
1271	$\chi_{31}^2\chi_{41}^{24}$	15	31
	$\chi_{31}^{10}\chi_{41}^{20}$	6	7
	$\chi_{31}^6\chi_{41}^{24}$	5	11
1287	$\chi_9^1\chi_{11}^2\chi_{13}^3$	60	61
1295	$\chi_5^2\chi_7^2\chi_{37}^{10}$	18	19
1304	$\chi_8^1\chi_{163}^{18}$	18	19
	$\omega_4^1\chi_8^1\chi_{163}^{81}$	2	3
1308	$\omega_4^1\chi_3^1\chi_{109}^{18}$	6	7
1311	$\chi_3^1\chi_{19}^2\chi_{23}^{11}$	18	19
1313	$\chi_{13}^6\chi_{101}^{20}$	10	31
1332	$\omega_4^1\chi_9^1\chi_{37}^6$	6	7
1339	$\chi_{13}^3\chi_{103}^{17}$	12	13
1343	$\chi_{17}^1\chi_{79}^{39}$	16	17
1345	$\chi_5^2\chi_{269}^{134}$	2	3
1353	$\chi_3^1\chi_{11}^1\chi_{41}^{12}$	10	11
1355	$\chi_5^2\chi_{271}^{30}$	18	37
1359	$\chi_9^1\chi_{151}^{125}$	6	7
1360	$\omega_4^1\chi_{16}^1\chi_5^1\chi_{17}^{12}$	4	5
1376	$\omega_4^1\chi_{32}^1\chi_{43}^7$	24	5^2
1384	$\chi_8^1\chi_{173}^{86}$	2	3

f_χ	χ	g_χ	p
1385	$\chi_5^2\chi_{277}^{46}$	6	7
	$\chi_5^1\chi_{277}^{207}$	4	5
1387	$\chi_{19}^2\chi_{73}^{18}$	36	17^2
	$\chi_{19}^2\chi_{73}^{22}$	36	37
	$\chi_{19}^2\chi_{73}^{8}$	9	19
1393	$\chi_7^3\chi_{199}^{99}$	2	5
1404	$\omega_4^1\chi_{27}^1\chi_{13}^8$	18	19
1407	$\chi_3^1\chi_7^3\chi_{67}^6$	22	23
1420	$\omega_4^1\chi_5^2\chi_{71}^7$	10	11
1421	$\chi_{49}^3\chi_{29}^{11}$	28	29
1424	$\omega_4^1\chi_{16}^1\chi_{89}^{11}$	8	17
1435	$\chi_5^1\chi_7^1\chi_{41}^{10}$	12	13
1436	$\omega_4^1\chi_{359}^{179}$	2	3
1455	$\chi_3^1\chi_5^1\chi_{97}^6$	16	17
1460	$\omega_4^1\chi_5^1\chi_{73}^{54}$	4	5
1461	$\chi_3^1\chi_{487}^{27}$	18	19
1465	$\chi_5^1\chi_{293}^{219}$	4	3^2
1477	$\chi_7^3\chi_{211}^{21}$	10	11
	$\chi_7^1\chi_{211}^{35}$	6	7
1496	$\omega_4^1\chi_8^1\chi_{11}^1\chi_{17}^8$	10	11
1509	$\chi_3^1\chi_{503}^{251}$	2	3
1513	$\chi_{17}^1\chi_{89}^{11}$	16	17
	$\chi_{17}^8\chi_{89}^{22}$	4	13
1516	$\omega_4^1\chi_{379}^1$	378	379
1525	$\chi_{25}^2\chi_{61}^{24}$	10	11
1547	$\chi_7^1\chi_{13}^1\chi_{17}^{12}$	12	37
1575	$\chi_9^1\chi_{25}^2\chi_7^5$	30	31
1576	$\omega_4^1\chi_8^1\chi_{197}^{49}$	4	3^2
1591	$\chi_{37}^{18}\chi_{43}^2$	42	43
1592	$\omega_4^1\chi_8^1\chi_{199}^{11}$	18	19
	$\omega_4^1\chi_8^1\chi_{199}^{33}$	6	7
1620	$\omega_4^1\chi_{81}^2\chi_5^1$	108	109
1623	$\chi_3^1\chi_{541}^{45}$	12	13
1629	$\chi_9^2\chi_{181}^{18}$	30	31
	$\chi_9^2\chi_{181}^{50}$	18	109
1640	$\omega_4^1\chi_8^1\chi_5^2\chi_{41}^5$	8	3^2
1641	$\chi_3^1\chi_{547}^{273}$	2	5
1643	$\chi_{31}^5\chi_{53}^{13}$	12	13
1651	$\chi_{13}^1\chi_{127}^{63}$	12	5^2
1665	$\chi_9^1\chi_5^1\chi_{37}^{24}$	12	13
1676	$\omega_4^1\chi_{419}^{19}$	22	23
1687	$\chi_7^2\chi_{241}^{80}$	3	13
1688	$\chi_8^1\chi_{211}^{42}$	10	31
1708	$\omega_4^1\chi_7^1\chi_{61}^{50}$	6	7
	$\omega_4^1\chi_7^3\chi_{61}^{30}$	2	3

f_χ	χ	g_χ	p
1729	$\chi_7^2\chi_{13}^3\chi_{19}^3$	12	5^2
	$\chi_7^1\chi_{13}^5\chi_{19}^{12}$	12	13
	$\chi_7^1\chi_{13}^2\chi_{19}^{15}$	6	7
1735	$\chi_5^1\chi_{347}^{173}$	4	5
1736	$\omega_4^1\chi_8^1\chi_7^2\chi_{31}^{15}$	6	7
1739	$\chi_{37}^9\chi_{47}^{23}$	4	5
1749	$\chi_3^1\chi_{11}^5\chi_{53}^2$	26	53
1751	$\chi_{17}^1\chi_{103}^{51}$	16	17
1755	$\chi_{27}^2\chi_5^1\chi_{13}^3$	36	73
1756	$\omega_4^1\chi_{439}^{219}$	2	5
1761	$\chi_3^1\chi_{587}^{293}$	2	7
1765	$\chi_5^2\chi_{353}^{176}$	2	3
1772	$\omega_4^1\chi_{443}^{221}$	2	3
1853	$\chi_{17}^8\chi_{109}^6$	18	19
1855	$\chi_5^2\chi_7^3\chi_{53}^{13}$	4	5
1865	$\chi_5^1\chi_{373}^{93}$	4	5
1872	$\chi_{16}^1\chi_9^2\chi_{13}^{10}$	12	13
1885	$\chi_5^1\chi_{13}^6\chi_{29}^1$	28	29
	$\chi_5^2\chi_{13}^3\chi_{29}^3$	28	113
	$\chi_5^1\chi_{13}^6\chi_{29}^7$	4	5
1887	$\chi_3^1\chi_{17}^4\chi_{37}^{27}$	4	5
1891	$\chi_{31}^3\chi_{61}^{21}$	20	41
	$\chi_{31}^2\chi_{61}^{28}$	15	31
	$\chi_{31}^6\chi_{61}^6$	10	11
1897	$\chi_7^3\chi_{271}^{135}$	2	5
1903	$\chi_{11}^5\chi_{173}^1$	172	173
1904	$\chi_{16}^1\chi_7^3\chi_{17}^3$	16	97
	$\omega_4^1\chi_{16}^1\chi_7^1\chi_{17}^{12}$	12	13
1921	$\chi_{17}^4\chi_{113}^8$	28	29
	$\chi_{17}^1\chi_{113}^{35}$	16	$17 \cdot 17^2$
1929	$\chi_3^1\chi_{643}^{321}$	2	3
1935	$\chi_9^2\chi_5^1\chi_{43}^7$	12	13
	$\chi_9^2\chi_5^1\chi_{43}^{21}$	12	13
1937	$\chi_{13}^1\chi_{149}^{111}$	12	109
	$\chi_{13}^6\chi_{149}^{74}$	2	3
1957	$\chi_{19}^9\chi_{103}^{51}$	2	3
1965	$\chi_3^1\chi_5^2\chi_{131}^{13}$	10	11
1971	$\chi_{27}^2\chi_{73}^4$	18	19
1972	$\omega_4^1\chi_{17}^2\chi_{29}^7$	8	3^2
1976	$\chi_8^1\chi_{13}^6\chi_{19}^2$	18	19
	$\chi_8^1\chi_{13}^1\chi_{19}^3$	12	13
1988	$\omega_4^1\chi_7^2\chi_{71}^5$	42	43
	$\omega_4^1\chi_7^1\chi_{71}^{14}$	30	31
1995	$\chi_3^1\chi_5^2\chi_7^2\chi_{19}^3$	6	7
1996	$\omega_4^1\chi_{499}^{249}$	2	5

Table 2. The probabilities for $p^k \mid \prod_{\tilde{\chi}} L_p(1,\chi)$ with $p \equiv 1 \pmod{g_\chi}$.

p	k	found	exp
3	1	42/147=.286	.333
	2	14/147=.0952	.111
	3	2/147=.0136	.0370
	4	1/147=.0068	.0123
	5	.0068	.0041
	6	.0068	.0014
5	1	53/215=.247	.251
	2	8/215=.0372	.0602
	3	0	.0141
	4	0	.0032
7	1	76/365=.208	.216
	2	23/365=.0630	.0413
	3	6/365=.0164	.0074
	4	2/365=.0055	.0013
11	1	41/255=.161	.187
	2	10/255=.0392	.0338
	3	2/255=.0078	.0056
	4	0	.0008
13	1	69/463=.149	.134
	2	9/463=.0194	.0156
	3	0	.0017
17	1	35/266=.132	.114
	2	5/266=.0188	.0144
	3	3/266=.011	.0019
19	1	52/434=.120	.113
	2	8/434=.0184	.0127
	3	1/434=.0023	.0014
23	1	16/184=.0870	.107
	2	2/184=.0109	.0176
	3	1/184=.0054	.0028
29	1	33/290=.114	.087
	2	3/290=.0103	.0087
	3	1/290=.0034	.0009

p	k	found	exp
31	1	45/522=.0862	.0827
	2	0	.0066
37	1	31/542=.0572	.0657
	2	2/542=.0037	.0044
	3	1/542=.0018	.0003
41	1	22/380=.0579	.0668
	2	3/380=.0079	.0046
43	1	37/462=.0801	.0644
	2	1/462=.0022	.0048
47	1	10/171=.0585	.0712
	2	2/171=.0117	.0124
	3	1/171=.0058	.0020
53	1	16/255=.0627	.0561
	2	0	.0054
59	1	5/164=.0305	.0546
	2	1/164=.0061	.0092
61	1	28/641=.0437	.0464
	2	3/641=.0047	.0021
67	1	14/419=.0334	.0435
	2	0	.0030
71	1	19/334=.0569	.0514
	2	0	.0034
73	1	19/334=.0234	.0395
	2	0	.0018
79	1	21/419=.0501	.0413
	2	5/419=.0119	.0031
	3	1/419=.0024	.0003
83	1	1/154=.0065	.0290
	2	0	.0041
89	1	9/295=.0305	.0371
	2	0	.0024
97	1	13/551=.0236	.0296
	2	0	.0013

Table 3. The probabilities for $p^{f_p k} \mid \prod_{\widetilde{\chi}} L_p(1,\chi)$ with $f_p > 1$.

p	f_p	found	exp
3	2	9/105=.0882	.144
	3	7/35=.200	.140
	4	2/150=.0133	.0178
5	2	19/298=.0638	.0542
	3	0	.0819
	4	1/93=.0108	.0086
7	$2, k = 1$	7/172=.0407	.0445
	$2, k = 2$	2/172=.0116	.0019
	3	2/97=.0206	.0106
	4	1/254=.0039	.0016
11	2	8/445=.0180	.0159
	3	1/107=.0093	.0040
13	2	4/167=.0240	.0257
17	2	2/374=.0053	.0093
19	2	3/366=.0082	.0089
23	2	2/419=.0048	.0044
29	2	4/547=.0073	.0037
31	2	1/228=.0044	.0046
43	2	1/237=.0042	.0026
53	2	4/444=.0090	.0016
79	2	1/403=.0025	.0008
83	2	1/488=.0020	.0005
89	2	1/624=.0016	.0006
97	2	1/138=.0072	.0009

Table 4. The values of the product $h_K R_p(K)/p^{g-1}$, $f_\chi < 2000$, $p < 100$.

f_χ	p	g_χ	v_p
5			
7	61	3	1
11			
13			
17	5	4^*	2
	61	4^*	1
19	3	$9, 3^*$	1,1
	67	3^*	1
23			
29	3	2^*	2
	11	2^*	1
	43	7	1
31	11	5	2
37	3	$9, 3^*$	1,1
	7	$18, 2^*$	3,1
	89	2^*	1
41	5	$20, 4^*$	1,1
	11	5	1
	29	$4^*, 2$	1,2
	53	2	1
43			
47			
53	5	2^*	1
59			
61	11	10	1
	13	6,3	2,1
	43	3	1
	71	5	1
67	43	3	1
71			
73	3	9,3	1,1
	5	4,2	1,2
	7	3,2	1,1
	19	9	1
	29	3	2
	37	12	2
	41	2	1
79	13	$39, 3^*$	1,1
83			
89	5	2	2
	7	2	1
	13	2	1
	23	11	1
	59	2	1
97	5	$24, 4^*$	2,1
	7	3^*	1
	17	2	1
	29	4	1
	31	3^*	1
	43	3^*	1
101	5	25,5	2,2
	7	2^*	1
	31	5	1
103	43	3	1
107			
109	3	54,27,18,9,	1,1,1,1,
		$6^*, 3, 2$	1,1,1

f_χ	p	g_χ	v_p
	5	2	1
	11	2	1
	19	2	1
113	3	2	1
	29	28	1
	53	2	1
127	3	9,3	1,1
	43	7	1
131			
137	3	2	2
139	19	3^*	1
	43	3^*	1
149	7	2	1
151	5	75,25,15,	2,1,2,
		5,3	1,2
	13	3	1
	31	15,3	1,1
	41	5	1
157	5	6^*	2
	19	6^*	1
	53	26	1
	79	78	1
163	3	$81, 27, 9, 3^*$	1,1,1,1
	7	3^*	1
	73	3^*	1
167			
173	3	2^*	1
179			
181	3	18,9,6,	1,1,1,
		3,2	1,1
	11	5	1
	31	15	1
	37	18	1
191	11	5^{+*}	1
193	7	6	1
	13	12	1
	19	2	2
	31	6	1
	37	12	1
	41	4	1
197	7	49,7	2,2
	29	7	1
	43	14	1
199	3	9,3	2,2
	19	9	1
	73	9	1
211	11	5	1
	29	7	1
	43	21	1
	71	35,5	1,1
223	43	3	1
227			
229	3	$6^*, 2^{+*}$	1,1
	67	3	1
233			
239	29	7	1
241	5	10,2	2,1

f_χ	p	g_χ	v_p
	29	2^*	1
	7	3	1
	11	12	2
	13	4^*	1
	31	30,15,10	1,1,1
	41	$40, 4^*$	2,1
	73	8	1
	89	2	1
251	5	125,25,5	1,1,1
	31	5	1
	41	5	1
257	3	2^{+*}	3
	5	2^*	1
	17	16,8	1,1
	41	4	1
	53	4	1
263			
269	11	2	1
271	3	27,9,3	2,2,2
	61	5	1
277	7	6^*	1
	13	6^*	1
	47	46	1
	73	6^*	1
281	3	20,2	4,1
	5	20,4	1,1
	11	2	1
	13	4	1
	17	2	1
	29	14	3
	71	70,7	1,1
	89	4	1
283			
293			
307	3	9,3	1,1
	19	3	1
	37	9	1
311	11	5	1
313	3	78,26	3,3
	5	4	1
	7	3^{+*}	2
	11	2	1
	37	12	1
	79	78,13	2,1
317	23	2	1
331	13	3	1
	23	11	1
	41	5	1
	71	5	1
337	3	6,2	1,1
	5	24,8	2,2
	7	14,2	1,1
	13	21	2
	17	8	1
	19	2	1
	29	56	2
	43	21	1
	73	12	1
	97	3	1
347			

f_χ	p	g_χ	v_p
349	7	6	1
	41	2	1
	59	58	1
353	3	4,2	2,2
	13	4	1
	23	22,11	1,1
	89	88	1
359			
367	5	3	2
373	7	6,3	1,1
	19	3	1
	43	3	1
379	3	27,9,3	1,1,1
	13	3	1
383			
389	19	2	1
	29	2	1
397	3	$18, 9, 6^*,$	1,1,1,
		3,2	1,1
	11	$66, 6^*$	2,2
	13	$6^*, 3$	1,1
	23	66	2
	37	9	1
401	3	$8^{+^2}, 2^*$	2,1
	5	100,50,25,20,	1,1,2,1,
		$10,5,4,2^{+*}$	1,2,1,1
	17	2^*	1
	23	2^*	1
	29	2^*	1
	41	40	1
409	7	6	2
	13	6,3	1,1
419			
421	11	10,5	1,1
	19	6	1
	37	3	1
	61	15	1
	71	70,35,7,5	1,1,1,1
431	11	5	3
433	3	27,9,3	1,1,1
	5	4,2	2,1
	7	2	1
	13	3	1
	17	8	1
	19	9	1
	37	36	1
	53	72	2
	73	72	1
	97	12	1
439			
443	3	13	3
449	3	2	1
	7	112,16,14,2	2,2,1,2
	13	4	1
	17	16	3
	29	14	1
	97	32	1
457	3	6,2	1,1
	5	$4^{+*},2$	1,1
	7	3	1

f_χ	p	g_χ	v_p
	13	4^*	1
	37	$4^*, 3$	1,1
461	3	2	1
	31	5	1
	47	46,23	1,1
	61	10	1
	71	10	1
463	7	21,3	1,1
	29	7	1
	43	7	1
	67	33	1
467			
479			
487	3	243,81,27,	2,2,2,
		9,3	2,2
491	7	49,7	1,1
499	13	3	1
503			
509	5	2	1
	11	2	1
	29	2	1
521	3	26^{+^3},2	3,2
	11	5,2	1,1
	29	4	1
	41	20	1
	53	13	1
523	3	9,3	3,2
	7	3	1
	19	9	1
541	3	27,9,3	2,2,2
	5	10,2	1,1
	19	3	1
	73	3	1
547	43	7	1
557			
563			
569	5	4	1
	11	2	1
571	13	3	1
577	3	72,24,9,	2,2,1
		8,3	2,1
	5	3	2
	7	6,3,2^{+*}	3,2,1
	13	12	1
	17	144,72,16	2,2,3
	29	4	1
	31	3	1
	67	3	1
	73	72	1
	97	32	1
587			
593	5	4	1
	7	2	1
	11	2	1
	19	2	1
	31	2	1
599	3	13	3
601	5	25,5	1,1
	7	300,6,3	4,1,1
	11	20	2

f_χ	p	g_χ	v_p
	29	4	1
	31	30,10,6	1,1,1
	59	2	1
	61	4	1
607			
613	3	9,3	1,1
	19	18,6	1,1
	37	18	1
617	5	2	2
	13	28,14,4,2	2,2,1,1
	23	22	1
	43	22,7	2,1
	53	2	1
619	19	3	1
	31	3	1
	43	3	1
631	3	9,3	1,1
	11	5^+	1
	43	7	1
641	3	$40, 8^{+^2 *}$	4,4
	5	$20, 4^{+*}$	1,1
	11	40,10,5^+	2,1,1
	17	16,2	1,1
	29	40	2
	31	320	2
	41	40	2
643	7	3	1
	31	3	1
647			
653	3	2	1
	19	2	1
659			
661	5	30,6	2,2
	7	3	1
	11	110,55,10,5	1,1,1,1
	13	2	1
	19	3	1
	23	22	1
	31	30	1
	43	2	1
	61	3	1
	67	22	1
	79	3	1
673	5	6,4,2	2,1,1
	7	336,48	2,2
	17	8	1
	31	3	1
	43	21,14	1,1
	71	14	1
677	3	26	3
	13	169,13	1,1
	43	2^*	1
	53	26	1
683			
691	11	5	1
	31	5	1
	71	5	1
701	5	25,5	2,2
709	31	3^*	1
	53	2	1

f_χ	p	g_χ	v_p
719			
727	11	121,11	1,1
	23	11	1
733	3	$6^*, 2^{+*}$	1,3
	7	6^*	1
739	3	9,3	1,1
743			
751	5	125,25,5	1,1,1
	13	3	1
	19	3	1
	31	15	1
757	3	27,9,3	1,1,1
	7	21,3	1,1
	29	7	1
	37	18	1
761	3	2^+	1
	5	10,2	1,1
	11	10	2
	29	4	1
	61	10	2
769	5	48	4
	7	3,2	1,1
	13	12	1
	17	16	1
	73	24	1
	97	64,3	2,1
773	3	2	1
	11	2	1
787			
797	7	2	3
809			
811	3	81,27,	1,1,
		9,3	1,1
	13	3	1
	41	5	1
	79	3	2
821	11	10^+,5	2,1
823	7	3	3
827	43	7	1
829	3	9,3	1,1
	7	2	2
	19	9,6	2,1
	37	18	1
	47	46^+,23	3,1
839			
853	11	6	2
	19	3	1
857	5	4^{+*},2	1,1
	17	2	1
	29	2	1
859	79	39	1
	89	11	1
863			
877	3	$6^*, 2$	1,2
	5	6^*	2
	7	$6^{+*}, 3^{+*}$	1,1
	13	$6^*, 3^*$	2,1
	37	3^*	1
881	5	10,2	1,1
	17	8	1

f_χ	p	g_χ	v_p
	23	22	1
	41	10	1
	89	55,44	2,1
883	3	9,3	1,1
	7	147,49,21,	2,1,2,
		7,3	1,2
	13	3	1
	19	9	1
	37	3	1
	43	7	1
887			
907	5	3	2
911	53	13	1
919	3	27,9,3	2,2,2
929	3	2	1
	5	4	1
	7	16	2
	11	2	1
	17	16	1
	53	2	1
937	3	$9, 3^*$	1,1
	7	6,2	1,1
	11	2	1
	17	4	1
	19	9,6	3,1
	37	36	1
	53	468	2
	79	78,39,26	1,1,1
941	61	5^*	1
947			
953	3	2	1
	11	2	1
	17	68,4	1,1
	29	4	1
	43	7	1
	71	7^+	1
967	7	21,3	1,1
	43	21	1
971	31	5	1
977	3	8	2
	5	4^{+*}	1
	11	8,2	2,2
	19	2	2
	31	2	1
	73	2	1
983			
991	3	9,3	1,1
	11	55,5	2,2
	31	15	1
	37	9	1
997	3	6,2	2,1
1009	3	18,9,6,	1,1,1,
		3,2	1,2
	5	4	1
	7	42,14,6,2^+	1,1,1,1
	13	12,8	1,2
	19	72	2
	29	21,4	2,1
1013	3	2	2
	47	23	1

f_χ	p	g_χ	v_p
1019			
1021	11	10,5	1,1
	13	3	1
1031	11	5	3
1033	5	12,4	2,1
	13	3	2
	19	6	1
	29	4	1
1039			
1049	11	2	1
	17	4	2
	19	2	1
	53	4	1
1051	5	25,5	1,1
	7	21,3	1,2
	41	5	1
	43	3	1
1061	17	2	1
	61	5	1
1063	3	$9,3^*$	1,1
	13	3^{+*}	1
	19	9	1
1069	7	6^{+*}	1
	13	6^*	1
	31	2	1
	41	2	1
1087	19	3	1
1091	11	5	1
1093	5	2^{+*}	1
	43	21	1
	67	3	1
	79	78,13	2,1
1097	5	4	1
	37	4,2	1,1
1103	59	29	1
1109	37	2	1
1117	3	18,9,6, 3,2	1,1,1, 1,2
	7	3	2
	13	6	1
	19	9	1
	43	6	1
1123	13	3	1
1129	3	$6^*, 2^{+^2}$	2,2
	5	4	1
	7	$6^*, 3^{+*}$	1,1
	13	2	1
	29	4	1
1151	5	25,5	1,1
	11	5	1
	47	23	1
	61	5	1
1153	3	18,9,6, 3,2	1,1,1, 1,1
	5	4	2
	7	24	2
	13	6,3	1,1
	19	$72,9^+$	2,1
	37	18	1
	73	24	1

f_χ	p	g_χ	v_p
	97	96	1
1163			
1171	3	9,3	1,1
	31	15	1
	53	13	1
	79	39	1
1181	3	2	1
	11	10,5	1,1
	13	2	1
	47	2	1
	61	5,2	1,1
	71	5	1
1187			
1193	5	4	1
	7	2	1
1201	5	25,5	2,2
	7	4	4
	11	10	1
	13	12,4	1,2
	19	60,6	2,1
	31	15	1
	61	60,30	1,2
	71	5	1
1213	3	6,2	1,6
	5	2	1
	7	3	2
	13	6	1
	19	3	2
	37	3	1
1217	3	8,2	2,1
1223	3	13	3
1229	3	2^{+*}	1
1231	7	3	2
	11	5	1
	83	41	1
1237	3	6,2	1,1
	5	6,3	2,2
	7	3	2
	13	2	1
	31	6	1
	37	3	1
	43	2	1
	53	2	1
	97	6	1
1249	3	6,2	2,1
	17	16	1
	61	6	1
	79	624,39,26	2,1,1
	97	16	1
1259			
1277	3	2	1
	23	11	2
1279	3	9,3	1,2
	7	3	1
	19	9	2
	37	9	1
1283			
1289	5	2	1
	29	28	1
1291	11	5	1

f_χ	p	g_χ	v_p
1297	3	162,81,54,	1,3,1,
		27,18,9,	3,1,3,
		6,3,2*	1,3,1
	5	8^{+^2},4	2,1
	7	3	2
	11	2^{+*}	1
	13	12	1
	67	6,3	1,1
	73	2*	1
1301	3	13	3
	5	50,25,10,	1,1,1,
		5,2	1,1
1303	5	3	2
	43	21	1
1307			
1319			
1321	5	60,12,	2,2,
		10,2	1,1
	11	55,5	2,2
	23	44,22,11	2,3,1
	31	15	1
	61	60	2
	89	44	1
1327	7	3	2
	67	3	1
	79	13	3
1361	11	10	1
	17	68,4	2,2
	31	5,2	1,1
	61	5	1
	97	8	1
1367			
1373	3	2^{+*}	1
	7	686,343,98,49,	1,1,1,1,
		14, 7, 2*	1,1,2
	19	2*	1
	29	7	1
	43	14	1
1381	7	6^+,3	5,4
	13	3,2	1,1
	19	6	1
	31	5	1
	41	10	1
	61	10,6	1,1
1399			
1409	17	16,4	1,1
	67	11	1
	89	44,11	1,1
1423	3	9,3	1,1
	11	3	2
	13	3	1
	19	9	2
1427			
1429	3	6,2	2,2
	5	2^+	1
	7	42,6	4,2
	13	6	1
	61	6	1
1433	3	2	2
	13	4	1

f_χ	p	g_χ	v_p
1439			
1447	13	3	1
1451	5	25,5	1,1
	11	5	2
1453	3	6,2	2,3
	11	121,11	1,1
	23	22	1
	31	6	1
	43	2	1
	79	3	1
1459	3	729,243,81,	1,1,1,
		27,9,3	1,1,1
	5	3	2
	13	3^+	2
	19	9^+	1
1471	7	49,7	2,2
	43	21	2
	71	35	1
1481	5	20,4	1,1
	61	5	1
1483	5	3	2
	7	57,3	3,1
	13	39,3	1,2
	79	39	1
1487			
1489	3	6,2^+	2,1
	7	24	4
	11	4	2
	13	4, 3*	2,1
	17	4	1
	19	3^{+*}	1
	73	12	1
1493	5	2	1
1499			
1511			
1523			
1531	3	9,3	3,2
	19	9,3	1,1
	37	9	3
	73	9	1
1543	7	3	1
	13	3	2
1549	3	9,3	1,1
	7	6,3	1,1
1553	3	8	2
	5	4	1
	7	4,2	2,1
	11	2	1
	13	4	1
	17	8,4	1,1
	73	4	1
1559			
1567	3	27, 9, 3*	1,1,1
	7	3^{+*}	2
	37	9	1
	59	29	2
1571	41	5	1
1579			
1583	29	7	1
	71	7	1

f_χ	p	g_χ	v_p
1597	5	2	1
	13	2	1
	29	14,7	1,1
1601	5	100,25,20,	1,1,1,
		5,4	1,1
	7	2^{+*}	1
	17	16,8	1,3
	61	4	1
1607			
1609	3	6,2	1,1
	13	2	2
	97	6	1
1613	13	26,2	1,1
1619			
1621	3	81,27,	2,2,
		9,3	2,2
	5	10,2	1,2
	31	15	1
1627	7	3	2
1637	5	2	1
1657	3	36,12,9,	2,2,1,
		4,3	2,1
	17	4	1
	19	9,6	2,1
	29	2	1
	43	6	1
	97	12	1
1663	7	3	1
	53	3	2
1667	7	49,7	1,1
1669	3	6,2	1,1
	7	3	1
	23	2	1
	67	2	1
1693	3	9,3	2,2
	7	6,3	1,3
	13	6	1
	19	6,3	1,1
	37	6	1
	61	6	1
1697	5	4^{*}	1
	17	4^{+*}	1
1699			
1709	7	14,2	1,1
	29	14	1
	47	2	1
	71	7	1
1721	17	4	1
	29	4	1
	31	5	1
	61	5	1
1723	7	21,3	1,1
	13	3	1
	37	3	1
	83	287	2
1733			
1741	5	10,2	1,1
	7	3	1
	31	30	1
	61	5	1

f_χ	p	g_χ	v_p
	67	6	1
	79	3	1
	97	3	1
1747	3	9,3	2,3
	13	3	2
	19	9	1
1753	3	6,2	1,1
	5	4	3
	13	12,4	1,1
	37	2	1
	41	4	1
	73	146,2	1,1
1759	7	3	1
	13	3	1
	67	3	1
1777	5	2	1
	7	3	2
	41	4	1
	53	4	1
1783	3	81,27,9,3	1,1,1,1
	19	9	1
	31	3	1
	67	33	1
1787			
1789	7	2	1
	17	2	1
1801	3	9,3	1,1
	5	300,60,25,	2,2,1,
		12,5	2,1
	11	5	2
	19	2	1
	31	30	1
	53	2	1
	61	60	1
	79	3	1
1811	41	5	1
	71	5	1
1823			
1831	7	3^{+}	1
1847			
1861	5	310,62,10,2	3,3,2,1
	7	3	1
	11	5	2
	19	6	1
	31	930,310,155,	1,1,1,
		30,10,5	1,1,1
	43	3	1
1867	43	3	1
1871			
1873	3	9,3	1,1
	5	8^{+^2}	2
	17	8	1
	29	4	1
	37	18	1
	53	936,52	2,1
	73	12,9	1,1
	79	78	2
1877	13	2	1
1879	7	3	1
1889	3	4	2

f_χ	p	g_χ	v_p
	5	4	2
	7	16^{+^2},2	2,2
	17	2	1
	97	16	1
1901	3	2^+	2
	5	25,5	1,1
	11	95,10	3,1
	31	5	1
1907			
1913	3	4	2
	5	4,2	1,1
1931			
1933	19	3	1
	29	14	2
	43	3	1
	47	46	3
1949			
1951	3	39,13	3,3
	5	25,5	1,1
	11	5	1

f_χ	p	g_χ	v_p
	19	3	1
	31	15	1
	41	5	2
	79	39	2
1973	3	2	1
	17	34,2	1,1
	37	2	1
1979			
1987	7	3^{+*}	2
1993	3	6,2	1,1
	5	4	1
	7	3	1
	13	12	1
	23	2	1
	61	12	1
	73	3	1
1997			
1999	3	27,9,3	2,2,2
	19	9	1

Table 5. The values of the product $h_K R_p(K)/p^{g-1}$, $f_\chi < 10000$, $p \mid h_K$.

f_χ	p	g_χ	v_p
1231	211	15^+	1
2029	7	2^{+*}	1
2081	5	$10^+,2^+$	1,1
2089	3	$18^+,9,6^+,$	1,1,1,
		$3,2^+$	1,1
2113	37	12^+	2
2153	5	2^+	1
2213	3	2^{+*}	1
2351	11	5^+	3
2381	11	10^+	1
2417	17	4^{+*}	1
	41	8^{+*}	1
2437	7	$21,3^+$	1,1
2473	5	4^+	1
2557	3	18,9,6,	1,1,1,
		$3^*,2^+$	1,1
	7	$6^+,3^{+*}$	2,3
2617	13	4^{+*}	1
2621	11	10^+	1
2659	19	3^{+*}	1
2677	3	$6,2^+$	1,1
2713	3	$6,2^+$	2,1
2753	3	$8^{+^2},2$	2,2
2777	3	$4,2^+$	2,2
2857	3	$6,2^+$	3,1
2917	3	1458,729,486,	2,2,2,
		243,162,81,	2,2,2,
		54,27,18,	2,2,2,
		$9,6^*,$	2,2,
		$3,2^+$	2,3
	7	$6^{+*},3$	2,1
3001	11	$10^+,5^+,2$	2,1,1
3041	13	4^{+*}	2
3121	5	20,10,	4,2,
		$4,2^+$	2,1
	61	20^+	1
3137	3	2^{+^2*}	3
3181	5	$10,2^+$	1,1
3217	7	3^+	1
3221	3	2^+	1
3229	3	$6^+,2^+$	1,1
3253	5	2^{+*}	3
3301	151	$150,75,15^+$	1,1,1
3313	7	6^{+*}	1
	19	$9,3^{+*}$	1,1
3433	37	12^+	1
3469	13	6^+	1
3529	19	$9,6,3^+$	1,1,1
3547	19	$9,3^{+*}$	1,1
	883	9^+	1
3571	7	$21,3^+$	1,1
3581	11	5^+	1
3697	5	$4^+,2$	1,1
3877	3	$6,2^+$	1,1
3889	3	486,243,162,	2,1,2,
		81,54,27,	1,2,1
		18,9,6,	2,1,2,

f_χ	p	g_χ	v_p
		$3,2^+$	1,1
4001	3	$20,8,2^+$	4,2,1
4049	23	$506,22^+$	1,1
4073	5	4^+	1
4177	19	$18^+,9$	1,1
4201	11	5^+	1
4219	7	3^+	1
4229	7	$14,2^{+*}$	1,1
4241	3	$4^{+^2*},2$	2,4
4339	7	3^+	1
4357	5	2^{+*}	2
4409	3	2^{+^2}	2
4441	5	20,15,10,	1,2,1,
		$4^+,3,2^+$	1,2,2
4457	5	4^+	2
4481	3	$40,8,2^+$	4,2,1
	97	32^+	1
4493	3	2^{+*}	2
4591	19	9^+	3
4597	3	$6^*,2^+$	1,1
	7	6^{+*}	1
4603	79	39^+	1
4649	3	2^+	1
4657	5	4^+	1
4729	3	$6,2^+$	1,4
	13	$12^+,6,$	1,1,
		4,2	1,1
4783	7	3^+	1
4793	5	4^+	1
4817	17	8^+	1
4861	7	6^+	1
4889	5	$4,2^+$	1,1
4933	3	$18,9,6^+,$	1,3,1,
		$3,2^+$	2,1
4937	5	4^+	1
4993	5	$24,4^+,2$	2,1,1
5051	1451	5^{+*}	1
5081	3	2^+	1
5101	11	10^+	1
5119	31	3^{+*}	1
5209	29	$28,14^+,$	1,1,
		7,4	1,1
5261	3	2^+	1
5273	7	2^+	1
5281	3	$6^+,2^+$	3,4
5297	3	2^+	1
5333	3	2^{+*}	1
5413	23	11^+	1
5417	7	2^+	1
5437	31	6^{+*}	1
5441	11	$10^+,5$	1,1
5477	3	2^{+*}	2
5501	11	$55,5^+$	3,1
5521	3	$6,2^+$	2,2
5557	19	3^{+*}	1
	73	6^+	2
5581	73	9^+	2

f_χ	p	g_χ	v_p
5641	3	$12, 4^{+^2*}$	2,2
5701	101	10^+	1
5741	3	2^+	2
5821	3	$6,2^+$	1,1
5827	13	3^+	1
5953	7	$3^+,2$	1,1
6037	7	$6^{+*},3$	1,1
6053	3	2^+	1
6073	13	$12^+,4$	1,1
6113	5	2^+	1
6133	3	$6,2^+$	2,1
6229	13	6^+	2
6257	29	4^{+*}	1
6337	97	$48^+,16$	2,1
6361	61	$20^+,12,$	2,1,
		5,3	1,1
6421	41	$10^+,2$	1,1
6449	5	$104,4^+$	4,1
6481	5	120,24,	2,2,
		$10,2^+$	1,1
6521	5	$20,4^+$	1,1
6529	13	12^+	1
6577	17	4^{+*}	1
	313	8^{+*}	1
6581	11	$10,5^+$	2,2
6637	3	$6^+,2^+$	2,1
6673	17	8^+	1
6709	7	6^+	1
6737	3	$4^{+^2},2$	2,1
6781	13	6^+	1
6949	5	2^+	1
6961	17	8^+	1
6991	7	3^+	1
6997	3	$6^*, 2^+$	1,1
	7	6^{+*}	1
7057	3	18,9,6,	2,1,2,
		$3, 2^{+*}$	1,1
	7	588,147,98,	2,1,1,
		84,49,21,	2,1,1,
		$14^+,12,7,$	1,2,1,
		$3, 2^{+*}$	1,1
7229	5	2^{+*}	1
7333	13	$78, 6^{+*}$	2,2
7351	7	$147,49,21^+,$	1,1,1,
		$7,3^+$	1,2
7369	13	12^+	2
7411	131	65^+	2
7417	109	12^+	1
7481	3	2^+	4
7489	7	$16, 3^{+*}$	2,1
7529	5	4^+	1
7537	3	$6,2^+$	1,1
7561	37	6^+	1
7573	3	$6, 2^{+^2*}$	2,2
7621	7	3^+	2
7673	3	2^+	1
7753	3	$6,2^+$	1,2
	5	$4^{+^2},3^{+^2}$	4,2
7817	5	2^+	1
7841	421	5^{+*}	1

f_χ	p	g_χ	v_p
7873	3	$6^+,2^{+^2}$	2,2
7937	41	4^{+*}	1
8017	3	$6^{+*},2^+$	1,1
	7	6^{+*}	1
	19	3^{+*}	1
	109	12^+	1
8069	3	2^+	2
8101	13	2^{+*}	1
8161	5	60,20,	2,1,
		$12,4^+$	2,1
8269	37	3^+	1
8287	7	3^+	1
8297	3	$4^{+^2*}, 2$	2,1
	5	4^{+*}	2
8317	113	14^+	1
8377	5	4^+	2
8389	19	6^{+*}	1
8431	31	15^+	1
8501	5	250,125,50,	1,1,1,
		25,10,	1,1,
		$5,2^+$	1,1
8563	7	3^{+^2*}	2
8581	3	78,66,26,	3,5,3,
		$22,6^+,2^+$	5,2,2
8597	3	2^+	1
8629	7	$3^+,2$	2,1
8681	11	$10^+,5$	1,2
8689	5	$24,2^+$	2,1
8713	3	18,9,6,	3,1,4,
		$3,2^+$	1,3
	67	33^+	3
8761	3	$6^+,2^{+^2}$	2,4
8837	3	2^{+*}	1
8893	7	$6^+,3,2$	1,1,2
9001	31	10^+	1
9013	7	6^+	1
9029	7	2^{+*}	1
9041	17	4^{+*}	1
9049	7	$6,2^+$	1,2
9127	31	3^{+*}	1
9133	3	$6^*, 2^+$	1,2
	7	6^{+*}	1
9161	5	20,10,	2,1,
		$4^+,2$	2,1
9181	5	$10^+,2^+$	2,2
9241	13	$84,3^+$	2,1
9277	7	3^+	1
9281	3	$8,5,2^+$	2,4,2
9293	3	2^+	1
9319	7	3^{+*}	2
9377	5	4^+	3
9413	3	$26^{+^3}, 2^{+*}$	3,1
9421	7	$6^+,3,2$	1,1,1
	11	$10^+,5^+$	1,1
9511	73	3^+	1
9521	113	28^+	1
9551	541	5^+	1
9601	5	100,25,20,	1,1,1,
		$5,4^+$	1,1
9613	7	6^+	1

f_χ	p	g_χ	v_p
9689	29	28^+	1
9697	3	$12,4^+$	2,2
9697	7	$8,6,3^+$	2,1,1
9749	3	2^+	2

f_χ	p	g_χ	v_p
9817	17	4^{+*}	1
9833	3	2^+	1
9857	73	8^+	1
9907	31	3^{+*}	1

Bibliography

[1] M. Aoki, T. Fukuda, *An algorithm for computing p-class groups of abelian number fields*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., **4076**, Springer, Berlin (2006), pp. 56–71

[2] J. Buhler, C. Pomerance, L. Robertson, *Heuristics for class numbers of prime-power real cyclotomic fields*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI (2004), pp. 149–157.

[3] H. Cohen, H. W. Lenstra, *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math. **1068**, Springer, Berlin (1984), pp. 33–62.

[4] C.-E. Fröberg, *On the prime zeta function*, BIT **8** (1968), pp. 187–202.

[5] G. Fee, A. Granville, *The prime factors of Wendt's binomial circulant determinant*, Math. Comp. **57** (1991), pp. 839–848.

[6] I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc. **72** (1952), pp. 327–340.

[7] M.-N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de* $\mathbf{Q}$, J. Reine Angew. Math. **277** (1975), pp. 89–116.

[8] M.-N. Gras, *Table numérique du nombre de classes et des unités dans les extensions cycliques réelles de degre* 4 *de* $\mathbf{Q}$, Publ. Math. Fac. Sci. Besançon 1977/78, Fasc. 2, 52 pp.

[9] M.-N. Gras, *Special units in real sextic fields*, Math. Comp. **48** (1987), pp. 179–182.

[10] G. and M.-N. Gras, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de* $\mathbf{Q}$, Bull. Sci. Math. (2) **101** (1977), no. 2, pp. 97–129.

[11] G. Gras and S. Jeannin, *Critère effectif de puissance p-ième dans un corps de nombres galoisien*, J. Number Theory **63** (1997), no. 2, pp. 339–356.

[12] R. Greenberg, *On p-adic L-functions and cyclotomic fields II*, Nagoya Math. J. **67** (1977), pp. 139–158.

[13] T. Hakkarainen, *On the computation of class numbers of real abelian fields*, submitted.

[14] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

[15] S. Jeannin, *Tables des nombres de classes et unités des corps quintiques cycliques de conducteur* $f \leq 10000$, Publ. Math. Fac. Sci. Besançon 1994/95–1995/96, 40 pp.

[16] Y. Koyama and K. Yoshino, *Prime divisors of real class number of* p^r*th cyclotomic field and characteristic polynomials attached to them*, Preprint (2003), 23 pp.

[17] H. W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat. 1953, no. 2 (1954), 48 pp.

[18] H. W. Leopoldt, *Über Klassenzahlprimteiler reeller abelscher Zahlkörper als Primteiler verallgemeinerter Bernoullischer Zahlen*, Abh. Math. Sem. Univ. Hamburg **23** (1959), pp. 36–47.

[19] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), pp. 535–541.

[20] F. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), pp. 693–707.

[21] J. M. Masley, *Class numbers of real cyclic number fields with small conductor*, Compositio Math. **37** (1978), no. 3, pp. 297–319.

[22] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), pp. 179–330.

[23] T. Metsänkylä, *An application of the p-adic class number formula*, Manuscripta Math. **93** (1997), pp. 481–498.

[24] S. Mäki, *The determination of units in real cyclic sextic fields*, Lecture Notes in Math. **797**, Springer, Berlin (1980), 198 pp.

[25] K. Nakamula, *Class number calculation of a sextic field from the elliptic unit*, Acta Arith. **45** (1985), no. 3, pp. 229–247.

[26] A. Odlyzko, *Discriminant bounds*, Unpublished tables, 1976, `http://www.dtc.umn.edu/~odlyzko/unpublished/`

[27] B. Oriat, *Groupes des classes d'idéaux des corps quadratiques réels* $\mathbf{Q}(d^{1/2}), 1 < d < 24572$, Publ. Math. Fac. Sci. Besançon 1986/87–1987/88, Fasc. 2, 65 pp.

[28] B. Oriat, *Quelques caractères utiles à l'arithmétique*, Publ. Math. Fac. Sci. Besançon 1974–1975, 26 pp.

[29] B. Oriat, *Traduction française de "Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper"*, Publ. Math. Fac. Sci. Besançon 1974–1975, 34 pp.

[30] PARI/GP, version `2.2.8`, Bordeaux, 2005, `http://pari.math.u-bordeaux.fr/`

[31] S. Perlis and G. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), pp. 420–426.

[32] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), pp. 913–937.

[33] R. Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), pp. 543-556.

[34] W. Schwarz, *Über die Klassenzahl abelscher Zahlkörper*, PhD Thesis, University of Saarbrücken (1995), 125 pp.

[35] D. Shanks, *Simplest cubic fields*, Math. Comp. **28** (1974), pp. 1137-1152.

[36] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.

[37] C. Wittmann, *p-class groups of certain extensions of degree p*, Math. Comp. **74** (2005), pp. 937–947.

[38] Wolfram Research, Inc., Mathematica, Version 4.1, Champaign, IL (2001).

[39] K. Yoshino, *A condition for divisibility of the class number of real pth cyclotomic field by an odd prime distinct from p*, Abh. Math. Sem. Univ. Hamburg **69** (1999), pp. 37–57.

Turku
Centre *for*
Computer
Science

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Information Technologies

Turku School of Economics
- Institute of Information Systems Sciences

ISBN 978-952-12-1881-1
ISSN 1239-1883