The field descent and class groups of CM-fields

Bernhard Schmidt
School of Physical & Mathematical Sciences
Nanyang Technological University
No. 1 Nanyang Walk, Blk 5, Level 3
Singapore 637616
Republic of Singapore
bernhard@ntu.edu.sg

April 15, 2005

Abstract

We consider the following "field descent problem" for principal ideals I of number fields K. Assume that I is invariant under a Galois automorphism σ of K; decide wether there is a generator g of I with $g^\sigma = g$, i.e., wether I can be generated by an element of Fix σ. We solve this problem for certain ideals by elementary methods. As a consequence, we are able to exhibit large explicit subgroups of class groups of CM-fields. This leads to some good lower bounds for the p-ranks of these class groups.

2000 Mathematics Subject Classification
11R29 (primary), 11R20 (secondary)

1 Introduction

Ideal class groups of algebraic number fields are usually studied in terms of class field theory and Galois cohomology, cf. [3, 4, 5, 6, 8, 11, 12, 19, 20]. The p-ranks of class groups are of particular interest since they are fundamental for the algebraic properties of the underlying number field, see [3, 8, 17]. Lower bounds on p-ranks of class groups are particularly desirable. For example, in view of the celebrated result of Golod and Shafarevic [7], such bounds can be used to show that certain number fields have infinite class field towers.

In this paper, we will use a different approach: In order to get class group estimates, we consider certain ideals above ramified prime ideals in CM-fields and show by elementary methods that these ideals are nonprincipal. The main idea of the proof is to show that principal ideals often necessarily have to lie in a quite small subfield of the underlying CM-field. This method of "field descent" already has been used successfully by the author for the study of combinatorial problems involving cyclotomic integers [18]. Our approach here will give us explicit subgroups of class groups of CM-fields. As a consequence, we will get lower bounds on p-ranks of class groups which are comparable to a bound obtained by Schoof [19, Prop. 3.1]. Schoof's result is more general, but it seems that our bounds are stronger in some cases. As examples for the application of our bound, we give simple explicit sufficient conditions for cyclotomic fields to have infinite p-class field towers.

2 Preliminaries

In this section, we introduce some notation and state some well known results we need later. Throughout this paper, we use the notation $\xi_t := \exp 2\pi i/t$ and write $\mathrm{ord}_m(a)$ for the multiplicative order of a modulo m. The Euler totient function is denoted by φ. The following is a basic lemma on the structure of the group of units of $\mathbb{Z}/p^b\mathbb{Z}$, see [10].

Lemma 2.1 *Let p be a prime, and let b be a positive integer such that $(p,b) \neq (2,1)$. If s is an integer satisfying $s \equiv 1 \pmod{p^b}$ and $s \not\equiv 1 \pmod{p^{b+1}}$ then $\mathrm{ord}_{p^c}(s) = p^{c-b}$ for all $c \geq b$.*

The following lemma of Kronecker's is an essential tool for most results of this paper. See [2, Section 2.3, Thm. 2] for a proof.

Lemma 2.2 *An algebraic integer all of whose conjugates have absolute value* 1 *is a root of unity.*

Note that Lemma 2.2 implies that any cyclotomic integer of absolute value 1 must be a root of unity since the Galois group of a cyclotomic field is abelian.
Now we recall some facts on CM-fields, see [20, p. 38].

Lemma 2.3 *Let* K *be a* CM*-field, i.e.,* $K = K^+(\sqrt{\alpha})$ *where* K^+ *is totally real and* $\alpha \in K^+$ *is totally negative.*
a) Complex conjugation induces an automorphism of K *which is independent of the imbedding of* K *in* $\mathbb{C}$*, i.e.,*

$$\alpha^{-1}(\overline{\alpha(x)}) = \beta^{-1}(\overline{\beta(x)})$$

for all $x \in K$ *and all imbeddings* α, β *of* K *in* $\mathbb{C}$*.*
b) We have $\alpha(\overline{x}) = \overline{\alpha(x)}$ *for all* $x \in K$ *and all imbeddings* α *of* K *in* $\mathbb{C}$*.*
c) If ε *is a unit in* K *of modulus* 1*, then* ε *is a root of unity.*

We remark that part c of Lemma 2.3 follows from part b and Kronecker's Lemma 2.2. The following are standard results on ideal factorization in cyclotomic fields. See [1, XI.§15] for easily accessible proofs.

Result 2.4 *Let* m *be a positive integer, and let* p *be a prime. Write* $m = p^a m'$ *with* $(m', p) = 1$ *and* $a \geq 0$*. Then* p *factors in* $\mathbb{Q}(\xi_m)$ *as*

$$(p) = \prod_{i=1}^{t} \pi_i^{\varphi(p^a)}$$

where $t = \varphi(m')/\mathrm{ord}_{m'}(p)$*, and the* π_i *are distinct prime ideals.*
Furthermore, the decomposition group of each P_i *consists exactly of those* $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ *for which there is an integer* j *such that*

$$\sigma(\xi_{m'}) = \xi_{m'}^{p^j}.$$

3 The fixing theorem

Let I be a principal ideal of a number field K. It will turn out that it is very useful to have conditions telling us if I can be generated by an element of a certain subfield of K. We call this the **field descent problem**. The study of the following *fixing problem* will help us finding answers to the field descent problem.

Problem 3.1 (Fixing Problem) *Let σ be an automorphism of a number field K, and let*

$$T := \{X \in K : X^\sigma = \varepsilon X \text{ for some root of unity } \varepsilon\}.$$

Is there, for every $X \in T$, a root of unity $\delta_X \in K$ such that $X\delta_X$ remains fixed by σ?

Actually, we will be able to do more than solving the fixing problem. Namely, we will determine a root of unity η only depending on K with the following property. For every $X \in T$ there is a root of unity $\delta_X \in K$ such that $(X\delta_X)^\sigma/(X\delta_X)$ is a power of η. In many cases, we will have $\eta = 1$ which means that the answer to the fixing problem is positive.
However, the answer to the fixing problem is not always positive. To see this, we consider the example of Gauss sums. Let p be an odd prime, and denote the finite field of order p by $\mathbb{F}_p$. We consider a Gauss sum $G(\chi) = \sum_{x\in\mathbb{F}_p^*} \chi(x)\xi_p^x$ where χ is a nontrivial character of $\mathbb{F}_p^*$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_{p(p-1)})/\mathbb{Q})$ be defined by $\sigma(\xi_{p-1}) = \xi_{p-1}$ and $\sigma(\xi_p) = \xi_p^a$ where a is a primitive root modulo p. Then

$$\begin{aligned} G(\chi)^\sigma &= \sum_{x\in\mathbb{F}_p^*} \chi(x)\xi_p^{ax} \\ &= \sum_{x\in\mathbb{F}_p^*} \chi(a^{-1}x)\xi_p^{x} \\ &= \chi(a^{-1})G(\chi). \end{aligned}$$

If the answer to the fixing problem was positive for the chosen σ, then $(G(\chi)\xi_p^i\xi_{p-1}^j)^\sigma = G(\chi)\xi_p^i\xi_{p-1}^j$ for some i, j. This implies $\chi(a^{-1})\xi_p^{ai}\xi_{p-1}^j = \xi_p^i\xi_{p-1}^j$ and thus $\xi_p^{(a-1)i} = \chi(a)$. But this is impossible since $\chi(a) \neq 1$ is a $(p-1)$th root of unity.

The following theorem in particular provides sufficient conditions for a positive answer to the fixing problem. In many cases, our conditions are also necessary as can be seen through the example of Gauss sums. One look at these conditions shows that they are messy. However, these are just numerical conditions which are easy to check for any given instance. As we will see later, this result is very useful for the study of class groups of CM-fields.

For a prime p and an integer x, let x_p be the p-part of x, i.e., $x = x_p x'$ where x_p is a power of p and $(x', p) = 1$.

Theorem 3.2 (Fixing Theorem) *Let K be an algebraic number field, and let σ be an automorphism of K of order y. Let $\mathbb{Q}(\xi_m)$, $m \not\equiv 2 \pmod 4$, be the largest cyclotomic field contained in K. Define t by $\sigma(\xi_m) = \xi_m^t$. Let S be the set of rational primes dividing m. Let*

$$T_{odd} := \{p \in S : p \text{ odd},\ t \equiv 1 \pmod p),\ y_p > \mathrm{ord}_{m_p}(t)\}$$

and

$$T := \begin{cases} T_{odd} \cup \{2\} & \text{if } t \equiv 1 \pmod 4 \text{ and } y_2 > \mathrm{ord}_{m_2}(t), \\ T_{odd} & \text{otherwise.} \end{cases}$$

Define

$$f(m,\sigma) := \begin{cases} 2 \gcd(m, \prod_{p\in T} y_p) & \text{if } \ m \text{ is odd and } y \text{ is even}, \\ m_2 \gcd(m, \prod_{p\in T} y_p) & \text{if } \ m \text{ is even},\ t \equiv 3 \pmod 4 \\ & \text{and } 2m_2 \text{ divides } t^y - 1, \\ \gcd(m, \prod_{p\in T} y_p) & \text{otherwise.} \end{cases}$$

If

$$X^\sigma = \varepsilon X \tag{1}$$

for $X \in K$ and some root of unity ε, then there is an mth root of unity α and an $f(m,\sigma)$th root of unity η with

$$(X\alpha)^\sigma = \eta(X\alpha).$$

Proof Since ε is a root of unity in K, we have $\varepsilon = \pm\xi_m^j$ for some j. Thus $\varepsilon^\sigma = \varepsilon^t$. Write $\varepsilon = \delta \prod_{p\in S} \lambda_p$ where each λ_p is m_pth root of unity and $\delta = \pm 1$. We choose $\delta = 1$ if m is even. We apply σ to (1) repeatedly $y - 1$

times and get $\varepsilon^{(t^y-1)/(t-1)} = 1$. Since we have chosen $\delta = 1$ if m is even, this implies

$$\delta^y = 1, \tag{2}$$

and

$$\lambda_p^{\frac{t^y-1}{t-1}} = 1 \tag{3}$$

for all $p \in S$.

Claim 1: If $p \in S$ is odd and $t \equiv 1 \pmod p$ or $p = 2$ and $t \equiv 1 \pmod 4$, then

$$y_p \;\;||\;\; \frac{t^y - 1}{t - 1}. \tag{4}$$

Proof of Claim 1: Define b by $p^b \,||\, t-1$. By Lemma 2.1, we have $\mathrm{ord}_{y_p p^b}(t^y) = \mathrm{ord}_{y_p p^b}(t)/y_p = y_p/y_p = 1$ and $\mathrm{ord}_{y_p p^{b+1}}(t^y) = p$. Thus $y_p p^b \,||\, t^y - 1$ and the claim follows.

Claim 2: Let $p \in S \setminus T$. If p is odd or $p = 2$ and $t \equiv 1 \pmod 4$, then there is a solution i_p to

$$\xi_{m_p}^{i_p(t-1)} = \lambda_p^{-1}. \tag{5}$$

Proof of Claim 2: If $t \not\equiv 1 \pmod p$, then (5) certainly has a solution since λ_p is a m_pth root of unity. Thus we may assume $t \equiv 1 \pmod p$. Then $\mathrm{ord}_{m_p}(t)$ is a power of p and thus divides y_p. Using the definition of T, we conclude $\mathrm{ord}_{m_p}(t) = y_p$. If $y_p = 1$, then by (3) and (4), we get $\lambda_p = 1$ and hence (5) has a solution. Thus we may assume $y_p > 1$. Again define b by $p^b \,||\, t-1$. Since $t \equiv 1 \pmod p$ and $\mathrm{ord}_{m_p}(t) = y_p > 1$, we have $p \le p^b < m_p$. From Lemma 2.1 we infer $y_p = \mathrm{ord}_{m_p}(t) = m_p/p^b$. Thus, by (3) and (4), we get $\lambda_p^{m_p/p^b} = 1$. This shows that (5) has a solution since $\xi_{m_p}^{t-1}$ is a primitive p^{m_p/p^b}th root of unity. Thus Claim 2 is proven.

Claim 3: Let m be even, $t \equiv 3 \pmod 4$ and assume that $2m_2$ does not divide $t^y - 1$. Then (5) has a solution for $p = 2$.

Proof of Claim 3: Since m_2 divides $t^y - 1$, we have $m_2 || t^y - 1$. Since $2 \mid\mid t-1$, we get $(m_2/2) \mid\mid (t^y - 1)/(t-1)$. Thus, by (3) and (4), we get $\lambda_2^{m_2/2} = 1$. Thus (5) has a solution since $\xi_{m_2}^{t-1}$ is a primitive $2^{m_2/2}$th root of unity. This proves Claim 3.

Claim 4: Let U be the set of primes p in S for which (5) has a solution i_p. Let $\gamma := \prod_{p\in U} \xi_{m_p}^{i_p}$. Then

$$(X\gamma)^\sigma = \left(\delta \prod_{p\in S\setminus U} \lambda_p\right)(X\gamma). \tag{6}$$

Proof of Claim 4: This is a straightforward calculation using $X^\sigma = \varepsilon X$, $\varepsilon = \delta \prod_{p\in S} \lambda_p$ and (5).

Claim 5: $\omega := \delta \prod_{p\in S\setminus U} \lambda_p$ is an $f(m, \sigma)$th root of unity.
Proof of Claim 5: First let p be odd. If $p \in S \setminus U$, then $p \in T$ by Claim 2. Furthermore, by (3) and (4), we get $\lambda_p^{y_p} = 1$. Thus, by the definition of $f(m, \sigma)$, we have

$$\left(\prod_{p\in S\setminus\{U\cup\{2\}\}} \lambda_p\right)^{f(m,\sigma)} = 1.$$

Now consider $p = 2$. If $2 \in S \setminus U$, then by Claims 2 and 3 we have $2 \in T$ and $t \equiv 1 \pmod 4$ or $t \equiv 3 \pmod 4$ and $2m_2$ divides $t^y - 1$. In both cases, the definition of $f(m, \sigma)$ together with (3) and (4) make sure that $\lambda_2^{f(m,\sigma)} = 1$. Summing up, we have shown $(\omega\delta)^{f(m,\sigma)} = 1$. It remains to show $\delta^{f(m,\sigma)} = 1$. For even m we have $\delta = 1$, i.e., in this case, there is nothing to show. Let m be odd. If y is odd, too, then $\delta = 1$ by (2) and we are done. If y is even, then $f(m, \sigma)$ is even by definition and thus $\delta^{f(m,\sigma)} = 1$. This proves Claim 5.

Conclusion of the proof: The assertion of the Theorem follows from Claims 4 and 5. We take $\alpha = \gamma$ and $\eta = \omega$. □

In the next section, we will use the following consequence of the fixing theorem for the study of class groups of CM-fields. For a Galois automorphism σ, we denote the fixed field of σ by Fix σ.

Corollary 3.3 *Let K/k be a Galois extension of number fields, and let $\mathbb{Q}(\xi_m)$, $m \not\equiv 2 \pmod 4$, be the largest cyclotomic field contained in K. If $X^\sigma = \varepsilon X$ for $X \in K$, $\sigma \in \mathrm{Gal}(K/k)$ and some root of unity ε, then there is a root of unity $\alpha \in K$ such that $(X\alpha)^\sigma/(X\alpha)$ is an $f(m,\sigma)$th root of unity. In particular,*

$$(X\alpha)^{f(m,\sigma)} \in \mathrm{Fix}\ \sigma.$$

The following property of the function f defined in Theorem 3.2 is important.

Lemma 3.4 *Let $f(m,\sigma)$ be the function defined in Theorem 3.2, and let p be a prime not dividing the order of σ. Then p does not divide $f(m,\sigma)$.*

Proof Denote the order of σ by y. If p is odd and divides $f(m,\sigma)$, then p divides y by the definition of f. Now let $p = 2$. If y is odd, then $f(m,\sigma) | \gcd(m,y)$ by the definition of f. Thus $f(m,\sigma)$ is odd, too. □

4 Explicit subgroups of class groups of CM-fields

Now we turn our attention to class groups of CM-fields. We will use the idea of the "field descent" to obtain some explicit subgroups of class groups of CM-fields. The idea of the field descent is as follows. Let K be a CM-field, and let σ be a Galois automorphism of K. Under some conditions, the fixing theorem shows that many principal ideals invariant under σ actually must be ideals of the subfield Fix σ. Since most ideals of K are *not* ideals of Fix σ, this will imply that many ideals of K invariant under σ are *nonprincipal*. These ideals correspond to primes ramified in $K/\mathrm{Fix}\ \sigma$ and can be determined explicitly. We illustrate our strategy by a quick example. We will show that the prime ideals above p in $\mathbb{Q}(\xi_{4p})$, $p \equiv 1 \pmod 4$, $p > 5$ prime, are nonprincipal.

Example 4.1 Let $K = \mathbb{Q}(\xi_{4p})$ where $p \equiv 1 \pmod 4$ is a prime. Then $(p) = (P\overline{P})^{p-1}$ where P is a prime ideal of K by Result 2.4. Assume that P is principal with generator $g \in \mathbb{Z}[\xi_{4p}]$. Let a be a primitive root mod p, and define $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ by $\xi_p \mapsto \xi_p^a$ and $i \mapsto i$. Then $P^\sigma = P$ by Result 2.4. Let $X := pg/\overline{g}$. Then X is an algebraic integer and $(X) = (X^\sigma)$. Thus

$X^\sigma = \varepsilon X$ for some unit ε of K. Also, $|X^\sigma|^2 = X^\sigma \overline{X^\sigma} = (X\overline{X})^\sigma = (p^2)^\sigma = p^2 = |X|^2$. Thus $|\varepsilon| = 1$ and Kronecker's lemma shows that ε is a root of unity. For the function f in Theorem 3.2, we get $f(4p, \sigma) = \gcd(4p, 4) = 4$. Thus $(X\eta)^4 \in \mathrm{Fix}\ \sigma = \mathbb{Q}(i)$ for some root of unity $\eta \in K$ by Theorem 3.2. But this implies that $P^4/\overline{P^4} = (X^4/p^4)$ is an ideal of $\mathbb{Q}(i)$ which is not true for $p > 5$. This shows that P is a nonprincipal ideal of K for $p > 5$. $\square$

Now we come to the formulation of our general result. For a group G and $g \in G$, we denote the order of g in G by $\mathrm{ord}(g)$. The ideal class group of a number field K is denoted by Cl_K. For a set L of ideals of a number field, we write $\overline{L} = \{\overline{I} : I \in L\}$ where the bar denotes the complex conjugation. The following is the main result of this paper.

Theorem 4.2 *Let K be a CM-field, and let k be a complex subfield of K such that K/k is Galois. Let $\mathbb{Q}(\xi_m)$, $m \not\equiv 2 \pmod 4$, be the largest cyclotomic field contained in K.*
Let $D := \mathrm{Gal}(K/k)$, and let $\{\sigma_1, ..., \sigma_s\}$ be a set of generators for D. Let $\mathcal{T}$ be a set of primes of k with $\mathcal{T} \cap \overline{\mathcal{T}} = \emptyset$. Denote the ramification index of $P \in \mathcal{T}$ in K/k by $R(P)$.
Then the ideal class group Cl_K of K contains a subgroup L isomorphic to Ω/Λ where

$$\Omega := \bigoplus_{P \in \mathcal{T}} (\mathbb{Z}/R(P)\mathbb{Z})$$

and Λ is a subgroup of Ω isomorphic to a subgroup of $\bigoplus_{i=1}^{s} (\mathbb{Z}/\lambda_i\mathbb{Z})$ where $\lambda_i = \mathrm{lcm}(f(m, \sigma_j), j = i, ..., s)$. Here f is the function defined in Theorem 3.2.
Moreover, L is contained in the subgroup of Cl_K generated by the primes of K above primes in $\mathcal{T}$.

Proof We first need some notation. Write $\mathcal{S} := \mathcal{T} \cup \overline{\mathcal{T}}$. Write $R(P) = R(\overline{P})$ for $P \in \overline{\mathcal{T}}$. We have $P = P_K^{R(P)}$ for $P \in \mathcal{S}$ where each P_K is an ideal of K. The ideals P_K are not necessarily prime ideals. For the convenience of the reader, we give a table of the notations we need for this proof. All occurring ideals are viewed as ideals of K.

$$
\begin{array}{rcl}
K: & & CM\text{-field} \\
K/k: & & \text{Galois extension, } k \text{ complex} \\
D: & = & \mathrm{Gal}(K/k) \\
\mathcal{T}: & = & \text{a set of primes of } k \text{ with } \mathcal{T} \cap \overline{\mathcal{T}} = \emptyset \\
\mathcal{S}: & = & \mathcal{T} \cup \overline{\mathcal{T}} \\
R(P): & & \text{the ramification index of } P \in \mathcal{S} \text{ in } K/k \\
P_K: & & \text{the ideal of } K \text{ with } P_K^{R(P)} = P,\ P \in \mathcal{S} \\
\Gamma: & & \text{the group of all ideals of } K \\
H: & & \text{the group of all principal ideals of } K \\
I: & = & \text{the subgroup of } \Gamma \text{ generated by the ideals } P_K,\ P \in \mathcal{S} \\
I^*: & = & \text{the subgroup of } I \text{ generated by the ideals } P_K,\ P \in \mathcal{T} \\
R: & = & \{J\overline{J} : J \in I\} \\
I_k: & = & \text{the subgroup of } I \text{ generated by the ideals in } \mathcal{S} \\
K_{\mathcal{S}}: & = & \{Y/\overline{Y} : Y \in K, (Y/\overline{Y}) \in I\} \\
\mathcal{Z}: & & \text{the subgroup of } I \text{ generated by } (Y_1), ..., (Y_s) \\
& & \text{(the } Y_i \text{ are defined below)} \\
W: & = & \{J \in I : J/\overline{J} \in \mathcal{Z} I_k\}.
\end{array}
$$

Claim 1: Let $X \in K_{\mathcal{S}}$. Then X^σ/X is a root of unity for all $\sigma \in D$.

Proof of Claim 1: Note that $|X| = 1$ for all $X \in K_{\mathcal{S}}$. Since σ fixes all ideals in I, we have $(X^\sigma) = (X)$. Thus $X^\sigma = \varepsilon X$ for some unit ε. But, since complex conjugation commutes with σ, we have $|\varepsilon|^2 = (X^\sigma/X)\overline{(X^\sigma/X)} = (|X|^2)^\sigma/|X|^2 = 1/1 = 1$. Thus ε is a root of unity by Lemma 2.3 c. This proves Claim 1.

Now we define some useful elements Y_i of K. Recall $D = \langle \sigma_1, ..., \sigma_s \rangle$. Define $F_1 := K_{\mathcal{S}}$ and $F_i := K_{\mathcal{S}} \cap \mathrm{Fix}\ \langle \sigma_1, ..., \sigma_{i-1} \rangle$ for $i = 2, ..., s+1$. For a root of unity ε, we write $\mathrm{ord}(\varepsilon)$ for the order of ε. Note that Y^{σ_i}/Y is a root of unity for all $Y \in F_i$ and $i = 1, ..., s$ by Claim 1 a. For $i = 1, ..., s$, let Y_i be an element of F_i such that

$$\mathrm{ord}(\frac{Y_i^{\sigma_i}}{Y_i}) = \max\{\mathrm{ord}(\frac{Y^{\sigma_i}}{Y}) : Y \in F_i\}.$$

Write $\eta_i := Y_i^{\sigma_i}/Y_i$. Note that

$$(7) \qquad \operatorname{ord}(\frac{Y^{\sigma_i}}{Y}) \text{ divides } \operatorname{ord}(\eta_i)$$

for all i and all $Y \in F_i$.

Claim 2:
a) Let $\mathcal{Z}$ be the subgroup of I generated by $(Y_1), ..., (Y_s)$. If $X \in K_{\mathcal{S}}$, then $(X) \in \mathcal{Z} I_k$.
b) Let $\lambda_i = \operatorname{lcm}(f(m, \sigma_j), j = i, ..., s)$. Then the ideal $(Y_i)^{\lambda_i}$ is an ideal of k, $i = 1, ..., s$.

Proof of Claim 2: a) Assertion a is proven if we can find an element $Y \in K$ with $(Y) \in \mathcal{Z}$ such that $XY \in k$. We recursively construct Y as follows. Define $X_1 := X$. Let $X_i \in F_i$, $1 \leq i \leq s$, be given. Then $X_i^{\sigma_i} = \eta_i^{j_i} X_i$ for some j_i by (7) and

$$X_{i+1} := X_i Y_i^{-j_i} \in \text{Fix } \sigma_i$$

since $(Y_i^{-j_i})^{\sigma_i} = \eta_i^{-j_i} Y_i^{-j_i}$. As $X_i, Y_i \in F_i$, we get $X_{i+1} \in F_{i+1}$. So we have $X_{s+1} = X \prod_{i=1}^{s} Y_i^{-j_i} \in F_{s+1} = k$. Thus we may choose $Y = \prod_{i=1}^{s} Y_i^{-j_i}$ proving part a.
b) Recall $D = \operatorname{Gal}(K/k) = \langle \sigma_1, ..., \sigma_s \rangle$. Fix an $i \in \{1, ..., s\}$. Recall $Y_i \in \text{Fix } \langle \sigma_1, ..., \sigma_{i-1} \rangle$. By Claim 1 a and Corollary 3.3, there is a root of unity α_i in $\text{Fix } \langle \sigma_1, ..., \sigma_{i-1} \rangle$ such that $(Y_i \alpha_i)^{\lambda_i} \in \text{Fix } \langle \sigma_1, ..., \sigma_i \rangle$. Again by Corollary 3.3, there is a root of unity α_{i+1} in $\text{Fix } \langle \sigma_1, ..., \sigma_i \rangle$ such that $(Y_i \alpha_i \alpha_{i+1})^{\lambda_i} \in \text{Fix } \langle \sigma_1, ..., \sigma_{i+1} \rangle$. Proceeding in this way, we see that there is a root of unity $\alpha \in K$ such that $(Y_i \alpha)^{\lambda_i} \in \text{Fix } \langle \sigma_1, ..., \sigma_s \rangle = k$. This shows that $(Y_i^{\lambda_i})$ is an ideal of k and concludes the proof of Claim 2.

Claim 3: We have $A \leq W$ for

$$\begin{aligned} A : &= I \cap I_k R H, \\ W : &= \{ J \in I : J/\overline{J} \in \mathcal{Z} I_k \}. \end{aligned}$$

Proof of Claim 3: Let $X \in A$, say $X = i_k r(h)$ with $i_k \in I_k$, $r \in R$ and $h \in K$. Then $h/\overline{h} \in K_{\mathcal{S}}$ and thus $(h/\overline{h}) \in \mathcal{Z} I_k$ by Claim 2. Thus $X/\overline{X} = (h/\overline{h})(i_k/\overline{i_k}) \in \mathcal{Z} I_k$ and hence $X \in W$ proving Claim 3.

Claim 4: Write $(Y_i) = A_i/\overline{A_i}$ with $A_i \in I^*$. Let $\mathcal{Z}^*$ be the subgroup of I^* generated by $A_1, ..., A_s$. Then

$$W = \mathcal{Z}^* R I_k.$$

Proof of Claim 4: From the definitions, we have $\mathcal{Z}^* R I_k \subset W$. It remains to show $W \subset \mathcal{Z}^* R I_k$. Let $X \in W$ be arbitrary. Write $X = a\overline{b}$ with $a, b \in I^*$. Then $X/\overline{X} = (a/b)(\overline{b}/\overline{a}) \in \mathcal{Z} I_k$ and thus $a/b \in \mathcal{Z}^* I_k$. Hence $X = a\overline{b} = (a/b)(b\overline{b}) \in \mathcal{Z}^* I_k R$ concluding the proof of Claim 4.

Claim 5: The group W/RI_k is isomorphic to a subgroup of $\bigoplus_{i=1}^{s}(\mathbb{Z}/\lambda_i\mathbb{Z})$.

Proof of Claim 5: By Claim 4, W/RI_k is generated by $A_i R I_k$, $i = 1, ..., s$. Recall that $(Y_i) = A_i/\overline{A_i}$ and $(Y_i)^{\lambda_i} \in I_k$ by Claim 2 b. This implies $A_i^{\lambda_i} \in I_k$ and thus the assertion.

Claim 6: $IRH/I_k RH$ has a factor group isomorphic to I/W.

Proof of Claim 6: Since $IRH/I_k RH \cong I/I \cap I_k RH$, the assertion follows from Claim 3.

Claim 7: Let $\Omega = \bigoplus_{P \in \mathcal{T}}(\mathbb{Z}/R(P)\mathbb{Z})$. Then

$$I/W \cong \Omega/U$$

where U is a subgroup of Ω isomorphic to a subgroup of $\bigoplus_{i=1}^{s}(\mathbb{Z}/\lambda_i\mathbb{Z})$.

Proof of Claim 7: This follows from $I/W \cong (I/RI_k)/(W/RI_k)$ and Claim 5 since $(I/RI_k) \cong \bigoplus_{P \in \mathcal{T}}(\mathbb{Z}/R(P)\mathbb{Z})$.

Conclusion of the proof of Theorem 4.2: From Claims 6 and 7 we know that $IRH/I_k RH$ has a factor group and thus a subgroup isomorphic to Ω/U. This implies the assertion of the theorem. $\Box$

In the following, the q-rank of a group G is denoted by $d_q G$.

Corollary 4.3 *Let q be a prime. In the situation of Theorem 4.2, the following hold.*

a) Let q be a prime, and let R_q be the number of $R(P)$s divisible by q. Then

$$d_q Cl_K \geq R_q - d_q D.$$

b) If m and $|D|$ are odd and relative prime, then Cl_K contains a subgroup isomorphic to

$$\bigoplus_{P \in \mathcal{T}} (\mathbb{Z}/R(P)\mathbb{Z}).$$

Proof a) By Theorem 4.2, we have $d_q Cl_K \geq R_q - N_q$ where N_q is the number of λ_i's divisible by q. Write $d := d_q D$. We may choose the generators σ_i of D such that the orders of $\sigma_{d+1}, ..., \sigma_s$ are not divisible by q. By Lemma 3.4, this implies that $\lambda_{d+1}, ..., \lambda_s$ also are not divisible by q. Thus $N_q \leq d$, and part a follows.
b) In this situation, we have $f(m, \sigma) = 1$ for all $\sigma \in D$, and thus $\lambda_i = 1$ for all i. Thus the assertion follows from Theorem 4.2. $\Box$

Note that in Theorem 4.2, the group D cannot contain the complex conjugation since it does not fix the occuring prime ideals of k. However, in the case where D consists only of the complex conjugation and the identity, we can prove the following analogon to Theorem 4.2. As we will explain later, we will end up in recovering a special case of a result of Martinet [13].

Theorem 4.4 *Let K be a CM-field with maximal real subfield K^+ and ideal class group Cl_K. Let r be the number of finite primes ramified in K/K^+. Then*

$$d_2 Cl_K \geq r - 1.$$

Proof Let I be the ideal group of K generated by the primes above the primes of K^+ ramified in K/K^+. Then $I^2 = \{J^2 : J \in I\}$ is the subgroup of the ideals in I which are ideals of K^+. Let $X \in K$ with $(X) \in I$. Then $\overline{X} = \varepsilon_X X$ for some unit ε since all ideals in I are invariant under complex conjugation. From Lemma 2.3 we know that ε_X is a root of unity since $|\varepsilon_X| = 1$. We choose an $X \in K$ such that the order of ε_X is maximum. Then, for every $Y \in K$ with $(Y) \in I$, there is a j such that $\overline{X^j Y} = X^j Y$ and thus $(X^j Y) \in I^2$. Let H respectively H_I be the group of all principal ideals of K respectively all principal ideals in I. Then, by what we have seen, $H_I \leq I^2 \langle (X) \rangle$ and thus $I^2 H_I \leq I^2 \langle (X) \rangle$. Note that $I/I^2 \cong (\mathbb{Z}/2Z)^r$ and that $\langle (X) I^2 / I^2 \rangle$ is of order at most 2. Thus $d_2 IH/I^2 H = d_2 I/I^2 H_I \geq r - 1$.
$\Box$

5 Application to p-ranks and class field towers

In this section, we use the field descent method to obtain some lower bounds on p-ranks of ideal class groups of CM-fields. We also explain the connection of these results to infinite class field towers. There is a vast literature on these problems. One of the most useful lower bounds on p-ranks of ideal class groups is due to Schoof [19]. We will obtain a similar bound which only is applicable to CM-fields, but apparently is stronger in some cases.
The p-ranks of ideal class groups of number fields play an important role in algebraic number theory, see [3, 17, 19, 20], for instance. In particular, lower bounds on p-ranks of class groups are desirable. One of the reasons for the interest in these lower bounds is the connection to the problem of class field towers. We give a quick review of the basics on class field towers.
Let K be an algebraic number field. Define $K_0 := K$ and for $n = 1, 2, ...$ let K_{n+1} be the Hilbert class field respectively the p-Hilbert class field of K_n for some prime p (see [3] for the terminology). Then

$$K_0 \subset K_1 \subset K_2 \subset \cdots$$

is called the **class field tower** respectively the **p-class field tower** of K. Such a class field tower is called **finite** if $\bigcup_{n=0}^{\infty} K_n$ is a finite extension of K and **infinite** otherwise. The existence of infinite class field towers had been conjectured for several decades and finally was proven by Golod and Shavarevic [7]. The following refinement of their result can be found in [3].

We first introduce some notation. By E_K respectively Cl_K we denote the group of units respectively the ideal class group of an algebraic number field K. For a prime p and a finitely generated abelian group G, we write $d_pG := \dim_{\mathbb{F}_p} G/pG$.

Result 5.1 *Let K be an algebraic number field, and let p be a prime. If*

$$d_pCl_K \geq 2 + 2\sqrt{d_pE_K + 1},$$

then K has an infinite p-class tower and thus an infinite class field tower.

The value of d_pE_K can be determined by Dirichlet's unit theorem (see [2]). Thus the essential step for the application of Result 5.1 is to find lower bounds for d_pCl_K. Many results in this direction are known, see [3], for instance. We will compare our results to a lower bound on d_pCl_K due to Martinet [13] and Schoof [19].

Result 5.2 (Martinet) *Let K/k be a cylic extension of algebraic number fields of prime degree p. Then*

$$d_pCl_K \geq \rho - d_pE_k - 1$$

where ρ is the number of finite and infinite primes of k ramified in K/k.

Martinet's Result [13] implies our Theorem 4.4 as can be seen as follows. Let K be a CM-field as in Theorem 4.4 and let $k = K^+$. The number of infinite primes of k ramified in K/k is $[k : \mathbb{Q}]$. Moreover, by Dirichlet's unit theorem (see [2]), we have $d_2E_k = [k : \mathbb{Q}]$. Thus Theorem 5.2 indeed shows that

$$d_2Cl_K \geq r + [k : \mathbb{Q}] - [k : \mathbb{Q}] - 1 = r - 1.$$

The following generalization of Result 5.2 was obtained by Schoof [19]. For the formulation of this result, we need some notation. For a group G, the commutator subgroup of G is denoted by $[G, G]$. Let K be an algebraic number field. We write U_K for the group of idèle units of K, i.e. the K-idèles which have trivial valuation at all finite places. For the definition of the cohomology groups we use, see [15, I §2].

Result 5.3 (Schoof) *Let K/k be a Galois extension of algebraic number fields of with Galois group D. Then*

$$d_pCl_K \geq d_p\hat{H}^0(D, U_K) - d_pD/[D, D] - d_pE_k/(E_k \cap NU_K).$$

Remark 5.4 In order to compare Result 5.3 with our method, we need to derive a simplified bound from 5.3 which can be calculated explicitly for our examples. Let K/k be a Galois extension of algebraic number fields with abelian Galois group D. Let S be the set of all (finite and infinite) primes of K and let S_∞ denote the set of infinite primes of K. For $\mathfrak{p} \in S$ let $K_\mathfrak{p}$ denote the completion of K with respect to a fixed prime $\mathfrak{P}$ of K above $\mathfrak{p}$. For $\mathfrak{p} \in S \setminus S_\infty$ let $U_\mathfrak{p}$ denote the ring of units of $K_\mathfrak{p}$ and write $T_\mathfrak{p}$ for the inertia group of $\mathfrak{P}$ in K/k.

By the same argument as in the proof of [15, 8.1.2], we have

$$\hat{H}^0(D,U_K) \cong \bigoplus_{\mathfrak{p}\in S\setminus S_\infty} \hat{H}^0(\mathrm{Gal}(K_\mathfrak{p}/k_\mathfrak{p}),U_\mathfrak{p}) \oplus \bigoplus_{\mathfrak{p}\in S_\infty} \hat{H}^0(\mathrm{Gal}(K_\mathfrak{p}/k_\mathfrak{p}),K_\mathfrak{p})$$

Since $K_\mathfrak{p}=\mathbb{R}$ or $K_\mathfrak{p}=\mathbb{C}$ for $\mathfrak{p}\in S_\infty$, we know that $\bigoplus_{\mathfrak{p}\in S_\infty} \hat{H}^0(\mathrm{Gal}(K_\mathfrak{p}/k_\mathfrak{p}),K_\mathfrak{p})$ is a (possibly trivial) elementary abelian 2-group. Furthermore, by [14, Thm. 6.2] we have $\hat{H}^0(\mathrm{Gal}(K_\mathfrak{p}/k_\mathfrak{p}),U_\mathfrak{p})\cong T_\mathfrak{p}$ for $\mathfrak{p}\in S\setminus S_\infty$.

Let r be an odd prime and assume that k does not contain the rth roots of unity. Let $\mathcal{R}$ be the set of finite primes of k ramified in K/k. Since $T_\mathfrak{p}=1$ if $\mathfrak{p}$ is unramified in K/k, we get

$$d_r\hat{H}^0(D,U_K)=\sum_{\mathfrak{p}\in\mathcal{R}} d_rT_\mathfrak{p}.$$

Since we assume that K/k is an abelian extension, Schoof's result implies

$$d_rCl_K \geq \sum_{\mathfrak{p}\in\mathcal{R}} d_rT_\mathfrak{p} - d_rD - s - t + 1 \tag{8}$$

where s respectively t is the number of real respectively complex embeddings of k.

From Theorem 4.2, we get a bound similar to Schoof's result. Our result only holds for CM-fields, but as a compensation sometimes gives slightly stronger bounds.

Corollary 5.5 *Let K be a CM-field, and let k be a subfield of K such that K/k is Galois with Galois group D. Let p be a rational prime, and let ω be the number of finite primes of k which are not invariant under complex conjugation and whose ramification index in K/k is divisible by p. Then*

$$d_pCl_K \geq \frac{\omega}{2} - \varepsilon$$

where $\varepsilon = d_pD$ if K contains the pth roots of unity and $\varepsilon=0$ otherwise.

Proof Corollary 4.3 a implies $d_pCl_K\geq \omega/2 - d_pD$. If K does not contain the pth roots of unity, then $f(m,\sigma)$ is not divisible by p for all $\sigma\in D$ by the definition of f. Thus $d_pCl_K\geq\omega/2$ in this case by Thereom 4.2. This proves the assertion. □

Example 5.6 Let $m = 259 = 7 \cdot 37$ and let k be the unique subfield of $K := \mathbb{Q}(\xi_m)$ of degree 8 over $\mathbb{Q}$. Since $\mathrm{ord}_7(37) = 3$ and $\mathrm{ord}_{37}(7) = 9$ we have $(7) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ and $(37) = \mathfrak{q}_1\mathfrak{q}_2$ over k where the $\mathfrak{p}_i$'s and $\mathfrak{q}_i$'s are prime ideals of k which are not invariant under complex conjugation. Using the notation of Remark 5.4, we have $T_{\mathfrak{p}_i} \cong \mathbb{Z}/3\mathbb{Z}$ and $T_{\mathfrak{q}_i} \cong \mathbb{Z}/9\mathbb{Z}$. Hence (8) implies

$$d_3 Cl_K \geq 6 - d_3 \mathrm{Gal}(K/k) - 3 + 1 = 6 - 2 - 3 + 1 = 2.$$

On the other hand, Corollary 5.5 implies

$$d_p Cl_K \geq \frac{\omega}{2} = 3.$$

Hence Corollary 5.5 gives a slightly stronger bound than (8). It might be possible to improve (8) by finding a better upper bound for $d_3 E_k/(E_k \cap NU_K)$, but this seems difficult.

Corollary 5.7 *Let K be a CM-field, and let k be a subfield of K such that K/k is a Galois extension of prime degree p. Let ω be the number of primes of k ramified in K/k and not invariant under complex conjugation. Then*

$$d_p Cl_K \geq \frac{\omega}{2} - \varepsilon$$

where $\varepsilon = 1$ if K contains the pth roots of unity and $\varepsilon = 0$ otherwise.

Often it is desirable to find number fields of low absolute degree whose class groups have large p-rank for some prime p. Therefore, the following result on cyclotomic fields is of interest.

Corollary 5.8 *Let $m = qm'$ where q is an odd prime with $(q, m') = 1$ such that -1 is not a power of q modulo m'. Let p be a prime divisor of $q - 1$. Then the cyclotomic field $\mathbb{Q}(\xi_m)$ has a complex subfield K of absolute degree $\varphi(m')p/\mathrm{ord}_{m'}(q)$ with*

$$d_p Cl_K \geq \frac{\varphi(m')}{2\mathrm{ord}_{m'}(p)} - \varepsilon$$

where $\varepsilon = 1$ if $p = 2$ or p divides m' and $\varepsilon = 0$ otherwise.

Proof Let x be a primitive root modulo q. By Result 2.4, the decomposition group of the primes above q in $\mathbb{Q}(\xi_m)$ is generated by σ_q and $\sigma_{m'}$ where σ_q is defined by $\xi_q \mapsto \xi_q^x$, $\xi_{m'} \mapsto \xi_{m'}$, and $\sigma_{m'}$ is defined by $\xi_q \mapsto \xi_q$, $\xi_{m'} \mapsto \xi_{m'}^q$. Let K be the fixed field of $\langle \sigma_q^p,\ \sigma_{m'} \rangle$. Then K has absolute degree $p\varphi(m')/\mathrm{ord}_{m'}(p)$. Let k be the fixed field of $\langle \sigma_q, \sigma_{m'} \rangle$. There are $\varphi(m')/\mathrm{ord}_{m'}(q)$ distinct primes of k above q which are all not invariant under complex conjugation by Result 2.4 since -1 is not a power of q modulo m'. The ramification index of these primes in K/k is p. Thus the assertion follows from Corollary 5.5 a. □

Corollary 5.9 *Let $m = qm'$ where q is an odd prime with $(q, m') = 1$ such that -1 is not a power of q modulo m'. Let p be a prime divisor of $q - 1$. If*

$$\frac{\varphi(m')}{\mathrm{ord}_{m'}(q)} \geq 8p + 12, \tag{9}$$

then $\mathbb{Q}(\xi_m)$ has an infinite p-class field tower.
Furthermore, if p is odd and does not divide m', then the same conclusion still holds if (9) is replaced by

$$\frac{\varphi(m')}{\mathrm{ord}_{m'}(q)} \geq 8(p + 1). \tag{10}$$

Proof Let K be the subfield of $\mathbb{Q}(\xi_m)$ defined in the proof of Corollary 5.8. Note that K is complex. Thus, by Dirichlet's unit theorem, $d_pE_K \leq [K/\mathbb{Q}]/2 = \varphi(m')p/(2\mathrm{ord}_{m'}(q))$. Moreover, $d_pCl_K \geq \varphi(m')/(2\mathrm{ord}_{m'}(q)) - 1$ by Corollary 5.8. Write $x := \varphi(m')/(2\mathrm{ord}_{m'}(q))$. By Result 5.1, K and thus $\mathbb{Q}(\xi_m)$ has an infinite p-class field tower if $x - 1 \geq 2 + 2\sqrt{px+1}$, i.e., if $x \geq 4p + 6$. This proves the first assertion of Corollary 5.9. The second assertion follows by the same argument since in this case $d_pE_K \leq \varphi(m')p/(2\mathrm{ord}_{m'}(q)) - 1$ and $d_pCl_K \geq \varphi(m')/(2\mathrm{ord}_{m'}(q))$. □

Corollary 5.10 *For every prime p, there are infinitely many cyclotomic fields $\mathbb{Q}(\xi_{qr})$, q, r prime, with infinite p-class field towers.*

Proof We use Dirichlet's theorem on primes in arithmetic progession (see [2]). We choose a prime $r \equiv 1 \pmod 3$ with $(r - 1)/3 \geq 8p + 12$. By Dirichlet's theorem, there are infinitely many primes q with $\mathrm{ord}_r(q) = 3$. By Corollary 5.9, $\mathbb{Q}(\xi_{qr})$ has an infinite class field tower for each of these q. □

The following bound on 2-ranks of subfields of cyclotomic fields is consequence of Theorem 4.4.

Corollary 5.11 *Let $m = m'p$ where p is an odd prime with $(p, m') = 1$. Let 2^b be the exact power of 2 dividing $p-1$. Let $\varepsilon = 0$ if -1 is a power of p modulo m' and $\varepsilon = 1$ otherwise. Then $\mathbb{Q}(\xi_m)$ has a complex subfield K of absolute degree $2^{b-\varepsilon}\varphi(m')/\mathrm{ord}_{m'}(p)$ with*

$$d_2 Cl_K \geq \varphi(m')/(2^\varepsilon \mathrm{ord}_{m'}(p)) - 1.$$

Proof Let U be the subgroup of $\mathrm{Gal}(\mathbb{Q}(\xi_m')/\mathbb{Q})$ generated by $\sigma_p : \xi_{m'} \to \xi_{m'}^p$ together with the complex conjugation. Let E be the subfield of $\mathbb{Q}(\xi_m')$ fixed by U, let F be the unique subfield of $\mathbb{Q}(\xi_p)$ of degree 2^b, and let $K := FG$. Then $[K : \mathbb{Q}] = 2^{b-\varepsilon}\varphi(m')/\mathrm{ord}_{m'}(p)$ as asserted. Let K^+ be the maximal real subfield of K. Then all $\varphi(m')/(2^\varepsilon \mathrm{ord}_{m'}(p))$ primes above p ramify in K/K^+. Thus the assertion follows from Theorem 4.4. □

Corollary 5.12 *Let $m = m'p$ where $p \equiv 3 \pmod 4$ is a prime with $(p, m') = 1$. Let $\varepsilon = 0$ if -1 is a power of p modulo m' and $\varepsilon = 1$ otherwise. If*

$$\frac{\varphi(m')}{2^\varepsilon \mathrm{ord}_{m'}(p)} \geq 10,$$

then $\mathbb{Q}(\xi_m)$ has an infinite 2-class field tower.

Proof This follows from Result 5.1 and Corollary 5.11. □

Remark 5.13 Corollary 5.12 gives a new proof for the fact that $\mathbb{Q}(\xi_{363})$ has an infinite 2-class field tower. To see this, take $p = 3$, $m' = 121$. Then $\varepsilon = 1$, and $\varphi(m')/(2^\varepsilon \mathrm{ord}_{m'}(p)) = 110/(2 \cdot 5) = 11$.

Acknowledgement

I am grateful to Werner Bley for useful discussions concerning Remark 5.4.

References

[1] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition). Cambridge University Press, Cambridge 1999.

[2] Z.I. Borevich, I.R. Shafarevich: *Number Theory.* Academic Press, New York/San Francisco/London 1966.

[3] J.W.S. Cassels, A. Froehlich: *Algebraic number theory.* Academic Press, London 1967.

[4] G. Cornell: Abhyankar's lemma and the class group. In: *Number Theory.* Ed. M. Nathanson, Lecture Notes in Math. 751, Springer, Berlin/Heidelberg/New York 1979, 82-88.

[5] G. Cornell, M. Rosen: Group-Theoretic Constraints on the Structure of the Class Group. *J. Number Theory* **13** (1981), 1-11.

[6] G. Cornell, L.C. Washington: Class Numbers of Cyclotomic Fields. *J. Number Theory* **21** (1985), 260-274.

[7] E.S. Golod, I.R. Shafarevic: On Class Field Towers. *Amer. Math. Soc. Transl. Ser. 2* **48** (1965), 91-102.

[8] H. Hasse: *Über die Klassenzahl Abelscher Zahlkörper.* Springer, Berlin/Heidelberg/New York 1985.

[9] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory.* Graduate Texts in Math. 84, Springer, Berlin/Heidelberg/New York 1990.

[10] N. Jacobson: *Basic Algebra I, II* (2nd edition). W. H. Freeman and Company, New York 1985.

[11] D. Kubert: The 2-divisibility of the class number of cyclotomic fields and the Stickelberger ideal. *J. Reine Angew. Math.* **369** (1986), 192-218.

[12] J. Masley: *On the Class Number of Cyclotomic Fields.* Ph.D. thesis, Princeton University, 1972.

[13] J. Martinet: Tours de corps de classes et estimations de discriminants. *Invent. Math.* **44** (1978), 65-73.

[14] J. Neukirch: *Algebraic number theory.* Springer 1999.

[15] J. Neukirch, A. Schmidt, K. Wingberg: *Cohomology of number fields.* Springer 2000.

[16] P. Ribenboim: *Algebraic Numbers.* Wiley, New York 1972.

[17] P. Ribenboim: *13 Lectures on Fermat's Last Theorem.* Springer, Berlin/Heidelberg/New York 1979.

[18] B. Schmidt: Cyclotomic Integers and Finite Geometry. *J. Am. Math. Soc.* **12** (1999), 929-952.

[19] R. Schoof: Infinite class field towers of quadratic fields. *J. Reine Angew. Math.* **372** (1986), 209-220.

[20] L.C. Washington: *Introduction to Cyclotomic Fields.* Graduate Texts in Math. 83, Springer, Berlin/Heidelberg/New York 1997.