ON 2-CLASS FIELD TOWERS OF SOME IMAGINARY QUADRATIC NUMBER FIELDS

FRANZ LEMMERMEYER

Abstract. We construct an infinite family of imaginary quadratic number fields with 2-class groups of type $(2,2,2)$ whose Hilbert 2-class fields are finite.

1. Introduction

Let k be an imaginary quadratic number field. It has been known for quite a while that the 2-class field tower of an imaginary quadratic number field is infinite if $\operatorname{rank} \mathrm{Cl}_2(k) \ge 5$, but it is not known how far from best possible this bound is. F. Hajir [4] has shown that the 2-class field tower is infinite if $\mathrm{Cl}(k) \supseteq (4,4,4)$, and again we do not know if this result can be improved. In this article we will study the 2-class field towers of a family of quadratic fields whose 2-class groups have rank 3.

For quadratic discriminants d, let $\mathrm{Cl}_2(d)$ and $h_2(d)$ denote the 2-class group and the 2-class number of $\mathbb{Q}(\sqrt{d}\,)$, respectively. The fundamental unit of $\mathbb{Q}(\sqrt{m}\,)$ will be denoted by ε_m, whether m is a discriminant or not. A factorization $d = d_1 \cdot d_2$ of a discriminant d into two coprime discriminants d_1, d_2 is called a C_4-factorization if $(d_1/p_2) = (d_2/p_1) = +1$ for all primes $p_1 \mid d_1$, $p_2 \mid d_2$. A D_4-factorization of d is a factorization $d = (d_1 \cdot d_2) \cdot d_3$ such that $d_1 \cdot d_2$ is a C_4-factorization. Finally, $d = d_1 \cdot d_2 \cdot d_3$ is called a H_8-factorization if $(d_1d_2/p_3) = (d_2d_3/p_1) = (d_3d_1/p_2) = +1$ for all primes $p_j \mid d_j$, $j = 1,2,3$. It is known (cf. [8]) that d admits a G-factorization ($G \in \{C_4, D_4\}$) if and only if $k = \mathbb{Q}(\sqrt{d}\,)$ admits an extension K/k which is unramified outside ∞, normal over $\mathbb{Q}$, and which has Galois group $\mathrm{Gal}(K/k) \simeq G$.

Let F^1 denote the 2-class field of a number field F, and put $F^2 = (F^1)^1$. Then in our case genus theory shows that $d = \operatorname{disc} k = d_1d_2d_3d_4$ is the product of exactly four prime discriminants, and moreover we have $k_{\rm gen} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{d_4}\,)$.

Our aim is to prove the following

Theorem 1. *Let $k = \mathbb{Q}(\sqrt{d}\,)$ be an imaginary quadratic number field with discriminant $d = -4pqq'$, where $p \equiv 5 \bmod 8$, $q \equiv 3 \bmod 8$ and $q' \equiv 7 \bmod 8$ are primes such that $(q/p) = (q'/p) = -1$. Then $\Gamma_n = \mathrm{Gal}(k^2/k)$ is given by*

$$\begin{aligned}\Gamma_n = \langle \rho, \sigma, \tau : \quad & \rho^4 = \sigma^{2^{n+1}} = \tau^4 = 1, \rho^2 = \sigma^{2^n}\tau^2, \\ & [\sigma,\tau] = 1, [\rho,\sigma] = \sigma^2, [\rho,\tau] = \sigma^{2^n}\tau^2 \rangle,\end{aligned}$$

where n is determined by $\mathrm{Cl}_2(-qq') = (2, 2^n)$. Moreover, $\mathrm{Cl}_2(k) \simeq (2,2,2)$ and $\mathrm{Cl}_2(k^1) \simeq (2, 2^n)$; for results about class and unit groups of subfields of k^1/k see the proof below.

We note a few relations which have proved to be useful for computing in Γ_n: $(\rho\sigma)^2 = \rho^2$, $(\rho\sigma\tau)^2 = (\rho\tau)^2 = \tau^2$, $[\rho, \tau^2] = 1$.

2. Preliminary Results on Quadratic Fields

We will use a few results on 2-class groups of quadratic number fields which can easily be deduced from genus theory. We put $m = pqq'$, where p, q, q' satisfy the conditions in Thm. 1, and set $k = \mathbb{Q}(\sqrt{-m}\,)$.

Lemma 2. *The ideal classes of* $\mathfrak{z} = (2, 1+\sqrt{-m}\,)$, $\mathfrak{p} = (p, \sqrt{-m}\,)$ *and* $\mathfrak{q} = (q, \sqrt{-m}\,)$ *generate* $\mathrm{Cl}_2(k) \simeq (2,2,2)$.

Proof. Since $(q/p) = (q/p') = -1$ and $p \equiv 5 \bmod 8$, there are no C_4-factorizations of d, and this shows that $\mathrm{Cl}_2(k) \simeq (2,2,2)$. The ideal classes generated by $\mathfrak{z}$, $\mathfrak{p}$ and $\mathfrak{q}$ are non-trivial simply because their norm is smaller than m; the same reasoning shows that they are independent. $\square$

Lemma 3. *The quadratic number field* $\widetilde{k} = \mathbb{Q}(\sqrt{-qq'}\,)$ *has* 2*-class group* $\mathrm{Cl}_2(\widetilde{k}) \simeq (2, 2^n)$ *for some* $n \geq 1$*; it is generated by the prime ideals* $\mathfrak{z} = (2, 1+\sqrt{-qq'}\,)$ *above* 2 *and a prime ideal* $\widetilde{\mathfrak{p}}$ *above* p. *Moreover, the ideal classes of* $\mathfrak{z}$ *and* $\mathfrak{q} = (q, \sqrt{-qq'}\,)$ *generate a subgroup* C_2 *of type* $(2,2)$*; we have* $n \geq 2$ *if and only if* $(q'/q) = -1$*, and in this case, the square class in* C_2 *is* $[\mathfrak{z}\mathfrak{q}]$.

Proof. Since $q \equiv 3 \bmod 8$, the only possible C_4-factorization is $d = -q' \cdot 4q$; this is a C_4-factorization if and only if $(-q'/q) = +1$. In this case, exactly one of the ideal classes $[\mathfrak{z}]$, $[\mathfrak{q}]$ and $[\mathfrak{z}\mathfrak{q}]$ is a square; by genus theory, this must be $[\mathfrak{z}\mathfrak{q}]$. Finally, let $\widetilde{\mathfrak{p}}$ denote a prime ideal above p. Then $[\,\widetilde{\mathfrak{p}}\,]$ is no square in $\mathrm{Cl}_2(\widetilde{k})$ because $(-q/p) = -1$, $[\mathfrak{z}\widetilde{\mathfrak{p}}\,]$ is no square because $(-q'/2p) = -1$, $[\mathfrak{q}\widetilde{\mathfrak{p}}\,]$ is no square because $(-q'/pq) = -1$, and $[\mathfrak{z}\mathfrak{q}\widetilde{\mathfrak{p}}\,]$ is no square because $(-q'/2qp) = -1$. This implies that $[\,\widetilde{\mathfrak{p}}\,]$ has order 2^n. $\square$

Lemma 4. *The real quadratic number field* $F = \mathbb{Q}(\sqrt{m}\,)$ *has* 2*-class number* 2*; the prime ideal* $\mathfrak{p}$ *above* p *is principal, and the fundamental unit* ε_m *of* $\mathcal{O}_F$ *becomes a square in* $F(\sqrt{p}\,)$.

Proof. Consider the prime ideals $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{q}'$ in $\mathcal{O}_F$ above p, q and q', respectively; since $h_2(m) = 2$ (by genus theory) and $N\varepsilon_m = +1$, there must be a relation between their ideal classes besides $\mathfrak{p}\mathfrak{q}\mathfrak{q}' \sim 1$. Now clearly $\mathfrak{q}$ cannot be principal, since this would imply $X^2 - my^2 = \pm 4q$; writing $X = qx$ and dividing by q gives $qx^2 - pq'y^2 = \pm 4$. But this contradicts our assumption that $(q/p) = -1$. By symmetry, $\mathfrak{q}'$ cannot be principal; since $h_2(F) = 2$, their product $\mathfrak{q}\mathfrak{q}'$ is, hence we have $\mathfrak{p} \sim \mathfrak{q}\mathfrak{q}' \sim 1$. The equation $X^2 - my^2 = \pm 4p$ then leads as above to $px^2 - qq'y^2 = -4$ (the plus sign cannot hold since it would imply that $(p/q) = 1$), and it is easy to see that the unit $\eta = \frac{1}{2}(x\sqrt{p} + y\sqrt{qq'}\,)$ satisfies $\eta^2 = \varepsilon_m^u$ for some odd integer u. $\square$

3. The 2-class field tower of k

In this section we prove that the 2-class field tower of k stops at k^2, and that $\mathrm{Gal}(k^2/k) \simeq \Gamma_n$.

3.1. **Class Numbers of Quadratic Extensions.** Let K/k be a quadratic unramified extension. Then $q(K) = 1$; we define

- $\zeta = \zeta_6$ if $q = 3$ and $\zeta = -1$ otherwise;
- e_j is the unit group of the maximal order $\mathcal{O}_j$ of k_j;
- N_j is the relative norm of k_j/k;

- κ_j is the subgroup of ideal classes in $\mathrm{Cl}(k)$ which capitulate in k_j;
- h_j denotes the 2-class number of k_j.

Then we claim that Table 1 gives the unit group, the relative norm of the unit group, the capitulation order, the 2-class number and the relative norm of the 2-class group for the quadratic unramified extensions k_j/k.

TABLE 1.

j	k_j	e_j	$N_j e_j$	$\#\kappa_j$	h_j	$N_j \,\mathrm{Cl}_2(k_j)$
1	$\mathbb{Q}(i, \sqrt{m}\,)$	$\langle i, \varepsilon_m \rangle$	$\langle 1 \rangle$	4	8	$\langle [\mathfrak{2}], [\mathfrak{p}] \rangle$
2	$\mathbb{Q}(\sqrt{-q}, \sqrt{pq'}\,)$	$\langle \zeta, \varepsilon_{pq'} \rangle$	$\langle 1 \rangle$	4	8	$\langle [\mathfrak{2p}], [\mathfrak{2q}] \rangle$ $\quad\langle [\mathfrak{2p}], [\mathfrak{q}] \rangle$
3	$\mathbb{Q}(\sqrt{-p}, \sqrt{qq'}\,)$	$\langle -1, \varepsilon_{qq'} \rangle$	$\langle 1 \rangle$	4	8	$\langle [\mathfrak{p}], [\mathfrak{q}] \rangle$
4	$\mathbb{Q}(\sqrt{p}, \sqrt{-qq'}\,)$	$\langle -1, \varepsilon_p \rangle$	$\langle -1 \rangle$	2	2^{n+3}	$\langle [\mathfrak{p}], [\mathfrak{2q}] \rangle$
5	$\mathbb{Q}(\sqrt{-q'}, \sqrt{pq}\,)$	$\langle -1, \varepsilon_{pq} \rangle$	$\langle 1 \rangle$	4	8	$\langle [\mathfrak{2}], [\mathfrak{pq}] \rangle$ $\quad\langle [\mathfrak{2}], [\mathfrak{q}] \rangle$
6	$\mathbb{Q}(\sqrt{-pq}, \sqrt{q'}\,)$	$\langle -1, \varepsilon_{q'} \rangle$	$\langle 1 \rangle$	4	8	$\langle [\mathfrak{2}], [\mathfrak{q}] \rangle$ $\quad\langle [\mathfrak{2}], [\mathfrak{pq}] \rangle$
7	$\mathbb{Q}(\sqrt{-pq'}, \sqrt{q}\,)$	$\langle -1, \varepsilon_q \rangle$	$\langle 1 \rangle$	4	8	$\langle [\mathfrak{2p}], [\mathfrak{q}] \rangle$ $\quad\langle [\mathfrak{2p}], [\mathfrak{2q}] \rangle$

The left hand side of the column $N_j \,\mathrm{Cl}_2(k_j)$ refers to case A (i.e. $(q/q') = -1$), the right hand side to case B. We will now verify the table. The unit groups are easy to determine - we simply use the following proposition from [2]:

Proposition 5. *Let k be an imaginary quadratic number field, and assume that K/k is a quadratic unramified extension. Then K is a V_4-extension, and $q(K) = 1$.*

Applying this to the extension $K = k_j$ we find that the unit group e_j is generated by the roots of unity in k_j and the fundamental unit of the real quadratic subfield. Since $\#\kappa_j = 2(E_k : N_{K/k}E_K)$ for unramified quadratic extensions K/k, (see [2]), the order of the capitulation kernel is easily computed from the unit groups. Similarly, the 2-class number of $h(k_j)$ is given by the class number formula (see [6]), and since the unit index equals 1 in all cases, its computation is trivial.

Let us compute $N_j \,\mathrm{Cl}_2(k_j)$ in a few cases. Take e.g. $k_j = \mathbb{Q}(\sqrt{p}, \sqrt{-qq'}\,)$: here the prime ideal $\mathfrak{p}$ is a norm because $(-qq'/p) = +1$, whereas $\mathfrak{2}$ and $\mathfrak{q}$ are inert, since $p \equiv 5 \bmod 8$ and $(p/q) = -1$. This implies that the ideal class $[\mathfrak{2q}]$ must be a norm, since $(\mathrm{Cl}_2(k) : N_j \,\mathrm{Cl}_2(k_j)) = 2$ by class field theory.

As another example, take $k_j = \mathbb{Q}(\sqrt{-q}, \sqrt{pq'}\,)$ and assume that we are in case B), i.e. that $(q/q') = 1$. Then $\mathfrak{q}$ is a norm since $(pq'/q) = +1$, and the ideals $\mathfrak{2}$ and $\mathfrak{p}$ are inert; this yields $N_j \,\mathrm{Cl}_2(k_j) = \langle [\mathfrak{q}], [\mathfrak{2p}] \rangle$.

3.2. **The 2-class group of k_4 is $(4, 2^{n+1})$.** We know $N_4 \,\mathrm{Cl}_2(k_4) = \langle [\mathfrak{p}], [\mathfrak{2q}] \rangle$ and $\#\kappa_4 = 2$. Since $\mathfrak{p} = (p, \sqrt{d}\,)$ becomes principal, we have $\kappa_4 = \langle [\mathfrak{p}] \rangle$.

Let $\widetilde{\mathfrak{p}}$ denote a prime ideal above p in $\mathbb{Q}(\sqrt{-qq'}\,)$; we have shown in Lemma 3 that $\widetilde{\mathfrak{p}}^{2^{n-1}} \sim \mathfrak{2q}$. Since this ideal class does not capitulate in k_4, we see that $\widetilde{\mathfrak{p}}$ generates a cyclic subgroup of order 2^n in $\mathrm{Cl}_2(k_4)$.

Let $\mathcal{O}$ denote the maximal order of k_4; then $p\mathcal{O} = \mathfrak{P}^2\mathfrak{P}'^2$. We claim that $\mathfrak{P}^2 \sim \widetilde{\mathfrak{p}}$. To this end, let s and t be the elements of order 2 in $\mathrm{Gal}(k_4/\mathbb{Q})$ which fix F and

k, respectively. Using the identity $2+(1+s+t+st)=(1+s)+(1+t)+(1+st)$ of the group ring $\mathbb{Z}[\mathrm{Gal}(k_4/\mathbb{Q})]$ and observing that $\mathbb{Q}$ and the fixed field of st have odd class numbers we find

$$\mathfrak{P}^2 \sim \mathfrak{P}^{1+s}\mathfrak{P}^{1+t}\mathfrak{P}^{1+st} \sim \widetilde{\mathfrak{p}}\mathfrak{p} \sim \widetilde{\mathfrak{p}},$$

where the last relation (in $\mathrm{Cl}_2(k_4)$) comes from the fact that $\mathfrak{p} \in \kappa_4$.

Thus $\langle[\mathfrak{2}],[\mathfrak{P}]\rangle$ is a subgroup of type $(2,2^{n+1})$ (hence of index 2) in $\mathrm{Cl}_2(k_4)$. Taking the norm to F we find $N_F\langle[\mathfrak{2}],[\mathfrak{P}]\rangle = \langle[\,\widetilde{\mathfrak{p}}\,]\rangle$; therefore there exists an ideal $\mathfrak{A}$ in $\mathcal{O}$ such that $N_F\mathfrak{A} \sim \mathfrak{2}$ (equivalence in $\mathrm{Cl}(F)$). We conclude that $\mathrm{Cl}_2(k_4) = \langle[\mathfrak{2}],[\mathfrak{A}],[\mathfrak{P}]\rangle$. Similarly, letting N_4 denote the norm in k_4/k we get $N_4\langle[\mathfrak{2}],[\mathfrak{P}]\rangle = \langle[\,\widetilde{\mathfrak{p}}\,]\rangle$; this shows that $N_4\mathfrak{A} \sim \mathfrak{2q}$ or $N_4\mathfrak{A} \sim \mathfrak{2qp}$ (equivalence in $\mathrm{Cl}(k)$; which of the two possibilities occurs will be determined below). But since $\mathfrak{p} \sim 1$ in $\mathrm{Cl}_2(k_4)$ we can conclude that $\mathfrak{A}^{1+t} \sim \mathfrak{2q}$. This gives $\mathfrak{A}^2 \sim \mathfrak{2}\cdot\mathfrak{2q} \sim \mathfrak{q}$, and in particular $[\mathfrak{A}]$ has order 4 in $\mathrm{Cl}_2(k_4)$.

Finally we claim that $\mathrm{Cl}_2(k_4) = \langle[\mathfrak{A}],[\mathfrak{P}]\rangle$, i.e. that $[\mathfrak{2}] \in \langle[\mathfrak{A}],[\mathfrak{P}]\rangle$. This is easy: from $\mathfrak{P}^2 \sim \widetilde{\mathfrak{p}}$ we deduce that $\mathfrak{P}^{2^n} \sim \mathfrak{2q}$, hence we get $\mathfrak{A}^2\mathfrak{P}^{2^n} \sim \mathfrak{2}$.

3.3. **Proof that** $k^2 = k^3$**.** Since $\mathrm{Cl}_2(k_4) \simeq (4, 2^{n+1})$, we can apply Prop. 4 of [1], which says that k_4 has abelian 2-class field tower if and only if it has a quadratic unramified extension K/k_4 such that $h_2(K) = \frac{1}{2}h_2(k_4)$.

Put $M = \mathbb{Q}(i, \sqrt{p}, \sqrt{qq'}\,)$, and consider its subfield $M^+ = \mathbb{Q}(\sqrt{p}, \sqrt{qq'}\,)$. M^+ is the Hilbert 2-class field of $F = \mathbb{Q}(\sqrt{m}\,)$, hence $h_2(M^+) = 1$, and the class number formula gives $q(M^+) = 2$. In fact it follows from Lemma 4 that $E_{M^+} = \langle -1, \varepsilon_p, \varepsilon_{qq'}, \sqrt{\varepsilon_m}\,\rangle$.

According to Thm. 1.ii).1. of [7], Hasse's unit index $Q(M)$ equals 1 if $w_M \equiv 4 \bmod 8$ (w_M denotes the number of roots of unity in M; in our case $w_M = 4$ or $w_M = 12$) and if the ideal generated by 2 is not a square in M^+ (this is the case here since $2 \nmid \operatorname{disc} M^+$). Thus $Q(M) = 1$ and $E_M = \langle \xi, \varepsilon_p, \varepsilon_{qq'}, \sqrt{\varepsilon_m}\,\rangle$, where ξ is a primitive 4^{th} ($q \neq 3$) or 12^{th} ($q = 3$) root of unity. This shows that the unit index of the extension $M/\mathbb{Q}(i)$ equals 2, and the class number formula finally gives

$$h_2(M) = \tfrac{1}{4}\cdot 2\cdot 1\cdot 2^n \cdot 8 = 2^{n+2} = \tfrac{1}{2}h_2(k_4).$$

3.4. **Computation of** $\mathrm{Gal}(k^2/k)$**.** Put $L = k^2$ and $K = k_4$; clearly $\sigma = \big(\frac{L/K}{\mathfrak{P}}\big)$ and $\tau = \big(\frac{L/K}{\mathfrak{A}}\big)$ generate the abelian subgroup $\mathrm{Gal}(L/K) \simeq (2^{n+1}, 4)$ of $\Gamma_n = \mathrm{Gal}(L/k)$. If we put $\rho = \big(\frac{L/k}{\mathfrak{2}}\big)$ then ρ restricts to the nontrivial automorphism of K/k (since $[\mathfrak{2}]$ is not a norm from k_4/k), which shows that $\Gamma_n = \langle\rho,\sigma,\tau\rangle$. The relations are easily computed: $\rho^2 = \big(\frac{L/K}{\mathfrak{2}}\big) = \sigma^{2^n}\tau^2$, since $\mathfrak{2} \sim \mathfrak{A}^2\mathfrak{P}^{2^n}$, $\rho^{-1}\sigma\rho = \big(\frac{L/K}{\mathfrak{P}^\rho}\big) = \sigma^{-1}$, since $\mathfrak{P}\mathfrak{P}^\rho = \mathfrak{p} \sim 1$, and $\tau\rho^{-1}\tau\rho = \big(\frac{L/K}{\mathfrak{A}^{1+\rho}}\big) = \big(\frac{L/K}{\mathfrak{2q}}\big) = \sigma^{2^n}$. Thus

$$\begin{aligned}\Gamma_n = \langle \rho,\sigma,\tau : \quad & \rho^4 = \sigma^{2^{n+1}} = \tau^4 = 1, \rho^2 = \sigma^{2^n}\tau^2, \\ & [\sigma,\tau] = 1, [\rho,\sigma] = \sigma^2, [\tau,\rho] = \sigma^{2^{n-1}}\tau^2\rangle\end{aligned}$$

as claimed. We refer the reader to Hasse's report [5] for the used properties of Artin symbols.

3.5. **Additional Information on Units and Class Groups.** Using the presentation of Γ_n it is easy to compute the abelianization of its subgroups of index 2; this shows at once that $\mathrm{Cl}_2(k_j) \simeq (2,4)$ for all $j \neq 4$ in case A and in for all $j \neq 5,7$ in case B. More results are contained in Table 2.

TABLE 2.

j	k_j	$\mathrm{Cl}_2(k_j)$	κ_j	$\mathrm{Gal}(k^2/k_j)$
1	$\mathbb{Q}(i,\sqrt{m}\,)$	$(2,4)$	$\langle[\mathfrak{2}],[\mathfrak{p}]\rangle$	$\langle\rho,\sigma,\tau^2\rangle$
2	$\mathbb{Q}(\sqrt{-q},\sqrt{pq'}\,)$	$(2,4)$	$\langle[\mathfrak{q}],[\mathfrak{2p}]\rangle$	$\langle\rho\sigma,\rho\tau,\sigma^2,\tau^2\rangle$
3	$\mathbb{Q}(\sqrt{-p},\sqrt{qq'}\,)$	$(2,4)$	$\langle[\mathfrak{p}],[\mathfrak{q}]\rangle$	$\langle\rho\tau,\sigma,\tau^2\rangle$
4	$\mathbb{Q}(\sqrt{p},\sqrt{-qq'}\,)$	$(4,2^{n+1})$	$\langle[\mathfrak{p}]\rangle$	$\langle\sigma,\tau\rangle$
5	$\mathbb{Q}(\sqrt{-q'},\sqrt{pq}\,)$	$(2,4)$ $(2,2,2)$	$\langle[\mathfrak{pq}],[\mathfrak{2p}]\rangle$	$\langle\rho,\sigma^2,\tau\rangle$
6	$\mathbb{Q}(\sqrt{-pq},\sqrt{q'}\,)$	$(2,4)$	$\langle[\mathfrak{pq}],[\mathfrak{2}]\rangle$	$\langle\rho,\sigma\tau,\sigma^2\rangle$
7	$\mathbb{Q}(\sqrt{-pq'},\sqrt{q}\,)$	$(2,4)$ $(2,2,2)$	$\langle[\mathfrak{2}],[\mathfrak{q}]\rangle$	$\langle\rho\sigma,\tau,\sigma^2\rangle$

The computation of the capitulation kernels κ_j is no problem at all: take k_1, for example. We have seen that $\mathfrak{p}$ is principal in $\mathbb{Q}(\sqrt{m}\,)$, hence it is principal in k_1. Moreover, $\mathfrak{2}=(1+i)$ is clearly principal, and since we know from Table 1 that $\#\kappa_1=4$ we conclude that $\kappa_1=\langle[\mathfrak{p}],[\mathfrak{2}]\rangle$.

Before we determine the Galois groups corresponding to the extensions k_j/k we examine whether $N_4\mathfrak{A}\sim\mathfrak{2q}$ or $N_4\mathfrak{A}\sim\mathfrak{2pq}$ (equivalence in $\mathrm{Cl}_2(k)$). We do this as follows: first we choose a prime ideal $\mathfrak{R}$ in $\mathcal{O}$ such that $[\mathfrak{A}]=[\mathfrak{R}]$ (this is always possible by Chebotarev's theorem). Then its norms $\widetilde{\mathfrak{r}}$ in $\mathcal{O}_F$ and $\mathfrak{r}$ in $\mathcal{O}_k$ are prime ideals, and we have $\mathfrak{2}\widetilde{\mathfrak{r}}\sim 1$ in $\mathrm{Cl}_2(F)$. This implies that $2r=x^2+2qq'y^2$, from which we deduce that $(2r/q)=+1$. If we had $\mathfrak{2q r}\sim 1$ in $\mathrm{Cl}_2(k)$, this would imply $2qr=U^2+mv^2$; writing $U=qu$ this gives $2r=qu^2+pq'v^2$. This in turn shows $(2r/q)=(pq'/q)=(-q'/q)$, which is a contradiction if $(q/q')=-1$. Thus $N_4\mathfrak{A}\sim\mathfrak{2pq}$ in case A). Similarly one shows that $N_4\mathfrak{A}\sim\mathfrak{2q}$ in case B).

Now consider the automorphism $\tau=\left(\frac{L/K}{\mathfrak{A}}\right)$; we have just shown that $\tau=\left(\frac{L/K}{\mathfrak{R}}\right)$. Let M be a quadratic extension of K in L; then the restriction of $\tau\in\mathrm{Gal}(L/K)$ to M is $\tau|_M=\left(\frac{M/K}{\mathfrak{R}}\right)$, and this is the identity if and only if the prime ideals in the ideal class $[\mathfrak{R}]$ split in M/K. But from $2r=x^2+2qq'y^2$ we get $r\equiv 3 \bmod 4$, $(2r/q)=+1$, hence $(q/r)=1$ since $q\equiv 3 \bmod 8$. This shows that $\mathfrak{R}$ splits in $K_5=K(\sqrt{q}\,)=\mathbb{Q}(\sqrt{p},\sqrt{q},\sqrt{-q'}\,)$, thus τ fixes K_5, and we find $\mathrm{Gal}(L/K_5)=\langle\tau,\sigma^2\rangle$.

Next $\mathfrak{P}$ splits in $K_1=K(\sqrt{-1}\,)$, hence σ fixes K_1, and we have $\mathrm{Gal}(L/K_1)=\langle\sigma,\tau^2\rangle$. Finally, ρ fixes those extensions k_j/k in which $[\mathfrak{2}]$ splits, i.e. k_1, k_5 and k_6. In particular, ρ fixes their compositum K_3, and we find $\mathrm{Gal}(L/K_3)=\langle\rho,\sigma^2,\tau^2\rangle$.

Using elementary properties of Galois theory we can fill in the entries in the last column of Tables 2 and 3.

The 2-class group structure for the subfields K_j of k^1/k of relative degree 4, the relative norms of their 2-class groups and their Galois groups are given in Table 3. The structure of $\mathrm{Cl}_2(K_j)$ is easily determined from $\mathrm{Cl}_2(K_j)\simeq\mathrm{Gal}(k^2/K_j)^{\mathrm{ab}}$. Note that in every extension K_j/k the whole 2-class group of k is capitulating.

It is also possible to determine the unit groups E_j of the fields K_j (see Table 4). In fact, applying the class number formula to the V_4-extensions K_j/k we can determine the unit index $q(K_j/k)$ since we already know the class numbers. Thus all we have to do is check that the square roots of certain units lie in the field K_j. This is done as follows: consider the quadratic number field $M=\mathbb{Q}(\sqrt{q}\,)$. Since

Table 3.

j	K_j	$\mathrm{Cl}_2(K_j)$	$N_j\,\mathrm{Cl}_2(K_j)$	$\mathrm{Gal}(k^2/K_j)$
1	$\mathbb{Q}(\sqrt{-1}, \sqrt{p}, \sqrt{qq'}\,)$	$(2, 2^{n+1})$	$\langle[\mathfrak{p}]\rangle$	$\langle\sigma, \tau^2\rangle$
2	$\mathbb{Q}(\sqrt{-1}, \sqrt{-q}, \sqrt{-pq'}\,)$	$(2, 4)$	$\langle[2\mathfrak{p}]\rangle$	$\langle\rho\sigma, \sigma^2\rangle$
3	$\mathbb{Q}(\sqrt{-1}, \sqrt{-q'}, \sqrt{-pq}\,)$	$(2, 4)$	$\langle[2]\rangle$	$\langle\rho, \sigma^2\rangle$
4	$\mathbb{Q}(\sqrt{p}, \sqrt{-q}, \sqrt{q'}\,)$	$(2, 2^{n+1})$	$\langle[2\mathfrak{q}]\rangle$ $\langle[2\mathfrak{p}\mathfrak{q}]\rangle$	$\langle\sigma\tau, \sigma^2\rangle$
5	$\mathbb{Q}(\sqrt{p}, \sqrt{-q'}, \sqrt{q}\,)$	$(4, 2^n)$	$\langle[2\mathfrak{p}\mathfrak{q}]\rangle$ $\langle[2\mathfrak{q}]\rangle$	$\langle\tau, \sigma^2\rangle$
6	$\mathbb{Q}(\sqrt{-q}, \sqrt{-p}, \sqrt{-q'}\,)$	$(2, 4)$	$\langle[\mathfrak{p}\mathfrak{q}]\rangle$ $\langle[\mathfrak{q}]\rangle$	$\langle\rho\tau, \sigma^2\rangle$
7	$\mathbb{Q}(\sqrt{q'}, \sqrt{-p}, \sqrt{q}\,)$	$(2, 4)$	$\langle[\mathfrak{q}]\rangle$ $\langle[\mathfrak{p}\mathfrak{q}]\rangle$	$\langle\rho\sigma\tau, \sigma^2\rangle$

Table 4.

j	E_j	$q(K_j/k)$
1	$\langle i, \varepsilon_p, \varepsilon_{qq'}, \sqrt{\varepsilon_m\varepsilon_{pq'}}\,\rangle$	2
2	$\langle \zeta, \sqrt{i\varepsilon_q}, \varepsilon_{pq'}, \sqrt{\varepsilon_m\varepsilon_{pq'}}\,\rangle$	4
3	$\langle i, \sqrt{i\varepsilon_{q'}}, \varepsilon_{pq}, \sqrt{\varepsilon_m\varepsilon_{pq}}\,\rangle$	4
4	$\langle -1, \varepsilon_p, \varepsilon_{q'}, \sqrt{\varepsilon_{q'}\varepsilon_{pq'}}\,\rangle$	2
5	$\langle -1, \varepsilon_p, \varepsilon_q, \sqrt{\varepsilon_q\varepsilon_{pq}}\,\rangle$	2
6	$\langle -1, \varepsilon_{pq}, \sqrt{\varepsilon_{pq}\varepsilon_{pq'}}, \sqrt{\varepsilon_{qq'}}\,\rangle$	4
7	$\langle -1, \varepsilon_q, \sqrt{\varepsilon_q\varepsilon_{q'}}, \sqrt{\varepsilon_{qq'}}\,\rangle$	4

it has odd class number and since 2 is ramified in M we conclude that there exist integers $x, y \in \mathbb{Z}$ such that $x^2 - qy^2 = \pm 2$; from $q \equiv 3 \bmod 8$ we deduce that, in fact, $x^2 - qy^2 = -2$. Put $\eta_q = (x + y\sqrt{q}\,)/(1+i)$; then $\eta_q^2 = -\varepsilon_q^u$ for some odd integer u shows that $i\varepsilon_q$ becomes a square in $M(i)$. Doing the same for the prime q' we also see that $\eta_q\eta_{q'}^{-1} \in \mathbb{Q}(\sqrt{q}, \sqrt{q'}\,)$, and this implies that $\sqrt{\varepsilon_q\varepsilon_{q'}} \in \mathbb{Q}(\sqrt{q}, \sqrt{q'}\,)$. The other entries in Table 4 are proved similarly.

Using the same methods we can actually show that

$$E = \langle \zeta, \varepsilon_p, \sqrt{i\varepsilon_q}, \sqrt{i\varepsilon_{q'}}, \sqrt{\varepsilon_{qq'}}, \sqrt{i\varepsilon_{pq}}, \sqrt{i\varepsilon_{pq'}}, \sqrt{\varepsilon_m}\,\rangle$$

has index 2 in the full unit group of k_{gen}.

4. The Field with Discriminant $d = -420$

The smallest example in our family of quadratic number fields is given by $d = -420 = -4 \cdot 3 \cdot 5 \cdot 7$. Poitou [10] noticed that the class field tower of $k = \mathbb{Q}(\sqrt{d}\,)$ must be finite, and Martinet [9] observed (without proof) that its class field tower terminates at the second step with k^2, and that $(k^2 : k) = 32$. In this section, we will give a complete proof (this will be used in [13]).

The unit group of the genus class field $k_{\rm gen}$ is

$$E = \langle \zeta_{12}, \varepsilon_5, \sqrt{i\varepsilon_3}, \sqrt{i\varepsilon_7}, \sqrt{i\varepsilon_{15}}, \sqrt{i\varepsilon_{35}}, \sqrt{\varepsilon_{21}}, \eta\rangle,$$

where $\eta = \sqrt{\varepsilon_7^{-1}\varepsilon_5\sqrt{\varepsilon_3\varepsilon_7\varepsilon_{15}\varepsilon_{35}\varepsilon_{105}}} = \frac{1}{2}(1 + 2\sqrt{5} + \sqrt{7} + \sqrt{15} + \sqrt{21}\,)$. Since $k_{\rm gen}$ has class number 4, the second Hilbert class field is just its 2-class field, which can be constructed explicitly: $k^2 = k^1(\sqrt{\mu}, \sqrt{\nu}\,)$, where $\mu = (4i - \sqrt{5}\,)(2 + \sqrt{5}\,)$ and $\nu = (2\sqrt{-5} + \sqrt{7}\,)(8 + 3\sqrt{7}\,)$.

We claim that k^2 has class number 1. Odlyzko's unconditional bounds show that $h(k^2) \le 10$, and since we know that it has odd class number, it suffices to prove that no odd prime ≤ 10 divides $h(k^2)$. For $p = 5$ and $p = 7$ we can use the following result which goes back to Grün [3]:

Proposition 6. *Let L/k be a normal extension of number fields, and let K denote the maximal subfield of L which is abelian over k.*

i) *If $\mathrm{Cl}(L/K)$ is cyclic, then $h(L/K) \mid (L : K)$;*
ii) *If $\mathrm{Cl}(L)$ is cyclic, then $h(L) \mid (L : K)e$, where e denotes the exponent of $N_{L/K}\,\mathrm{Cl}(L)$. Observe that $e \mid h(K)$, and that $e = 1$ if L contains the Hilbert class field K^1 of K.*

Similar results hold for the p-Sylow subgroups.

Proof. Let C be a cyclic group of order h on which $\Gamma = \mathrm{Gal}(L/k)$ acts. This is equivalent to the existence of a homomorphism $\Phi : \Gamma \longrightarrow \mathrm{Aut}(C) \simeq \mathbb{Z}/(h-1)\mathbb{Z}$. Since im Φ is abelian, $\Gamma' \subseteq \ker\Phi$, hence Γ' acts trivially on C. Now Γ' corresponds to the field K via Galois theory, and we find $N_{L/K}c = c^{(L:K)}$. Putting $C = \mathrm{Cl}(L/K)$, we see at once that $(L : K)$ annihilates $\mathrm{Cl}(L/K)$; if we denote the exponent of $N_{L/K}\,\mathrm{Cl}(L)$ by e and put $C = \mathrm{Cl}(L)$, then we find in a similar way that $(L : K)e$ annihilates $\mathrm{Cl}(L)$. $\square$

This shows at once that $h(k^2)$ is not divisible by 5 or 7. For $p = 3$, the proof is more complicated. First we use an observation due to R. Schoof:

Proposition 7. *Let L/k be a normal extension with Galois group Γ, and suppose that $3 \nmid \#\Gamma$. Let K be the maximal abelian extension of k contained in L. If Γ does not have a quotient of type SD_{16}, if $\mathrm{Cl}_3(L) \simeq (3,3)$, and if $3 \nmid h(k)$, then there exists a subfield E of L/k such that $\mathrm{Cl}_3(E) \simeq (3,3)$ and $\mathrm{Gal}(E/k) \simeq D_4$ or H_8.*

Proof. Put $A = \mathrm{Cl}_3(L)$; then Γ acts on A, i.e. there is a homomorphism $\Phi : \Gamma \longrightarrow \mathrm{Aut}(A) \simeq \mathrm{GL}(2,3)$. From $\#\,\mathrm{GL}(2,3) = 48$ and $3 \nmid \Gamma$ we conclude that im Φ is contained in the 2-Sylow subgroup of $\mathrm{GL}(2,3)$, which is $\simeq SD_{16}$.

We claim that im Φ is not abelian. In fact, assume that it is. Then im $\Phi \simeq \Gamma/\ker\Phi$ shows that $\Gamma' \subseteq \ker\Phi$; hence Γ' acts trivially on A. The fixed field of Γ' is K, and now $\mathrm{Cl}_3(K) \supseteq N_{L/K}\,\mathrm{Cl}_3(L) = A^{(L:K)} \simeq A$ shows that $3 \mid h(K)$ contradicting our assumptions.

Thus im Φ is a nonabelian 2-group, and we conclude that $\#\,\mathrm{im}\,\Phi \ge 8$. On the other hand, Γ does not have SD_{16} as a quotient, hence $\#\,\mathrm{im}\,\Phi = 8$, and we have im $\Phi \simeq D_4$ or H_8, since these are the only nonabelian groups of order 8. Let E be the fixed field of $\ker\Phi$. Since $\ker\Phi$ acts trivially on A, we see $\mathrm{Cl}_3(E) \supseteq N_{L/E}\,\mathrm{Cl}_3(L) = A^{(L:E)} \simeq A$ (note that $(L : E) \mid \Gamma$ is not divisible by 3). The other assertions are clear. $\square$

Applying the proposition to the extension k^2/k (we have to check that $\mathrm{Gal}(k^2/\mathbb{Q})$ does not have SD_{16} as a quotient. But $\mathrm{Gal}(k^2/\mathbb{Q})$ is a group extension

$$1 \longrightarrow \mathrm{Gal}(k^2/k^1) \longrightarrow \mathrm{Gal}(k^2/\mathbb{Q}) \longrightarrow \mathrm{Gal}(k^1/\mathbb{Q}) \longrightarrow 1$$

of an elementary abelian group $\mathrm{Gal}(k^1/\mathbb{Q}) \simeq (2,2,2,2)$ by another elementary abelian group $\mathrm{Gal}(k^2/k^1) \simeq (2,2)$, from which we deduce that $\mathrm{Gal}(k^2/\mathbb{Q})$ has exponent 4. Now observe that SD_{16} has exponent 8) we find that $3 \nmid h(k^2)$ unless k^2 contains a normal extension $E/\mathbb{Q}$ with 3-class group of type $(3,3)$ and Galois group isomorphic to D_4 or H_8. Let E_0 be the maximal abelian subfield of E; this is a V_4-extension of $\mathbb{Q}$ with quadratic subfields k_0, k_1 and k_2. Let k_0 denote a quadratic subfield over which E is cyclic. If a prime ideal $\mathfrak{p}$ ramifies in E_0/k_0, then it must ramify completely in E/k_0; but since all prime ideals have ramification index ≤ 2 in E (since $E \subset k^2$), this is a contradiction.

Thus E/k_0 is unramified. If we put $d_j = \operatorname{disc} k_j$, then this happens if and only if $d_0 = d_1 d_2$ and $(d_1, d_2) = 1$. For quaternion extensions, this is already a contradiction, since we conclude by symmetry that $d_1 = d_0 d_2$ and $d_2 = d_0 d_1$. Assume therefore that $\mathrm{Gal}(E/\mathbb{Q}) \simeq D_4$. From a result of Richter [11] we know that E_0 can only be embedded into a dihedral extension if $(d_1/p_2) = (d_2/p_1) = +1$ for all $p_1 \mid d_1$ and all $p_2 \mid d_2$. But E_0 is an abelian extension contained in k^2, hence it is contained in k_{gen}, and we see that d is a product of the prime discriminants -3, -4, 5, and -7. Since no combination of these factors satisfies Richter's conditions, E_0 cannot be embedded into a D_4-extension $E/\mathbb{Q}$. This contradiction concludes our proof that $3 \nmid h(k_2)$.

Acknowledgement

Much of Section 4, in particular Proposition 7, is due to R. Schoof [12], whom I would like to thank for his help. I also thank C. Snyder for correcting an error in Table 2.

References

[1] E. Benjamin, F. Lemmermeyer, C. Snyder, *Real Quadratic Fields with Abelian 2-Class Field Tower*, submitted 4

[2] E. Benjamin, F. Sanborn, C. Snyder, *Capitulation in Unramified Quadratic Extensions of Real Quadratic Number Fields*, Glasgow Math. J. **36** (1994), 385–392 3

[3] O. Grün, *Aufgabe* 153; Lösungen von L. Holzer und A. Scholz, Jahresber. DMV **45** (1934), 74–75 (kursiv)

[4] F. Hajir, *On a theorem of Koch*, Pac. J. Math. **176** (1996), 15–18 7 1

[5] H. Hasse, *Zahlbericht. Teil II*, Würzburg-Wien 1970 4

[6] F. Lemmermeyer, *Kuroda's Class Number Formula*, Acta Arith. **66.3** (1994), 245–260. 3

[7] F. Lemmermeyer, *Ideal class groups of cyclotomic number fields I*, Acta Arith. **72** (1995), 347–359 4

[8] F. Lemmermeyer, *Unramified quaternion extensions of quadratic number fields*, J. Théor. Nombres Bordeaux **9** (1997), 51–68 1

[9] J. Martinet, *Petits discriminants des corps de nombres*, Journées Arithmétiques 1980 (J. V. Armitage, ed.), Cambridge Univ. Press 1982, 151–193, 6

[10] G. Poitou, *Minorations de discriminants*, Sém. Bourbaki (1975/76) **479** (1977), 136–153 6

[11] H. Richter, *Über die Lösbarkeit einiger nicht-Abelscher Einbettungsprobleme*, Math. Annalen **112** (1936), 69–84 8
[12] R. Schoof, *Letter from Nov. 13, 1992* 8
[13] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*, preprint 1996 6

Bilkent University, Dept. Mathematics, 06533 Bilkent, Ankara
E-mail address: hb3@ix.urz.uni-heidelberg.de, franz@fen.bilkent.edu.tr