JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

FRANZ LEMMERMEYER

On 2-class field towers of imaginary quadratic number fields

Journal de Théorie des Nombres de Bordeaux, tome 6, n° 2 (1994), p. 261-272

<http://www.numdam.org/item?id=JTNB_1994__6_2_261_0>

Journal de Théorie des Nombres
de Bordeaux **6** *(1994), 261–272*

On 2-class field towers of imaginary quadratic number fields

par FRANZ LEMMERMEYER

ABSTRACT. For a number field k, let k^1 denote its Hilbert 2-class field, and put $k^2 = (k^1)^1$. We will determine all imaginary quadratic number fields k such that $G = Gal(k^2/k)$ is abelian or metacyclic, and we will give G in terms of generators and relations.

1. Introduction

Let $k = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic number field with discriminant $d < 0$. It is well known that the structure of the 2-class group $Cl_2(k)$ depends on the factorization of d into prime discriminants: these are discriminants which are prime powers, i.e. -4, ± 8, $-q, (q \equiv 3 \bmod 4)$, and $p\,(p \equiv 1 \bmod 4)$. We say that d has t factors if d is the product of exactly t prime discriminants. Here we will study the question how far these factorizations determine the 2-class field tower of k.

To this end let k^1 denote the Hilbert 2-class field of k, i.e. the maximal unramified normal extension of k whose Galois group is an abelian 2-group. Moreover, let $k^2 = (k^1)^1$. We will classify the discriminants d of imaginary quadratic number fields according to the structure of $G = Gal(k^2/k)$, and we will determine all d such that $k = \mathbb{Q}(\sqrt{d})$ has abelian or metacyclic $Gal(k^2/k)$. Partial classifications have been obtained in [1] and [10]; whereas Benjamin and Snyder used Koch's Satz 1 of [9], we will employ his Satz 2 instead. The formulation of this theorem contains some errors; its correction reads (see [10]; a G-extension of k is an extension K/k with $Gal(K/k) \simeq G$, the notation of the groups is the one used in [2]):

THEOREM 1. *Let k be a quadratic number field; there exists a G-extension K/k which is unramified at the finite places and such that $K/\mathbb{Q}$ is normal if and only if there is a factorization $d = disc\,k = d_1d_2d_3$ into relatively prime discriminants such that the Kronecker symbols (d_i/p_j) in $(*)$ below equal $+1$ (here p_j runs through all primes dividing d_j):*

Manuscrit reçu le 20 Juin 1994.

G	$(*)$	$Gal(K/\mathbb{Q})$
D_4	(d_1/p_2), (d_2/p_1)	16.06
H_8	(d_1d_2/p_3), (d_2d_3/p_1), (d_3d_1/p_2)	16.08
16.09	(d_1/p_2), (d_1/p_3), (d_2/p_1), (d_3/p_1)	32.33
16.10	(d_1/p_2), (d_2/p_1), (d_1d_2/p_3), (d_3/p_1), (d_3/p_2)	32.36
$(4,4)$	*all* (d_i/p_j) *with* $i \neq j$	32.34

If $(d_i/p_j) = 1$ *for all* $i \neq j$, *there also exists an unramified extension* L/k *such that* $Gal(L/k) \simeq 32.18$ *and* $Gal(L/\mathbb{Q}) \simeq 64.144$.

The following two propositions will help us in deciding if the p-class field tower of a quadratic number field terminates at some stage; the basic observation is due to Iwasawa [5]:

PROPOSITION 1. *Let* k *be a number field and suppose that its* p*-class field tower terminates with* K. *Then* $\mathfrak{M}(Gal(K/k)) \simeq E_k/N_{K/k}E_K$, *where* $\mathfrak{M}(G)$ *denotes the Schur multiplier of a group* G *and* E_k *denotes the unit group of the ring of integers* $\mathfrak{O}_k$ *of* k.

If, for example, K/k is an unramified and normal 2-extension of an imaginary quadratic number field k with $|\mathfrak{M}(Gal(K/k))| \geq 4$, then $K^1 \neq K$. For showing that a certain class field tower terminates we use the following result (cf. [10]):

PROPOSITION 2. *Let* k *be a number field and let* K^1 *be a normal unramified extension containing the* p*-class field* k^1 *of* k; *if* $\mathfrak{M}(Gal(K/k)) = 1$, *then the* p*-class field tower of* k *terminates with* K.

Proof. Suppose otherwise; then there exists an unramified extension L/K, which is central with respect to K/k. i.e. which satisfies $Gal(L/K) \subseteq Z(Gal(L/k))$. Moreover, $Gal(L/K) \subseteq Gal(L/k)'$ because K contains k^1. Recalling the most elementary properties of Schur multipliers (cf. [13] or [7]), this gives the contradiction $\mathfrak{M}(Gal(K/k)) \neq 1$.

In particular, the p-class field tower of a field with cyclic p-class group terminates with k^1, because cyclic groups have trivial multiplier.

2. Abelian groups as $Gal(k^2/k)$

The fields $\mathbb{Q}(\sqrt{d})$, $d < 0$, such that $G = Gal(k^2/k)$ is abelian, have been determined in [10]; for fields with $G/G' \simeq (2, 2^m)$ this result has been obtained independently by Benjamin and Snyder [1].

THEOREM 2. *Let $\mathbb{Q}(\sqrt{d})$ be an imaginary quadratic number field with discriminant d. Then $Gal(k^2/k)$ is abelian if and only if d has at most three factors and if at most one of them is positive. Actually, we have (p and q, q' etc. denote primes $\equiv 1$ and $\equiv 3 \bmod 4$, respectively):*

G	$disc\, k$	$\lvert G\rvert$
1	$-4, -8, -q$	1
$2^m,\ m \geq 1$	$-4p, -8p, -pq$	$h_2(k)$
$(2,2)$	$-4qq',\ q \equiv 3 \bmod 8,\ (q/q') = -1$	4
	$-8qq',\ q \equiv 3 \bmod 8,\ (q/q') = -1$	4
	$-qq'q'',\ (q/q') = (q'/q'') = (q''/q)$	4
$(2,2^m),\ m \geq 2$	$-4qq',\ q \equiv 7 \bmod 8,\ (q/q') = -1$	$h_2(k)$
	$-8qq',\ q \equiv 7 \bmod 8,\ (q/q') = -1$	$h_2(k)$
	$-qq'q'',\ (q/q') = (q'/q'') = (q/q'')$	$h_2(k)$

The "only-if"-part of the theorem can be proved quite simply: suppose that $G = Gal(k^2/k)$ is abelian. Then the 2-class field tower of k terminates with $K = k^1$. Since k is imaginary quadratic and $disc\, k \neq -3, -4$ (recall that we have assumed d to have three prime factors), we find $E_k = \{-1, +1\}$, so $E_k/N_{K/k}E_K$ has order ≤ 2. This implies that the abelian 2-groups possibly occuring as $Gal(k^2/k)$ must have Schur multiplier of order ≤ 2. The only such 2-groups are the cyclic groups and those of type $(2,2^m)$, $m \geq 1$ (see [7]).

If $Gal(k^2/k)$ is cyclic, then so is $Cl_2(k)$, and by genus theory this is equivalent to $disc\, k$ being the product of exactly two prime discriminants. The theory of Rédei, Reichardt and Scholz allows us to find all d such that $Cl_2(k) \simeq (2,2^m), m \geq 1$; we will outline the method used to compute $Gal(k^2/k)$ in case $d = -4p \cdot q$ is the corresponding factorization of the second kind. Here we have $(-q/p) = 1$ and $q \equiv 7 \bmod 8$; the ideal classes of $\mathfrak{z} = (2, 1 + \sqrt{-pq})$ and $\mathfrak{p} = (p, \sqrt{-pq})$ have order 2 in $Cl(k)$ and differ from each other. Genus theory shows that the ideal class of $\mathfrak{p}$ is no square in $Cl(k)$; class field theory implies that the quadratic unramified extension $K_1 = k(\sqrt{-q})$ belongs to a subgroup of index 2 in $Cl_2(k)$, and since $\mathfrak{p}$ splits in K_1/k, this subgroup is not cyclic. Therefore, the fields $K = k(\sqrt{-1})$ and $k(\sqrt{q})$ belong to the cyclic subgroups of index 2 in $Cl_2(k)$, i.e. $N_{K/k}Cl_2(K)$ is a cyclic group of order 2^m.

Now we notice that the quadratic field $\mathbb{Q}(\sqrt{pq})$ has odd class number, and that $K = k(\sqrt{-1})$ has unit group $E_K = < i, \varepsilon_{pq} >$, where ε_{pq} is the fundamental unit of $\mathbb{Q}(\sqrt{pq})$ (for a proof, see [8]). The class number formula now gives $h_2(K) = 2^m$, and since the norm of $Cl_2(K)$ to k is cyclic of order 2^m, so is $Cl_2(K)$. In particular, the 2-class field tower of k

terminates with K^1, and the equality $(K^1 : k) = 2^{m+1} = (k^1 : k)$ shows that in fact $K^1 = k$.

Remark. The knowledge of k^2/k allows us to compute the structure of $Cl_2(L)$ for the subfields L of k^1/k; we are also able to compute the subgroups of those $Cl_2(L)$ which capitulate in any given extension L/K contained in k^1/k. For fields with $k^1 = k^2$, however, this is hardly interesting: in this case, exactly the ideal classes of order $\leq (L : K)$ capitulate in any extension L/K such that $k \subset K \subset L \subset k^1$ (this fact was already known to Scholz and can be proved immediately by computing the kernel of the corresponding transfer maps).

3. Metacyclic groups as $Gal(k^2/k)$

Our primary aim is to show:

THEOREM 3. *Let $k = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic number field with discriminant d. Then $Gal(k^2/k)$ is metacyclic if and only if*

i) *G is abelian and k is one of the fields described in Section 2, or*
ii) *$G/G' \simeq (2,2)$; then G is dihedral, semidihedral or quaternionic, and k is one of the fields listed in* [8] *and* [10], *or*
iii) *$d = -4pq$, where p and q are primes $\equiv 5 \bmod 8$.*

For groups $G = Gal(k^2/k)$ such that $G/G' \simeq (2, 2^m)$ this has been obtained by Benjamin and Snyder [1]; the proof of theorem 3 that we will offer depends partly on their results. We begin our proof with the well known observation that factor groups of metacyclic groups are metacyclic. If, therefore, $G = Gal(k^2/k)$ is metacyclic, then so is $G/G' \simeq Cl_2(k)$. Genus theory now implies that $d = d_1d_2d_3$ for prime discriminants d_j. If $Cl_2(k)$ has a subgroup of type $(4,4)$, then theorem 1 shows that G has a factor group $\simeq 32.18$. Since 32.18 is not metacyclic, neither is G.

So far we have seen: if $G = Gal(k^2/k)$ is metacyclic, then $G/G' \simeq (2, 2^m)$ for some $m \geq 1$. If $m = 1$, G is dihedral, semidihedral or quaternionic, and this case has already been settled by Kisilevsky [8] (see also [10]). The case $m > 1$ has been studied by Benjamin and Snyder [1]: they have shown that metacyclic groups G with $G/G' \simeq (2, 2^m)$ occur as $G = Gal(k^2/k)$ if and only if $d = -4pq$, where p and q are primes $\equiv 5 \bmod 8$. Using theorem 1, we can prove this as follows: since $Cl(k)$ is assumed to have a cyclic subgroup of order 4, we must have $d = d_1d_2d_3$ for prime discriminants d_j, such that $d_1 \cdot d_2d_3$ is a factorization of the second kind (in the terminology of Rédei and Reichardt): this is to say that $(d_2d_3/p_1) = (d_1/p_2) = (d_1/p_3) = +1$, where p_j is the unique prime dividing d_j.

Now we observe the following: if d_1 and d_2 are prime discriminants such that $(d_1/p_2) = +1$, then we also have $(d_2/p_1) = +1$ except when both d_1 and d_2 are negative or when $d_1 = -4, d_2 = p \equiv 5 \bmod 8$ (or vice versa).

Returning to the situation discussed above we see that there are three cases to consider:

1. All three d_j are negative: then $G = Gal(k^2/k)$ is abelian, as we have seen in Section 2.
2. Exactly one d_j is negative, and d is not of the form $-4pq$, where p and q are primes $\equiv 5 \bmod 8$: then $(d_1/p_2) = (d_1/p_3) = +1$ implies, from what we have seen, that $(d_2/p_1) = (d_3/p_1) = 1$. By theorem 1, these relations imply the existence of an unramified 16.09–extensions of k. Since 16.09 is not metacyclic, neither is $G = Gal(k^2/k)$.
3. $disc\, k = -4pq$, $p \equiv q \equiv 5 \bmod 8$.

We will now use the techniques sketched in [10] to compute the structure of $Gal(k^2/k)$ for the fields k in 3. To this end, suppose that $p \equiv q \equiv 5 \bmod 8$ are primes such that $(p/q) = 1$; suppose moreover that the fundamental unit ε_{pq} of $F = \mathbb{Q}(\sqrt{pq})$ has norm -1. The theory of Rédei, Reichardt and Scholz now gives $(p/q)_4 = (q/p)_4$ and $Cl_2(F) \simeq \mathbb{Z}/2^n\mathbb{Z}$ for some $n \geq 2$. The prime ideal $\mathfrak{p}$ in F above p is not principal: for if $\mathfrak{p} = (\pi)$ for some $\pi \in \mathfrak{O}_F$, then π^2/p would be a unit with positive norm; this would imply that $\pm\pi^2/p$ and therefore $\pm p$ are squares in F. This contradiction shows that the ideal class $[\mathfrak{p}]$ has order 2; since $Cl_2(F)$ is cyclic, it is generated by an ideal class $[\mathfrak{a}]$ such that $\mathfrak{a}^{2^{n-1}} \sim \mathfrak{p}$. In fact we may choose $\mathfrak{a}$ as one of the two prime ideals above $2\mathbb{Z}$, because genus theory shows that their ideal classes are not squares in $Cl(F)$.

Similarly, the prime ideals $\mathfrak{z} = (2, 1 + \sqrt{-pq})$ and $\mathfrak{p} = (p, \sqrt{-pq})$ in k are not principal (the prime ideals $\mathfrak{p}$ in F and in k coincide in kF), and from genus theory we infer that the ideal class $[\mathfrak{p}]$ is a square in $Cl(k)$. Kaplan ([6]) has shown that the condition $(p/q)_4 = (q/p)_4$ deduced above implies that $Cl_2(k) \simeq (2, 4)$. Therefore, $Cl_2(k) = <\mathfrak{z}, \mathfrak{b}>$ (we will write $<\mathfrak{z}, \mathfrak{b}>$ for the rather clumsy $<[\mathfrak{z}], [\mathfrak{b}]>$), where $\mathfrak{b}^2 \sim \mathfrak{p}$.

Now let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{pq})$; this quadratic extension of k and F is contained in the 2-class field k^1 of k. It is an easy exercise to show that the unit group $E_K = <i, \varepsilon_{pq}>$ and that $h_2(K) = 2^{n+2}$. Since $N\varepsilon_{pq} = -1$, there exists exactly one non-trivial ideal class which capitulates in K/k; in fact, $\kappa_{K/k} = <\mathfrak{z}>$ (here $\kappa_{K/k}$ denotes the subgroup of ideal classes in $Cl(k)$ becoming principal in K), because $\mathfrak{z}\mathfrak{O}_K = (1 + i)$. From this we deduce that $\mathfrak{p}\mathfrak{O}_K$ is not principal, and that the ideal class of $\mathfrak{b}\mathfrak{O}_K$ generates a subgroup of order 4 in $Cl(K)$. The same argument yields that

the class of $\mathfrak{a}O_K$ generates a subgroup of order 2^n in $Cl(K)$. We claim that the subgroup $< \mathfrak{a}, \mathfrak{b} >$ of $Cl(K)$ has index 2 in $Cl_2(K)$. This index is certainly ≥ 2 because $\mathfrak{a}^{2^{n-1}} \sim \mathfrak{p} \sim \mathfrak{b}^2$. Now suppose that $\mathfrak{a}^s \sim \mathfrak{b}$ in K; taking the norm to k gives $1 \sim \mathfrak{b}^2$ as a relation in $Cl(k)$, which is clearly a contradiction.

The prime ideal $\mathfrak{2}$ splits in K/k. Let $\mathfrak{2}\mathfrak{O}_K = \mathfrak{A}\mathfrak{A}'$; then $N_{K/k} < \mathfrak{a}, \mathfrak{b} > = < \mathfrak{p} >$, because $N_{K/k}\mathfrak{a}$ and $\mathfrak{b}^2 \sim \mathfrak{p}$, and therefore the subgroup of $Cl_2(K)$ generated by the classes of $\mathfrak{a}$ and $\mathfrak{b}$ does not contain the ideal class of $\mathfrak{A}$, because $N_{K/k} < \mathfrak{A} > = < \mathfrak{2} >$ is not contained in $< \mathfrak{p} >$. Since $< \mathfrak{a}, \mathfrak{b} >$ has index 2 in $Cl_2(K)$, we must have $Cl_2(K) = < \mathfrak{A}, \mathfrak{a}, \mathfrak{b} >$.

Let ρ denote the automorphism of $K/\mathbb{Q}$ which fixes F; then $\mathfrak{A}^{1+\rho}$ is a prime ideal in F above $2\mathbb{Z}$, and without loss of generality we may assume that it equals $\mathfrak{a}$. Similarly, let σ denote the automorphism fixing k; then $\mathfrak{A}^{1+\sigma} = \mathfrak{2}$. We therefore get the following relations between ideal classes in K, keeping in mind that $1 + \sigma$ acts on $Cl(K)$, whereas $N_{K/k}$ maps $Cl(K)$ to $Cl(k)$:

$$\mathfrak{A}^{1+\rho} \sim \mathfrak{a}, \quad \mathfrak{A}^{1+\sigma} \sim \mathfrak{2} \sim 1, \quad \mathfrak{A}^{1+\rho\sigma} \sim 1;$$

the least relation holds because $\rho\sigma$ fixes $\mathbb{Q}(i)$ which has class number one. Now we see that

$$\mathfrak{A}^2 \sim \mathfrak{A}^{1+\rho}\mathfrak{A}^{1+\sigma}\mathfrak{A}^{1+\rho\sigma} \sim \mathfrak{a},$$

which shows that the ideal class of $\mathfrak{A}$ has order 2^{n+1} in $Cl(K)$, and that $Cl_2(K) = < \mathfrak{A}, \mathfrak{b} >$. The relation $\mathfrak{A}^{2^n} \sim \mathfrak{b}^2 = \mathfrak{p}$ reveals that $Cl_2(K) \simeq (2, 2^{n+1})$.

The fact that we know the structure of $Cl_2(K)$ as a $Gal(K/k)$-module allows us to compute $Gal(K^1/k)$. To this end, let $(L/k, \mathfrak{a})$ denote the Artin symbol of a normal extension L/K (for properties of Artin symbols see Hasse's Zahlbericht [3]), and let $\sigma = (K^1/k, \mathfrak{b})$ be an extension of the automorphism $(k^1/k, \mathfrak{b})$; then $\sigma^2 = (K^1/K, \mathfrak{b})$ has order 4, and σ^2 and $\tau = (K^1/K, \mathfrak{A})$ generate $Gal(K^1/K)$. Therefore, $Gal(K^1/k) = < \sigma, \tau >$, and we have the relations

$$< \sigma^2, \tau > \simeq Cl_2(K), \text{ i.e. } \sigma^4 = \tau^{2^{n+1}}, \text{ and}$$

$$\sigma^{-1}\tau\sigma = (K^1/K, \mathfrak{A}^\sigma) = (K^1/K, \mathfrak{A}^{-1}) = \tau^{-1}.$$

Now it is easy to see that $\mathfrak{M}(G) = 1$ (there is actually a formula for the order of $\mathfrak{M}(G)$ for metacyclic groups G; cf. [7]); this implies that $K^1 = k^2$ (we also could have deduced this from [1, prop. 2]). Since G' is cyclic,

the 2-class field tower of k terminates with k^2. We note that the group $G = Gal(k^2/k)$ in theorem 4 is the group of type 2 in [1, prop. 2], with $\alpha = n - 1$. We have proved:

THEOREM 4. *Let $p \equiv q \equiv 5 \bmod 8$ be primes such that $(p/q) = 1$, and suppose that the fundamental unit ε_{pq} of $\mathbb{Q}(\sqrt{pq})$ has norm -1. Then*

1. $Cl_2(k) \simeq (2,4)$ *for* $k = \mathbb{Q}(\sqrt{-pq})$;
2. $Cl_2(F) \simeq (2^n)$, $n \geq 2$, *for* $F = \mathbb{Q}(\sqrt{pq})$;
3. $Cl_2(K) \simeq (2, 2^{n+1})$ *for* $K = \mathbb{Q}(i, \sqrt{pq})$;
4. $G = Gal(K^1/k) = < \sigma, \tau \mid \tau^{2^{n+1}} = 1, \sigma^4 = \tau^{2^n}, \sigma^{-1}\tau\sigma = \tau^{-1} >$;
5. $K^1 = k^2 = k^3$, *and* $\mathfrak{M}(G) = 1$.

Examples:

p	q	$h(k)$	$h(F)$
5	29	8	4
5	229	24	4
13	101	24	4
5	349	40	4
13	173	40	4
5	461	24	16
5	509	24	4
5	541	72	8

Now we will examine the case where $N\varepsilon_{pq} = +1$. In $F = \mathbb{Q}(\sqrt{pq})$, the prime ideals $\mathfrak{2}_1$ and $\mathfrak{2}_2$ above $2\mathbb{Z}$ are not principal because the equation $x^2 - pqy^2 = \pm 8$ has no solutions mod p. Moreover, genus theory shows that $[\mathfrak{2}_1]$ is no square in $Cl(F)$; since $Cl_2(F)$ is cyclic, the ideal class $[\mathfrak{2}_1]$ generates $Cl_2(F)$. We will need the fact that there is no non-trivial capitulation in K/F, where $K = \mathbb{Q}(i, \sqrt{pq})$. This will follow from the slightly more general

PROPOSITION 3. *Let F be a real quadratic number field and $K = F(i)$. There is non-trivial capitulation in K/F if and only if $2\mathfrak{O}_F = \mathfrak{2}^2$, i.e. 2 is ramified in $F/\mathbb{Q}$; in this case, the ideal class of $\mathfrak{2}$ capitulates.*

Proof. Let $\mathfrak{a}$ be a non-principal ideal in $\mathfrak{O}_F$ which capitulates in K. Then there is an $\alpha \in \mathfrak{O}_K$ such that $\mathfrak{a}\mathfrak{O}_K = (\alpha)$. Let σ denote the non-trivial automorphism of K/F; then $\alpha^{\sigma-1} = \varepsilon$ is a unit in $\mathfrak{O}_K$, and since $K/\mathbb{Q}$ is abelian, we have $|\varepsilon| = 1$. Now ε^2 is a root of unity times a unit in $\mathfrak{O}_F$ (this comes from the identity $\varepsilon^2 = \varepsilon^{1+\sigma}\varepsilon^{1+\rho}\varepsilon^{1+\rho\sigma}$, keeping in mind that the units of the two complex quadratic fields are roots of unity); the only units in $\mathfrak{O}_F$ with absolute value equal to 1 are ± 1. Therefore, $\alpha^{\sigma-1}$ must be a root of unity. There are the following possibilities:

1. $\alpha^{\sigma-1} = +1$: then $\alpha \in F$, and this contradicts the assumption that

$\mathfrak{a}$ be non-principal in $\mathfrak{O}_F$;

2. $\alpha^{\sigma-1} = -1$: then $i\alpha \in F$, and again $\mathfrak{a} = (i\alpha)$ would be principal in $\mathfrak{O}_F$;
3. $\alpha^{\sigma-1} = +i$: then $(1-i)\alpha \in F$; since $\mathfrak{a}$ and $\alpha\mathfrak{O}_F$ are ideals in $\mathfrak{O}_F$, it follows that $\mathfrak{z} = (1-i)\mathfrak{O}_K \cap \mathfrak{O}_F$ must be an ideal in $\mathfrak{O}_F$: but this implies $\mathfrak{z}^2 = 2\mathfrak{O}_F$;
4. $\alpha^{\sigma-1} = -i$: then $(1+i)\alpha \in F$, and again we must have $\mathfrak{z}^2 = 2\mathfrak{O}_F$.

Now assume that $\mathfrak{z}^2 = 2\mathfrak{O}_F$ and that $\mathfrak{z}$ is a non-principal ideal in $\mathfrak{O}_F$; then $2\mathfrak{O}_K = (1+i)$ is principal in K, i.e. $\mathfrak{z}$ capitulates.

Let 2^n be the order of $[\mathfrak{z}_1]$ in $Cl_2(F)$; since there is no capitulation in K/F, the prime ideal $\mathfrak{A}$ in K above $\mathfrak{z}_1$ generates an ideal class of order 2^{n+1}, because $\mathfrak{A}^2 = \mathfrak{z}_1\mathfrak{O}_K$. In $k = \mathbb{Q}(\sqrt{-pq})$ we have $Cl_2(k) = <\mathfrak{z}, \mathfrak{b}>$, where $\mathfrak{b}^{2^{m-1}} \sim \mathfrak{p}$. Since $N\varepsilon_{pq} = +1$, the ideal classes $[\mathfrak{z}]$ and $[\mathfrak{p}]$ both capitulate in K/k, and so $\mathfrak{b}$ generates a subgroup of order 2^{m-1} in $Cl(K)$. The computation of the 2-class number of K yields $h_2(K) = \frac{1}{2}q(K)h_2(F)h_2(k) = 2^{m+n}$; we claim that the ideal classes of $\mathfrak{b}$ and $\mathfrak{A}$ generate $Cl_2(K)$. For suppose that $\mathfrak{b}^s \sim \mathfrak{A}^t$: then $\mathfrak{b}^{2s} = N_{K/k}\mathfrak{b}^s \sim N_{K/k}\mathfrak{A}^t = \mathfrak{z}^t$ shows that t is even and that $s \equiv 0 \bmod 2^{m-1}$ (recall that $\mathfrak{z}$ and $\mathfrak{b}$ generate different subgroups of $Cl_2(k)$). But the order of $[\mathfrak{b}]$ in $Cl_2(K)$ equals 2^{m-1}, and therefore the relation $\mathfrak{b}^s \sim \mathfrak{A}^t$ is necessarily trivial. This proves that indeed $Cl_2(K) = <\mathfrak{b}, \mathfrak{A}>$.

Putting $\rho = (K^1/K, \mathfrak{A})$ and $\tau = (K^1/K, \mathfrak{b})$, $<\rho, \tau \,|\, \rho^{2^{n+1}} = \tau^{2^{m-1}} = 1>$ is an abelian subgroup of index 2 in $G = Gal(K^1/k)$. Let $\sigma \in (K^1/k, \mathfrak{b})$ be an extension of $(k^1/k, \mathfrak{b}) \in Gal(k^1/k)$; then we have $G = <\rho, \sigma, \tau>$, and we find the relations $\sigma^2 = (K^1/K, \mathfrak{b}) = \tau, \sigma^{-1}\rho\sigma = (K^1/K, \mathfrak{A}^\sigma) = \rho^{-1}$; to prove the last relation we use the fact that $\mathfrak{A}^{\sigma+1} = \mathfrak{z} = (1+i) \sim 1$ lies in the kernel of the Artin symbol of K^1/K. We finally remark that it follows from [6] that we either have $n = 1$ or $m = 2$, and that $\mathfrak{M}(G) \simeq \mathbb{Z}/2\mathbb{Z}$. This is in agreement with prop. 1, because $-1 \in E_k \setminus N_{K/k}E_K$. The fact that $k^2 = K^1$ follows from [1]: they proved that $Gal(k^2/k)$ has an abelian subgroup of order 2, which necessarily must be $Gal(k^2/K)$. We also observe that G is their metacyclic group of type 1. We have shown:

THEOREM 5. *Let $p \equiv q \equiv 5 \bmod 8$ be primes such that $(p/q) = 1$, and assume that the fundamental unit ε_{pq} of $\mathbb{Q}(\sqrt{pq})$ has norm $+1$. Then*

1. $Cl_2(k) \simeq (2, 2^m)$, $m \geq 2$, *for* $k = \mathbb{Q}(\sqrt{-pq})$;
2. $Cl_2(F) \simeq (2^n), n \geq 1$, *for* $F = \mathbb{Q}(\sqrt{pq})$;
3. $Cl_2(K) \simeq (2^{n+1}, 2^{m-1})$ *for* $K = \mathbb{Q}(i, \sqrt{pq})$, *and either* $n = 1$ *or*

$m = 2$;

4. $G = Gal(K^1/k) = < \rho, \sigma \mid \rho^{2^{n+1}} = \sigma^{2^m} = 1, \sigma^{-1}\rho\sigma = \rho^{-1} >$;
5. $K^1 = k^2 = k^3$, *and* $\mathfrak{M}(G) \simeq \mathbb{Z}/2\mathbb{Z}$.

The only case left to consider is $d = -4pq, p \equiv q \equiv 5 \bmod 8$, $(p/q) = -1$. Then we have $N\varepsilon_{pq} = -1$ and $h_2(F) = 2$ for $F = \mathbb{Q}(\sqrt{pq})$; we leave it as an exercise to the reader to prove the following theorem, using the methods described in this paper. Theorem 6 has already been announced in [10], and a proof using Koch's Satz 1 can be found in [1].

Examples:

p	q	$h(k)$	$h(F)$
5	61	16	2
13	29	16	2
5	101	8	4
5	109	32	2
13	53	40	4
5	149	16	2
13	61	8	4
5	181	24	4
5	269	16	6
29	53	16	2

THEOREM 6. *Let* $p \equiv q \equiv 5 \bmod 8$ *be primes such that* $(p/q) = -1$. *Then*

1. $Cl_2(k) \simeq (2, 2^m)$, $m \geq 2$, *for* $k = \mathbb{Q}(\sqrt{-pq})$;
2. $Cl_2(K) \simeq (2, 2^m)$ *for* $K = \mathbb{Q}(i, \sqrt{pq})$;
3. $G = Gal(K^1/k) \simeq < \rho, \sigma \mid \rho^2 = \sigma^{2^m}, \rho^4 = 1, \sigma^{-1}\rho\sigma = \rho^{-1} >$;
4. $K^1 = k^2 = k^3$, *and* $\mathfrak{M}(G) = 1$.

Obviously, theorems 4, 5 and 6 prove the part of theorem 3.(iii) that was still open.

4. Hasse's rank formula

On p. 52 of his book "Über die Klassenzahl abelscher Zahlkörper" [4], Hasse gave a formula for computing the 2-rank of class groups in CM-fields K/K_0 which reduces to the well known ambiguous class number formula in case K_0 has odd class number. If K_0 has even class number, however, Hasse's formula does not always give the correct rank: the cyclic quartic field $\mathbb{Q}\left(\sqrt{-10 + 3\sqrt{10}}\right)$ has cyclic 2-class group of order 4, and it is easily seen that this contradicts Hasse's formula. In fact, the fields listed in theorem 5, for example, provide infinitely many counterexamples. The

formula stated in [4] reads

$$Cl_2(K) = \gamma + r_0^* + s_0^* + \kappa,$$

where

$\gamma = t-1+rank\, E_{K_0} \cap N_{K/K_0} K/E_{K_0}^2$, where t is the number of (finite) prime ideals ramifying in K/K_0
r_0^* denotes the 2-rank of $Cl(K_0)^j$,
$j : Cl(K_0) \to Cl(K)$ is the transfer of ideal classes,
$s_0^* =$ rank $Cl(K_0)^j/Cl(K_0)^j \cap Cl(K)^2$ denotes the rank of the group of ideal classes becoming squares in $Cl(K)$. It follows from our proof below, that we also have $s_0^* =$ rank $H/H \cap Cl(K)^2$, where $H = Cl(K)^{1-\sigma}$;
$\kappa = |\ker j|$ is the order of the capitulation kernel.

To see that the formula is incorrect, we let $K_0 = \mathbb{Q}(\sqrt{pq})$ as in theorem 5, i.e. we assume that $p \equiv q \equiv 5 \bmod 8$ are primes such that $(p/q) = 1$ and $N\varepsilon_{pq} = -1$; if we assume moreover that $m = 2$, then we find

$E_{K_0} \cap N_{K/K_0} K = <1, \varepsilon_{pq}>$: to verify this claim, it is sufficient to show that ε_{pq} is norm from K. This can be done as follows: since ε_{pq} has norm $+1$, the prime ideal $\mathfrak{p}$ above p is principal, i.e. $\mathfrak{p} = (\pi)$. Obviously, $\eta = \pi^{\sigma-1}$ is a unit in $\mathfrak{O}_K$; if η were a square, so were $p = \pi^{\sigma+1}$. Now it is easily seen that we can choose π in such a way that $\pi^{\sigma-1} = \varepsilon_{pq}$. This implies $\varepsilon_{pq} = \pi^{\sigma+1}/p$, and since $p = a^2 + b^2 = N_{K/k}(a + bi)$, we find that $\varepsilon_{pq} = N_{K/k}\left(\frac{\pi}{a+bi}\right)$ is indeed a norm.
$\gamma = t - 1 + 1 = 2$, because only the two prime ideals above 2 ramify;
$r_0^* = 1$;
$H = Cl(K)^{1-\sigma} = 1$: we have $\mathfrak{b}^{1-\sigma} \sim \mathfrak{p} \sim 1$ and $\mathfrak{A}^{1-\sigma} \sim 1$. In particular, we have $s_0^* = 0$;
$\kappa = 0$, because there is only trivial capitulation in K/F.

Hasse's formula gives $r = 3$, although rank $Cl_2(K) = 2$.

The correct rank formula can be deduced as follows: let σ denote complex conjugation (hence σ is the non-trivial automorphism of K/K_0), and put $C = Cl_2(K)$, $r =$ rank C, $C_0 = Cl_2(K_0)$, and $H = Cl_2(K)^{1-\sigma}$. Then the formula $2 = 1 + \sigma + 1 - \sigma$ shows that $C^2 C^{1+\sigma} = C^{1-\sigma} C^{1+\sigma} = C_0^j H$ (the fact that also $C^2 C^{1-\sigma} = C_0^j H$ proves our previous claim that $s_0^* =$ rank

$H/H \cap Cl(K)^2$), and now we find

$$\begin{aligned} 2^r = (C : C^2) &= (C : C^2C^{1+\sigma})(C^2C^{1+\sigma} : C^2) \\ &= (C : C_0^j H)(C^2C_0^j : C^2) \\ &= \frac{(C : H)}{(C_0^j H : H)} (C_0^j : C_0^j \cap C^2) \end{aligned}$$

Now, $(C : H)$ equals the number of ideal classes in C fixed by σ, because

$$1 \to C^G \to C \to C^{1-\sigma} \to 1$$

is a short exact sequence (C^G is the subgroup of C fixed by $G = < \sigma >$). Moreover,

$$\begin{aligned} (C_0^j H : H) &= (C_0^j : C_0^j \cap H) \\ &= (C_0^j : {}_2C_0^j)({}_2C_0^j : C_0^j \cap H), \end{aligned}$$

where ${}_2G$ denotes the subgroup of elements of order ≤ 2 of an abelian group G. Let $c \in C_0^j \cap H$; then σ fixes c, and applying σ to the equation $c = d^{1-\sigma}$ yields $c = c^{-1}$, i.e. $c \in {}_2C_0^j$. Hasse claimed that in fact $C_0^j \cap H = {}_2C_0^j$: but an ideal class of order 2 is not necessarily of the form $d^{1-\sigma}$ for some $d \in C$. Actually, in the counterexamples presented above, $1-\sigma$ annihilates the whole 2-class group of K.

Using the ambiguous class number formula $(C : H) = 2^\gamma h_2(K_0)$, where γ was defined above, we find that

$$rank\ Cl_2(K) = \gamma + r_0^* + s_0^* + \kappa - \lambda,$$

with $2^\lambda = ({}_2C_0^j : C_0^j \cap H)$.

The main problem with this rank formula is the fact that λ usually is quite hard to compute. The trivial bounds $0 \leq \lambda \leq r_0^*$ yield

$$\gamma + s_0^* + \kappa \leq rank\ Cl_2(K) \leq \gamma + r_0^* + s_0^* + \kappa.$$

It should be noted that Hasse applied his formula only to fields K_0 with odd class number; we have already observed that in this case it coincides with the ambiguous class number formula, because then obviously $r_0^* = s_0^* = \kappa = 0$, and the formula simplifies to $rank\ Cl_2(K) = \gamma$.

ACKNOWLEDGMENTS

I would like to thank E. Benjamin and C. Snyder for sending me their preprint, and Prof. Kida for providing UBasic; the examples in this paper (and many more) have been computed with version 8.65. Prof. M. Olivier has kindly verified that the 2-class group of the quartic cyclic field $\mathbb{Q}\left(\sqrt{-10+3\sqrt{10}}\right)$ is cyclic of order 4 using PARI, and Prof. J. Martinet has suggested the possibility of bicyclic counterexamples to Hasse's rank formula.

REFERENCES

[1] E. Benjamin, C. Snyder, *Number fields with 2-class groups isomorphic to* $(2, 2^m)$, Austr. J. Math.

[2] M. Hall, J. K. Senior, *The groups of order* $2^n (n \leq 6)$;, Macmillan, New York (1964).

[3] H. Hasse, *Zahlbericht*, Physica Verlag, Würzburg, 1965.

[4] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, l Springer Verlag, Heidelberg.

[5] K. Iwasawa, *A note on the group of units of an algebraic number field*, . Math. pures appl. **35** (1956), 189–192.

[6] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. reine angew. Math. **283/284** (1974), 313–363.

[7] G. Karpilovsky, *The Schur multiplier*, London Math. Soc. monographs (1987), Oxford.

[8] H. Kisilevsky, *Number fields with class number congruent to* 4 mod 8 *and Hilbert's theorem 94*, J. Number Theory **8** (1976), 271–279.

[9] H. Koch, *Über den 2-Klassenkörperturm eines quadratischen Zahlkörpers*, J. reine angew. Math. **214/215** (1963), 201-206.

[10] F. Lemmermeyer, *Die Konstruktion von Klassenkörpern*, Diss. Univ. Heidelberg (1994).

[11] L. Rédei, H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. reine angew. Math. **170** (1933), 69–74.

[12] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - du^2 = -4$, Math. Z. **39** (1934), 95–111.

[13] A. Scholz, *Abelsche Durchkreuzung*, Monatsh. Math. Phys. **48** (1939), 340–352.

Franz Lemmermeyer
Institut für Mathematik
Universität Heidelberg
Im Neuenheimer Feld 288
69120 HEIDELBERG
ALLEMAGNE