Infinite class field towers of quadratic fields.

Schoof, René

Journal für die reine und angewandte Mathematik

Volume 372 / 1986 / Article

Infinite class field towers of quadratic fields

By *René Schoof* at Berkeley

§ 1. Introduction

Let K be an algebraic number field. We define a sequence of extensions of K as follows: Let $K_0 = K$ and for $n \geqq 0$ put $K_{n+1} =$ Hilbert class field of K_n. We have that

$$K = K_0 \subseteqq K_1 \subseteqq K_2 \subseteqq \cdots.$$

We call this sequence of fields the *class field tower* of K. The class field tower of K is called finite if $\bigcup_n K_n$ is a finite extension of K and infinite otherwise. For any prime number p we define a sequence of extensions of K as follows: Let $K_0^{(p)} = K$ and for $n \geqq 0$ put $K_{n+1}^{(p)} = p$-Hilbert class field of $K_n^{(p)}$, i.e., $K_{n+1}^{(p)}$ is the maximal abelian everywhere unramified p-extension of $K_n^{(p)}$. This sequence of fields $K_n^{(p)}$ is called the *p-class field tower* of K. The p-class field tower is said to be finite if $\bigcup_n K_n^{(p)}$ is a finite extension of K and infinite otherwise. It is easy to show that if K has a finite class field tower, then K has finite p-class field towers for all primes p.

In 1964 Golod and Šafarevič proved in [3] that there exist algebraic number fields which possess infinite class field towers. The existence of such fields is a consequence of a theorem on finite p-groups that they proved. The example they presented is the quadratic number field

$$K = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19}).$$

In fact, this field possesses an infinite 2-class field tower. In the extension $K/\mathbb{Q}$ eight finite primes are ramified.

In this paper we show how to obtain examples of quadratic number fields K with few primes ramified in the extension $K/\mathbb{Q}$ which possess infinite class field towers or even infinite 2-class field towers.

In section 2 we prove a refined version of the theorem of Golod and Šafarevič on finite p-groups. This refined theorem is due to Koch [5] and Vinberg [12]. We present our proof since our formulation differs from theirs and because our theorem is better suited for the application we give in section 4. Our proof is an adaptation of Gaschütz's proof which is presented by Roquette in [1]. In section 3 we prove the existence of infinitely many quadratic fields, both real and complex, with two ramified primes over $\mathbb{Q}$ and an infinite class field tower. We also prove the existence of infinitely many quadratic fields, both real and complex, with three ramified primes over $\mathbb{Q}$ and an infinite 2-class field tower. These results improve upon theorems of Koch [6] and Schmithals [10].

In section 4 we give some examples of quadratic fields, both real and complex, which have only one finite prime ramified over $\mathbb{Q}$ and which yet possess an infinite class field tower. Our result is a consequence of a generalization of a theorem of Koch and Venkov [7]. Finally in section 5, we give some examples of cyclotomic fields with infinite class field towers.

For the results from class field theory and cohomology of groups that we use see [1].

§ 2. The theorem of Koch and Vinberg

In this section we prove a refinement of the theorem of Golod and Šafarevič which is due to Koch [4], [5], [6] and Vinberg [12].

Let p be a prime number and let G be a finite p-group. Put

$$d = \dim_{\mathbb{F}_p} H_1(G, \mathbb{F}_p) \quad \text{and} \quad r = \dim_{\mathbb{F}_p} H_2(G, \mathbb{F}_p).$$

Let I denote the augmentation ideal of the group ring $\mathbb{F}_p[G]$; we have an exact sequence

$$0 \to I \to \mathbb{F}_p[G] \to \mathbb{F}_p \to 0$$

from which we obtain a canonical isomorphism

$$H_2(G, \mathbb{F}_p) \xrightarrow{\sim} H_1(G, I).$$

From the natural maps

$$\cdots \to H_1(G, I^3) \to H_1(G, I^2) \to H_1(G, I)$$

we obtain a filtration of $H_1(G, I)$ by the images of the $H_1(G, I^k)$; we denote the subquotients of this filtration by R_k:

$$R_k = \frac{\text{image}\,(H_1(G, I^{k-1}) \to H_1(G, I))}{\text{image}\,(H_1(G, I^k) \to H_1(G, I))} \qquad (k \geqq 2).$$

We put $r_k = \dim_{\mathbb{F}_p} R_k$; clearly only finitely many of the r_k's are nonzero and we have that $\sum_{k=2}^{\infty} r_k = r$. We will give a proof of the following theorem.

(2. 1) Theorem. *If G is a finite p-group then*

$$\sum_{k=2}^{\infty} r_k t^k - dt + 1 > 0 \quad \text{for} \quad 0 < t < 1.$$

Proof. In the notation from above we have that

$$d = \dim_{\mathbb{F}_p} H_1(G, \mathbb{F}_p) = \dim_{\mathbb{F}_p} H_0(G, I),$$

which implies that there exists F, a free $\mathbb{F}_p[G]$-module of rank d, mapping onto I; we obtain an exact sequence

$$0 \to A_0 \to F \to I \to 0.$$

By construction the canonical map $H_0(G, F) \to H_0(G, I)$ is an isomorphism; since $H_1(G, F) = 0$ we obtain from the long cohomology sequence a canonical isomorphism $H_1(G, I) \cong H_0(G, A_0)$.

We will construct a morphism $F_1 \twoheadrightarrow A_0$ with F_1 a free $\mathbb{F}_p[G]$-module of rank r. This morphism will have certain special properties.

From the above sequence we obtain a diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_0 & \longrightarrow & F & \longrightarrow & I & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & A_1 & \longrightarrow & IF & \longrightarrow & I^2 & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & A_2 & \longrightarrow & I^2F & \longrightarrow & I^3 & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

with exact rows. Here A_k denotes $I^k F \cap A_0$. Taking homology of the exact rows we obtain the following commutative diagram

$$\begin{array}{ccccc}
H_1(G, I) & \xrightarrow{\sim} & H_0(G, A_0) & \longrightarrow & H_0(G, F) \\
\uparrow & & \uparrow & & \uparrow \\
H_1(G, I^2) & \longrightarrow & H_0(G, A_1) & \longrightarrow & H_0(G, IF) \\
\uparrow & & \uparrow & & \uparrow \\
H_1(G, I^3) & \longrightarrow & H_0(G, A_2) & \longrightarrow & H_0(G, I^2F) \\
\uparrow & & \uparrow & & \uparrow \\
\vdots & & \vdots & & \vdots
\end{array}$$

with exact rows.

Next we construct a special set of $\mathbb{F}_p[G]$-generators of $A_0 \subset F$.

Choose $g_1^{(2)}, \ldots, g_{r_2}^{(2)}$ in $H_1(G, I)$ that form an $\mathbb{F}_p[G]$-basis for $R_2 = H_1(G, I)/\text{image}\, H_1(G, I^2)$; map these elements to $H_0(G, A_0) = A_0/IA_0$ and lift them to A_0; we will call the lifted elements $e_1^{(2)}, \ldots, e_{r_2}^{(2)}$; the $e_i^{(2)}$ are in IF since $H_1(G, I) \to H_0(G, A_0) \to H_0(G, F) = F/IF$ is the zero-map.

Choose $g_1^{(3)}, \ldots, g_{r_3}^{(3)}$ in $H_1(G, I^2)$ that map to an $\mathbb{F}_p[G]$-basis for R_3; map this basis to $H_0(G, A_1)$ and lift it to $A_1 \subset A_0$; call the lifted elements $e_1^{(3)}, \ldots, e_{r_3}^{(3)}$. These elements are in I^2F because $H_1(G, I^2) \to H_0(G, A_1) \to H_0(G, IF)$ is the zero-map. Etcetera.

After finitely many steps we obtain $r_2 + r_3 + \cdots = r$ elements in A_0 that generate A_0/IA_0 by construction; Nakayama's lemma implies that they generate A_0. We have that $e_1^{(k)}, \ldots, e_{r_k}^{(k)} \in I^{k-1}F$ for $k \geqq 2$.

Define for $k \geqq 2$ the module F_k to be a free $\mathbb{F}_p[G]$-module of rank r_k. Let $f_i^{(k)}$, $1 \leqq i \leqq r_k$, denote an $\mathbb{F}_p[G]$-basis for F_k. Define a map $F_k \to A_0$ by mapping $f_i^{(k)}$ to $e_i^{(k)}$ for $1 \leqq i \leqq r_k$. If we let $F_1 = \bigoplus_{k=2}^{\infty} F_k$ we obtain an exact sequence

$$F_1 = \bigoplus_{k=2}^{\infty} F_k \to F \to I \to 0$$

where $\text{image}(F_k) \subset I^{k-1}F$. From this exact sequence we deduce the exact sequences

$$\bigoplus_{k=2}^{i} F_k/I^{i-k+1}F_k \to F/I^iF \to I/I^{i+1} \to 0 \qquad (i \geqq 1)$$

and we obtain

$$\sum_{i=1}^{\infty} \sum_{k=2}^{i} \dim_{\mathbb{F}_p} F_k/I^{i-k+1}F_k \cdot t^i + \sum_{i=1}^{\infty} \dim_{\mathbb{F}_p} I/I^{i+1} \cdot t^i \geqq \sum_{i=1}^{\infty} \dim_{\mathbb{F}_p} F/I^iF \cdot t^i$$

for $0 < t < 1$. Note that all series converge because both I^m and F_m are zero if m is sufficiently large.

After changing the summation variables in the first sum we get

$$\sum_{k=2}^{\infty} t^k \cdot \sum_{i=0}^{\infty} \dim_{\mathbb{F}_p} F_k/I^{i+1}F_k \cdot t^i + \sum_{i=1}^{\infty} \dim_{\mathbb{F}_p} I/I^{i+1} \cdot t^i \geqq \sum_{i=1}^{\infty} \dim_{\mathbb{F}_p} F/I^iF \cdot t^i.$$

Let $P(t)$ denote $\sum_{i=0}^{\infty} \dim_{\mathbb{F}_p} I^i/I^{i+1} \cdot t^i \in \mathbb{Z}[t]$. Here $I^0 = \mathbb{F}_p[G]$ and we have that

$$\frac{P(t)}{1-t} = \sum_{i=0}^{\infty} \dim_{\mathbb{F}_p} \mathbb{F}_p[G]/I^{i+1} \cdot t^i$$

and for every free module M of rank m we get that

$$\sum_{i=0}^{\infty} \dim_{\mathbb{F}_p} M/I^{i+1}M \cdot t^i = \frac{mP(t)}{1-t}.$$

The modules F and F_k are free and substituting the above we get

$$\sum_{k=2}^{\infty} \frac{r_k \cdot t^k \cdot P(t)}{1-t} + \frac{P(t)-1}{1-t} \geqq \frac{t \cdot d \cdot P(t)}{1-t}$$

for $0<t<1$. From this we obtain

$$\sum_{k=2}^{\infty} r_k \cdot t^k - dt + 1 \geqq \frac{1}{P(t)} > 0,$$

since $P(t)$ is a polynomial with only positive coefficients. This proves Theorem (2. 1).

For any abelian group M, let $d_p M$ denote $\dim_{\mathbb{F}_p} M/pM$, the p-rank of M and let $M[p]$ denote $\{x \in M: px=0\}$. From the long homology sequence of the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{F}_p \to 0$ one easily obtains

$$d_p H_1(G, \mathbb{Z}) = d \quad \text{and} \quad d_p H_2(G, \mathbb{Z}) = r - d. \tag{2. 2}$$

It follows that $r \geqq d$ and substituting $t = \frac{d}{2r}$ in the inequality

$$rt^2 - dt + 1 \geqq \sum_{k=2}^{\infty} r_k t^k - dt + 1 > 0 \quad \text{for} \quad 0<t<1$$

one finds the following consequence of Theorem (2. 1).

(2. 3) Corollary (Vinberg-Gaschütz). *For every finite p-group G it holds that* $r > \frac{d^2}{4}$.

§ 3. Class group estimates

For an algebraic number field K, we denote by O_K its ring of integers, by E_K the units of this ring, by Cl_K the class group of O_K and by h_K the order of Cl_K. By U_K we denote the idèle units, i.e., the K-idèles which have trivial valuation at the finite places. Let C_K denote the idèle class group of K.

Let K be an algebraic number field, galois over a number field k with $\Delta = \mathrm{Gal}(K/k)$. Let p be a prime.

(3. 1) Proposition. *The p-rank of* Cl_K *satisfies*

$$d_p Cl_K \geqq d_p \hat{H}^0(\Delta, U_K) - d_p \Delta/[\Delta, \Delta] - d_p E_k/(E_k \cap N U_K).$$

Proof. From the long cohomology sequences of the exact sequences

$$0 \to E_K \to U_K \to U_K/E_K \to 0$$

and

$$0 \to U_K/E_K \to C_K \to Cl_K \to 0$$

one obtains

$$\begin{aligned} d_p Cl_K &\geqq d_p \hat{H}^{-1}(\Delta, Cl_K) \geqq d_p \hat{H}^0(\Delta, U_K/E_K) - d_p \hat{H}^0(\Delta, C_K) \\ &\geqq d_p \hat{H}^0(\Delta, U_K) - d_p \operatorname{im}(\hat{H}^0(\Delta, E_K) \to \hat{H}^0(\Delta, U_K)) - d_p \hat{H}^{-2}(\Delta, \mathbb{Z}) \\ &\geqq d_p \hat{H}^0(\Delta, U_K) - d_p E_k/(E_k \cap N U_K) - d_p \Delta/[\Delta, \Delta]. \end{aligned}$$

This proves the proposition.

It is well known that class field theory and an application of Corollary (2. 3) to the Galois group G of the maximal unramified p-extension of K imply that K has an infinite p-class field tower if

$$d_p Cl_K \geqq 2 + 2\sqrt{d_p E_K + 1}. \tag{3. 2}$$

(See [1], p. 235.)

A combination of (3. 2) and Proposition (3. 1) yields the following:

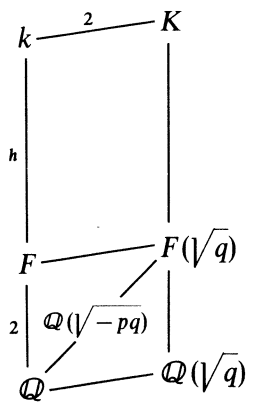
(3. 3) Proposition. *Let ϱ denote the number of finite and infinite primes of k ramified in K/k and assume that $\Delta = \mathrm{Gal}(K/k)$ is cyclic of order p. Then, K has an infinite p-class field tower if*

$$\varrho \geqq 3 + d_p E_k/(E_k \cap N U_K) + 2\sqrt{d_p E_K + 1}.$$

Proof. We have that $d_p \Delta/[\Delta, \Delta] = 1$ and that $\varrho = d_p \hat{H}^0(\Delta, U_K)$ by [1], pp. 104—142 and 177. This proves the proposition.

In the sequel, Proposition (3. 3) will be used to prove that certain fields have infinite p-class field towers.

(3. 4) Theorem. *There exists infinitely many complex quadratic number fields with two finite primes ramified over $\mathbb{Q}$ which have infinite class field towers.*



Proof. Let p be a prime congruent to 3 (mod 4); let $F = \mathbb{Q}(\sqrt{-p})$ and assume that $h = \# Cl_F \geqq 15$. Let k denote the Hilbert class field of F. Let q be a prime that splits completely in the extension $k(i)/\mathbb{Q}$; this is equivalent to q being congruent to 1 (mod 4) and being of the form $X^2 + XY + \frac{p+1}{4} Y^2$ for some $X, Y \in \mathbb{Z}$. Consider the extension $K = k(\sqrt{q})$ over k. In this extension all $2h$ primes over q ramify and they are the only ramified primes; so $\varrho = 2h$. We have that $d_2 E_K = 2 d_2 E_k = 2h$ since k is totally complex. Also $d_2 E_k/(E_k \cap N U_K) \leqq d_2 E_k = h$. According to Proposition (3. 3) the field K has an infinite 2-class field tower if $2h \geqq 3 + h + 2\sqrt{2h+1}$.

Since $h \geqq 15$, we conclude that K has an infinite class field tower. Since $K/(\mathbb{Q}(\sqrt{-pq}))$ is unramified we conclude that $\mathbb{Q}(\sqrt{-pq})$ has an infinite class field tower. The only primes that ramify in $\mathbb{Q}(\sqrt{-pq})$ over $\mathbb{Q}$ are p and q. We choose $p = 239$, then $h = 15$. By the Čebotarev density theorem there are infinitely many primes q that split completely in $k(i)/\mathbb{Q}$. This proves the theorem. An explicit example is provided by $\mathbb{Q}(\sqrt{-239 \cdot 1181})$ since $1181 = 15^2 + 2^2 \cdot 239$.

(3. 5) Remark. We can do slightly better in Theorem (3. 4) by observing that in the above situation it holds that

$$d_2 E_k/(E_k \cap N U_K) \leqq d_2 E_k - 1.$$

Proof. Since $F = \mathbb{Q}(\sqrt{-p})$ with p a prime, it follows that all roots of unity in k are in fact in F. Since -1 is a generator of the 2-part of the group of roots of unity in k, we clearly have that $d_2 E_k/(E_k \cap N U_K) \leqq d_2 E_k - 1$ if we prove that $-1 \in N U_K$. Since K/k is a quadratic extension it suffices to show that -1 is a square modulo the primes in k that ramify in K/k. The only primes that ramify in K/k are the primes in k over q. Since q is congruent to 1 (mod 4) we have that -1 is a square modulo every prime $\mathfrak{q}$ over q in K. This proves that $-1 \in N U_K$.

As in the proof of Theorem (3. 4) we find that K has an infinite 2-class field tower if $2h \geqq 3 + (h-1) + 2\sqrt{2h+1}$, i.e., $h \geqq 13$ instead of 15. An explicit example is $\mathbb{Q}(\sqrt{-191 \cdot 773})$. This field has an infinite 2-class field tower since $773 = 3^2 + 2^2 \cdot 191$. And $Cl_{\mathbb{Q}(\sqrt{-191})} \cong \mathbb{Z}/13\mathbb{Z}$.

(3. 6) Remark. In the proof of Theorem (3. 5) one can also take F to be a real quadratic field $\mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \pmod 4$ and take $K = k(\sqrt{-q})$ with $q \equiv 3 \pmod 4$ with q completely splitting in $k/\mathbb{Q}$. In this situation the *infinite* primes ramify in K/k as well and the analogous inequality involving h now becomes $4h \geqq 3 + 2h + 2\sqrt{2h+1}$, i.e., $h \geqq 5$. An example is provided by $\mathbb{Q}(\sqrt{-401 \cdot 83})$ because $Cl_{\mathbb{Q}(\sqrt{401})} \cong \mathbb{Z}/5\mathbb{Z}$ and $83 = 22^2 - 401$.

(3. 7) Theorem. *There exist infinitely many real quadratic number fields with two finite primes ramified over $\mathbb{Q}$ which have infinite class field towers.*

Proof. The proof differs in one respect from the proof of Theorem (3. 4). Let p be a prime congruent to 1 (mod 4). Let $F = \mathbb{Q}(\sqrt{p})$ have class number $\geqq 7$. Let k denote the Hilbert class field of F. As in Theorem (3. 5) we pick a prime q and we put $K = k(\sqrt{q})$. In this case, however, we require q to split completely in the field $k(\sqrt{E_k})$. We have in the same notation as before that $\varrho = 2h$ and $d_2 E_K = 4h$.

Claim. $E_k/(E_k \cap N U_K) = 0$.

Proof. The only primes that ramify in K/k are the primes over q since q splits in $k(\sqrt{-1})$ and so it is congruent to 1 (mod 4). It suffices to show that $E_k \subset U_{\mathfrak{q}}^2$ for all primes $\mathfrak{q}$ over q in k. This is immediate since q splits completely in $k(\sqrt{E_k})$. By Proposition (3. 3) the field K has an infinite 2-class field tower if $2h \geqq 3 + 0 + 2\sqrt{4h+1}$, i.e., if $h \geqq 7$. We conclude that $k(\sqrt{q})$ has an infinite 2-class field tower and this implies that $\mathbb{Q}(\sqrt{pq})$ has an infinite class field tower since $k(\sqrt{q})/\mathbb{Q}(\sqrt{pq})$ is unramified.

We take $p=577$, then $h=7$. By Čebotarev's density theorem there are infinitely many primes that split completely in the extension $k(\sqrt{E_k})$ over $\mathbb{Q}$. (This is an extension of degree $7 \cdot 2^{15}$.) This proves the theorem.

(3. 8) Theorem. *There exist infinitely many real quadratic fields with only three primes ramified over $\mathbb{Q}$ and an infinite 2-class field tower.*

Proof. In the notation of the proof of Theorem (3. 7), we take $F=\mathbb{Q}(\sqrt{226})$; we have that $h=8$. Let q be a prime that splits completely in $k(\sqrt{E_k})/\mathbb{Q}$; here k denotes the Hilbert class field of F. As before the field $k(\sqrt{q})$ has an infinite 2-class field tower. Since $k(\sqrt{q})/\mathbb{Q}(\sqrt{226q})$ is an unramified 2-*extension*, we conclude that $\mathbb{Q}(\sqrt{226q})$ has an infinite 2-class field tower as well. By Čebotarev's theorem there exist infinitely many primes q with the indicated properties. This proves the theorem.

The corresponding result for complex quadratic fields was proved by Schmithals [10].

(3. 9) Theorem. $K=\mathbb{Q}(\sqrt{226 \cdot 7002157954478808257})$ *has an infinite 2-class field tower. In $K/\mathbb{Q}$ only three primes are ramified.*

"*Proof*". One checks that the Hilbert class field k of $\mathbb{Q}(\sqrt{226})$ equals $\mathbb{Q}(\sqrt{2}, \alpha, \beta, \gamma)$ where

$$\alpha^2-(1+\sqrt{2})\alpha-2=0,$$
$$\beta^2-(1-\sqrt{2})\beta-2=0,$$
$$\gamma^2-(1-\alpha\sqrt{2})\gamma-(1+\sqrt{2})=0.$$

Let $x \in O_k$ such that $N_{k/\mathbb{Q}}(4x^2+1)=p$ a prime. Clearly $4x^2+1$ generates a prime ideal. The conductor of $\mathbb{Q}(\sqrt{\varepsilon})$ divides $4 \cdot$ (infinite primes) for every unit $\varepsilon \in E_k$ so, since $4x^2+1$ is totally positive and congruent to 1 (mod 4) the prime p splits completely in every field $k(\sqrt{\varepsilon})$ and hence in $k(\sqrt{E_k})$. We conclude that $\mathbb{Q}(\sqrt{226 \cdot p})$ is a real quadratic field which has an infinite 2-class field tower and only three primes ramified over $\mathbb{Q}$.

For $x=\sqrt{2}+\beta+\gamma$ we have that $N_{k/\mathbb{Q}}(4x^2+1)=7002157954478808257$ which is a prime.

§ 4. The theorem of Koch and Venkov

In this section we prove a generalization of a theorem of Koch and Venkov [7]. Let K be a quadratic number field (either real or complex). Let p be an odd prime and $\Delta=\mathrm{Gal}(K/\mathbb{Q})$ and let σ be the generator of Δ.

Assume that K has a finite p-class field tower; let L denote the maximal unramified p-extension of K; put $G=\mathrm{Gal}(L/K)$. Since $L/\mathbb{Q}$ is a Galois extension, the group Δ acts in a natural way on all G-cohomology groups. We will exploit the action of Δ on these cohomology groups.

(4. 1) Lemma. *σ acts as -1 on $H_1(G, \mathbb{F}_p)$ and $H_2(G, \mathbb{F}_p)$.*

Proof. Consider the Δ-norm map:

$$N: Cl_K \to Cl_{\mathbb{Q}} \to Cl_K,$$
$$N: E_K/E_K^p \to E_{\mathbb{Q}}/E_{\mathbb{Q}}^p \to E_K/E_K^p.$$

Since $Cl_{\mathbb{Q}} = 0$ and $E_{\mathbb{Q}}/E_{\mathbb{Q}}^p = (\pm 1)/(\pm 1)^p = 0$, we see that the norm annihilates Cl_K and E_K/E_K^p; in other words, σ acts as -1 on both of these groups. From the homology of the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{F}_p \to 0$ we obtain

$$H_1(G, \mathbb{F}_p) \xrightarrow{\sim} H_1(G, \mathbb{Z})/pH_1(G, \mathbb{Z})$$

and an exact sequence

$$0 \to H_2(G, \mathbb{Z})/pH_2(G, \mathbb{Z}) \to H_2(G, \mathbb{F}_p) \to H_1(G, \mathbb{Z})[p] \to 0.$$

We have, as follows from the proof of (3. 2) in [1], p. 235,

$$H_1(G, \mathbb{Z}) \cong Cl_K$$

and

$$E_K/E_K^p \twoheadrightarrow \hat{H}^0(G, E_L) = H_2(G, \mathbb{Z}).$$

We obtain an isomorphism

$$H_1(G, \mathbb{F}_p) \xrightarrow{\sim} Cl_K/Cl_K^p$$

and an exact sequence

$$E_K/E_K^p \to H_2(G, \mathbb{F}_p) \to Cl_K[p] \to 0.$$

All morphisms are Δ-morphisms. Since σ acts as -1 on both Cl_K and E_K/E_K^p and since $p \neq 2$, we conclude that σ acts as -1 on $H_1(G, \mathbb{F}_p)$ and $H_2(G, \mathbb{F}_p)$. This proves Lemma (4. 1).

(4. 2) Lemma. *σ acts as $(-1)^k$ on R_k.*

Proof. We recall that

$$R_k = \frac{\text{image}(H_1(G, I^{k-1}) \to H_1(G, I))}{\text{image}(H_1(G, I^k) \to H_1(G, I))}.$$

From the exact sequence

$$\to H_1(G, I^k) \to H_1(G, I^{k-1}) \to H_1(G, I^{k-1}/I^k) \to$$

we obtain

$$R_k \twoheadleftarrow \frac{H_1(G, I^{k-1})}{\text{im}\, H_1(G, I^k)} \hookrightarrow H_1(G, I^{k-1}/I^k).$$

Again, all morphisms are Δ-morphisms and the action of Δ on R_k is induced by the action of Δ on $H_1(G, I^{k-1}/I^k)$. We have that

$$H_1(G, I^{k-1}/I^k) \cong I^{k-1}/I^k \otimes I/I^2 \leftarrow\!\!\!\!\!\!\leftarrow (I/I^2)^{\otimes k}$$

because I^{k-1}/I^k has trivial G-action. We also have that $I/I^2 \cong G/[G, G]G^p \cong Cl_K/Cl_K^p$. Since σ acts as -1 on Cl_K/Cl_K^p by Lemma (4. 1), we see that σ acts as $(-1)^k$ on $H_1(G, I^{k-1}/I^k)$ whence on R_k. This proves Lemma (4. 2).

(4. 3) Theorem. *Let K be a quadratic field and let p be an odd prime. If $d_p Cl_K \geqq 3$ then K has an infinite p-class field tower.*

Proof. Assume that K has a finite p-class field tower and adopt the notation introduced at the beginning of this section. Put $d = d_p Cl_K$. We claim that the group R_k is zero whenever k is even: Lemma (4. 1) implies that R_k, being a subquotient of $H_2(G, \mathbb{F}_p)$ is acted upon by σ via -1, but, on the other hand, Lemma (4. 2) says that σ acts via $+1$ on R_k whenever k is even. Since $p \neq 2$, we conclude that $R_k = 0$. By Theorem (2. 1) we have that

$$0 < \sum_{k=2}^{\infty} r_k t^k - dt + 1 \leqq rt^3 - dt + 1 \quad \text{for} \quad 0 < t < 1$$

since in particular $r_2 = 0$. By (2. 2) we have that

$$r - d \leqq d_p H_2(G, \mathbb{Z}) \leqq d_p E_K \leqq 1$$

since K is a quadratic field. We obtain

$$(d+1)t^3 - dt + 1 > 0 \quad \text{for} \quad 0 < t < 1.$$

Substituting $t = \frac{1}{2}$ gives that $d < 3$ which proves the theorem.

Remark. We did not use all of Theorem (2. 1); we merely needed that $r_2 = 0$. A direct application of (3. 2) would give that for odd primes p the finiteness of the class field tower of K implies that $d_p Cl_K < 4$ for complex quadratic fields K and that $d_p Cl_K < 5$ for real quadratic K. For quadratic extensions of a complex quadratic field one can show an analogous result:

Let p be an odd prime and let k be a complex quadratic field not equal to $\mathbb{Q}(\sqrt{-3})$ and with p not dividing its class number. Every quadratic extension K of k with $d_p Cl_K \geqq 3$ has an infinite p-class field tower.

(4. 4) Corollary. *There exist quadratic fields, both real and complex, with only one finite prime ramified over $\mathbb{Q}$ and an infinite class field tower.*

Proof. It suffices, in view of Theorem (4. 3), to give examples of quadratic fields K with prime discriminant and $d_p Cl_K \geqq 3$ for some odd prime p. Some examples are

$$K_1 = \mathbb{Q}(\sqrt{-3321607}) \qquad d_3 Cl_K = 3 \quad \text{cf. [2]},$$
$$K_2 = \mathbb{Q}(\sqrt{39345017}) \qquad d_3 Cl_K = 3 \quad \text{cf. [2]},$$
$$K_3 = \mathbb{Q}(\sqrt{-222637549223}) \quad d_5 Cl_K = 3 \quad \text{cf. [11]},$$

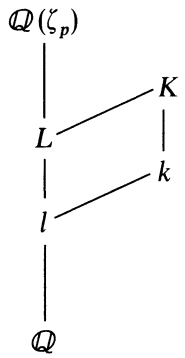
I don't know whether there exist infinitely many quadratic fields with prime discriminants and infinite class field towers.

§ 5. A cyclotomic field with small prime conductor and an infinite class field tower

In this section we give an example of a prime p such that $\mathbb{Q}(\zeta_p)$ has an infinite class field tower. Of course, one can obtain examples like that by taking p a prime such that $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$ has an infinite class field tower. In this way I can only get examples with p large. In this example the conductor is rather small. We prove the following theorem.

(5. 1) Theorem. *The field $\mathbb{Q}(\zeta_{877})$ has an infinite class field tower.*

Proof. The number $p = 877 = 1 + 12 \cdot 73$ is prime. Let l denote the unique subfield of $\mathbb{Q}(\zeta_p)$ of degree 6 over $\mathbb{Q}$ and let L denote the unique subfield of degree 12 of $\mathbb{Q}(\zeta_p)$. We let k be the Hilbert class field of l and we put $K = L \cdot k$. By Mäki [8], the class number of l equals 49. Since the prime $\mathfrak{p}$ over p in l is principal it splits completely in the Hilbert class field k of l. In the extension K/k all $6 \cdot 49$ infinite primes and all 49 primes over $\mathfrak{p}$ ramify. Since $d_2 E_K = d_2 E_k = 6 \cdot 49$ it follows from Proposition (3. 3) that K has an infinite class field tower. Since K/L is unramified and since $L \subset \mathbb{Q}(\zeta_p)$ we see that $\mathbb{Q}(\zeta_p)$ has an infinite class field tower as well. This proves the theorem.



Finally, we mention the cyclotomic field with smallest conductor that we know has an infinite class field tower. It is the field $\mathbb{Q}(\zeta_{363})$. One can prove that $\mathbb{Q}(\zeta_{363})$ has an infinite class field tower by considering the extension K/k where k denotes the unique subfield of degree 11 over $\mathbb{Q}$ in $\mathbb{Q}(\zeta_{121})$ and $K = k(\sqrt{-3})$. Proposition (3. 3) applies in this case and one concludes that $k(\sqrt{-3})$ and $\mathbb{Q}(\zeta_{363})$ have infinite class field towers.

References

[1] *J. W. S. Cassels* and *A. Fröhlich* eds., Algebraic Number Theory, London 1967.
[2] *F. Diaz y Diaz*, Sur le 3-rang des corps quadratiques, Thèse 3° cycle, Paris 1978.
[3] *E. S. Golod* and *I. R. Šafarevič*, On Class Field Towers, Izv. Ak. Nauk. SSSR **28** (1964), 273—276 (russian), AMS Translations **48** (1965), 91—102.
[4] *K. Haberland*, Galois cohomology of number fields, Berlin 1978.
[5] *H. Koch*, Zum Satz von Golod-Schafarewitsch, Math. Nachr. **42** (1969), 321—333.
[6] *H. Koch*, Galoissche Theorie der p-Erweiterungen, Berlin 1970.
[7] *H. Koch* und *B. B. Venkov*, Über den p-Klassenkörperturm eines imaginär quadratischen Zahlkörpers, Astérisque **24/25** (1975), 57—67.
[8] *S. Mäki*, The determination of units in real cyclic sextic fields, Lecture Notes in Math. **797**, Berlin-Heidelberg-New York 1980.
[9] *N. Matsumura*, On the class field tower of an imaginary quadratic number field, Mem. Fac. Sci. Kyushu Univ. A **31** (1977), 165—177.
[10] *B. Schmithals*, Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm, Archiv. Math. **34** (1980), 307—312.
[11] *R. J. Schoof*, Class groups of complex quadratic fields, Math. Comp. **44** (1983), 295—302.
[12] *E. B. Vinberg*, On the dimension theorem of associative algebras, Izv. Ak. Nauk. SSSR **29** (1965), 209—214 (russian).

Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, Calif. 94720, USA

Eingegangen 16. Dezember 1985, in revidierter Form 2. Mai 1986