

ON THE 2-CLASS FIELD TOWER OF A QUADRATIC NUMBER FIELD

HELMUT KOCH

1. INTRODUCTION

Let $k = k^{(0,2)}$ be a quadratic number field with discriminant Δ . For $n \geq 0$, we define fields $k^{(n,2)}$ inductively by taking $k^{(n+1,2)}$ as the compositum of all unramified¹ quadratic extensions of $k^{(n,2)}$ that are central over k . Then $k^{(\infty)} = \bigcup_{n=0}^{\infty} k^{(n,2)}$ is the 2-class field tower of k . In the following, we call $k^{(n,2)}$ the n^{th} central 2-step.

The structure of the Galois group $\text{Gal}(k^{(1,2)}/k)$ of the first central 2-step is determined by the principal genus theorem. We want to show (Theorem 1 and 3), that $\text{Gal}(k^{(2,2)}/k)$ is determined completely by the values of the Legendre symbols $(\frac{a}{p})$, where $a \mid \Delta$ and $p \mid \Delta$. Known results in this direction are the theorem of L. Rédei and H. Reichardt [4] on the invariants of the class group of k divisible by 4, as well as a sufficient condition by A. Fröhlich [2] for the class field tower of k to be non-abelian.

Moreover we investigate in which cases the 2-class field tower terminates after the first and second central 2-step, i.e., when $k^{(\infty)} = k^{(1,2)}$ and $k^{(\infty)} = k^{(2,2)}$, respectively. According to A. Fröhlich [2], we have $k^{(\infty)} \neq k^{(1,2)}$ if Δ has more than three prime divisors. In the case where Δ has two prime divisors, the theorem of Rédei and Reichardt gives rise to a necessary and sufficient condition for $k^{(\infty)} \neq k^{(1,2)}$. In this paper, we give a necessary and sufficient condition for $k^{(\infty)} \neq k^{(1,2)}$ in the remaining case where Δ has three prime divisors (Theorem 4) and show that the 2-class field tower terminates after the second central 2-step if $\text{Gal}(k^{(2,2)}/k)$ is the quaternion group (Theorem 5).

In part II of this paper we shall prove that $k^{(\infty)} \neq k^{(2,2)}$ if Δ has more than four prime divisors. If Δ has exactly four prime divisors, then the 2-class field tower stops for some groups $\text{Gal}(k^{(2,2)}/k)$ of order 32 after the second central 2-step. In all other cases we have $k^{(\infty)} \neq k^{(2,2)}$.

I would like to thank Professor H. Reichardt for some very valuable suggestions.

2. NOTATION

A prime discriminant p^* is an integer of the form

$$(-1)^{\frac{p-1}{2}} p, -4, \pm 8,$$

where p is an odd prime. Every discriminant of a quadratic number field can be written uniquely as a product of prime discriminants. The prime $|p^*|$ will be denoted by p .

¹In this note, we only consider ramification at finite primes.

Let \mathbb{Q} be the field of rational numbers. We define a symbol $[\Delta, p]$ for discriminants Δ of quadratic number fields and primes p : write $\Delta = \Delta' p^{*\nu}$, where $(\Delta', p) = 1$ and $\nu \in \{0, 1\}$. Then we put $[\Delta, p] = 1$ or $= 0$ according as p is inert or split in $\mathbb{Q}(\sqrt{\Delta'})/\mathbb{Q}$; we also put $[p^*, p] = 0$. If p is unramified in $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$, then we have the relation

$$\left(\frac{\Delta}{p}\right) = (-1)^{[\Delta, p]}$$

between $[\Delta, p]$ and the Legendre symbol $\left(\frac{\Delta}{p}\right)$.

Let $k = k_S^{(0)} = k_S^{(0,2)}$ be a number field and S a set of finite primes of k . We then define the fields $k_S^{(n)}$ ($k_S^{(n,2)}$) for $n \geq 0$ recursively. Let $k_S^{(n+1)}$ ($k_S^{(n+1,2)}$) be the compositum of all cyclic extensions of $k_S^{(n)}$ ($k_S^{(n,2)}$) of degree a power of 2 (of degree 2) that are unramified outside S and central over k . Then

$$\bigcup_{n=0}^{\infty} k_S^{(n)} = \bigcup_{n=0}^{\infty} k_S^{(n,2)} = k_S^{(\infty)}.$$

Let $G = G^{(0)} = G^{(0,2)}$ be an arbitrary group. We define recursively two central series $G^{(n)}$ and $G^{(n,2)}$ by

$$G^{(n+1)} = [G, G^{(n)}], \quad G^{(n+1,2)} = \langle (G^{(n,2)})^2, [G, G^{(n,2)}] \rangle,$$

where $[G, G^{(n)}]$ denotes the commutator group of G and $G^{(n)}$, and where $(G^{(n,2)})^2$ is the group generated by the squares of $G^{(n,2)}$.

Let K/k be a finite normal extension unramified outside S . Then $\text{Gal}(K/k)$ and $k_S^{(n)}$ are connected by the relation

$$(1) \quad \text{Gal}(K/k)^{(n)} = \text{Gal}(K/K \cap k_S^{(n)}).$$

Accordingly, we have

$$(2) \quad \text{Gal}(K/k)^{(2,2)} = \text{Gal}(K/K \cap k_S^{(n,2)}).$$

3. GROUP THEORETICAL PRELIMINARIES

We first prove two group-theoretical lemmas:

Lemma 1. *Let G be an arbitrary group with generators s_1, \dots, s_n , and let H be the normal subgroup of G generated by $(G)^2$ and $s_1 s_2, s_1 s_3, \dots, s_1 s_n$. Moreover, let L denote the normal subgroup of G generated by s_1^2, \dots, s_n^2 . Then*

$$LG^{(2)} = LG^{(2,2)} = LH^{(2,2)}.$$

Proof. We first prove that $LG^{(2)} = LG^{(2,2)}$. The inclusion $LG^{(2)} \subseteq LG^{(2,2)}$ holds trivially. Thus it suffices to prove that $G^{(2,2)} \subseteq LG^{(2)}$. The elements $s \in G^{(1,2)}$ can be written in the form

$$s = t \prod_{\nu=1}^n s_{\nu}^{2a_{\nu}}, \quad t \in G^{(1)}.$$

Then $s^2 \equiv t^2 \pmod{LG^{(2)}}$, and t is congruent modulo $G^{(2)}$ to a product of commutators of the form $[s_{\nu}, s_{\mu}] = s_{\nu} s_{\mu} s_{\nu}^{-1} s_{\mu}^{-1}$. For the proof of $G^{(2,2)} \subseteq LG^{(2)}$ it is therefore sufficient to show that

$$[s_{\nu}, s_{\mu}]^2 \equiv 1 \pmod{LG^{(2)}}.$$

In fact, we have

$$[s_\nu, s_\mu]^2 \equiv s_\nu [s_\nu, s_\mu] s_\mu s_\nu^{-1} s_\mu^{-1} \equiv 1 \pmod{LG^{(2)}}.$$

Next we prove that $LG^{(2,2)} = LH^{(2,2)}$. It is sufficient to prove the claim for free groups G . Trivially, we have $LH^{(2,2)} \subseteq LG^{(2,2)}$. Moreover, H/L is a group with $n-1$ generators $s_1 s_2 L, \dots, s_1 s_n L$. According to [3], the group

$$(H/L)^{(1,2)} / (H/L)^{(2,2)} \simeq LH^{(1,2)} / LH^{(2,2)}$$

has order at most $2^{n(n-1)/2}$. Again according to [3], we have $(G^{(1,2)} : G^{(2,2)}) = 2^{n(n+1)/2}$.

The elements $s \in L$ have the form

$$s \equiv \prod_{\nu=1}^n s_\nu^{2a_\nu} \pmod{G^{(2,2)}}.$$

Therefore, $(LG^{(2,2)} : G^{(2,2)}) = 2^n$, hence

$$(G^{(1,2)} : LG^{(2,2)}) = 2^{n(n-1)/2}.$$

Moreover, $(G : H) = 2$, $(G : G^{(1,2)}) = 2^n$, $(H : LH^{(1,2)}) = 2^{n-1}$ and $(H : G^{(1,2)}) = 2^{n-1}$. This implies that

$$(H : LH^{(2,2)}) \leq (H : LG^{(2,2)}).$$

Since $LH^{(2,2)} \subseteq LG^{(2,2)}$, the claim follows. \square

Lemma 2. *Let G be a group whose quotient group mod $G^{(2,2)}$ is isomorphic to the quaternion group Q . Then $G = Q$.*

Proof. The group Q has two generators t_1, t_2 and relations

$$t_1^2 t_2^2 = 1, \quad t_1^2 [t_1, t_2] = 1, \quad Q^{(2,2)} = \{1\}.$$

Therefore, G is a group with two generators s_1 and s_2 , and we have the relations

$$(3) \quad s_1^2 s_2^2 \equiv 1 \pmod{G^{(2,2)}},$$

$$(4) \quad s_1^2 [s_1, s_2] \equiv 1 \pmod{G^{(2,2)}}.$$

From (3) we deduce

$$\begin{aligned} (s_1^2 s_2^2)^2 &\equiv s_1^4 s_2^4 \equiv 1 \pmod{G^{(3,2)}}, \\ [s_1^2 s_2^2, s_1] &\equiv [s_2^2, s_1] \equiv [s_1, s_2]^2 [[s_1, s_2], s_2] \equiv 1 \pmod{G^{(3,2)}}, \\ [s_1^2 s_2^2, s_2] &\equiv [s_1^2, s_2] \equiv [s_1, s_2]^2 [[s_1, s_2], s_1] \equiv 1 \pmod{G^{(3,2)}}. \end{aligned}$$

From (4) we get

$$\begin{aligned} (s_1^2 [s_1, s_2])^2 &\equiv s_1^4 [s_1, s_2]^2 \equiv 1 \pmod{G^{(3,2)}} \\ [s_1^2 [s_1, s_2], s_1] &\equiv [[s_1, s_2], s_1] \equiv 1 \pmod{G^{(3,2)}}. \end{aligned}$$

This implies that the elements $s_1^4, s_2^4, [s_1, s_2]^2, [[s_1, s_2], s_1], [[s_1, s_2], s_2]$ are in $G^{(3,2)}$. On the other hand, according to [3] these elements generate $G^{(2,2)} \pmod{G^{(3,2)}}$. Thus $G^{(2,2)} = G^{(3,2)}$. This implies by induction that $G^{(2,2)} = G^{(n,2)}$ for all $n \geq 2$. Since $\bigcap_{n=2}^{\infty} G^{(n,2)} = \{1\}$, we see that $G^{(2,2)} = 1$, which is what we wanted to prove. \square

4. THE MAIN RESULT

Now we can prove the main result of this note.

Theorem 1. *Let k be a quadratic number field with discriminant $\Delta = p_1^* \cdots p_n^*$. Then the Galois group $G = \text{Gal}(k^{(2,2)}/k)$ has $n - 1$ generators s_1, \dots, s_{n-1} satisfying the relations*

$$(5) \quad \begin{aligned} G^{(2,2)} &= 1 \\ \prod_{\nu=1}^{n-1} (s_\nu^2 [s_\nu, s_\mu])^{[p_\nu^*, p_\mu]} &= s_\mu^{2[\Delta, p_\mu]}, \quad \mu = 1, \dots, n-1 \\ \prod_{\nu=1}^{n-1} s_\nu^{2[p_\nu^*, p_n]} &= 1. \end{aligned}$$

Proof. Set $S = \{p_1, \dots, p_n\}$. According to Fröhlich [1], $\text{Gal}(k^{(\infty)} \cap \mathbb{Q}_S^{(2)}/\mathbb{Q})$ is a finite group with n generators t_1, \dots, t_n and relations

$$(6) \quad \begin{aligned} \text{Gal}(k^{(\infty)} \cap \mathbb{Q}_S^{(2)}/\mathbb{Q})^{(2)} &= \{1\}, \\ t_\mu^2 &= 1, \quad \mu = 1, \dots, n, \\ \prod_{\nu=1}^n [t_\nu, t_\mu]^{[p_\nu^*, p_\mu]} &= 1, \quad \mu = 1, \dots, n. \end{aligned}$$

Here t_μ is a generator of the inertia subgroup of a prime divisor \mathfrak{p}_μ of p_μ in $k^{(\infty)} \cap \mathbb{Q}_S^{(2)}/\mathbb{Q}$.

Put $K = (k^{(\infty)} \cap \mathbb{Q}_S^{(2)})k^{(2,2)}$. We show next that $k^{(\infty)} \cap \mathbb{Q}_S^{(2)} = k^{(2,2)} = K$. By the principal genus theorem we have $k^{(1,2)} \subseteq \mathbb{Q}_S^{(2)}$. Therefore, the group $G = \text{Gal}(K/\mathbb{Q})$ is generated by lifts $\bar{t}_1, \dots, \bar{t}_n$ of the automorphisms t_1, \dots, t_n to K . We choose the \bar{t}_μ as generators of the inertia groups of a prime divisor of \mathfrak{p}_μ in K/\mathbb{Q} , $\mu = 1, \dots, n$. We also put $H = \text{Gal}(K/k)$ and $L = \text{Gal}(K/K \cap k^{(\infty)})$. By Hilbert's theory of ramification, L is the normal closure in G of the group generated by the elements $\bar{t}_1^2, \dots, \bar{t}_n^2$, and H is generated as a normal subgroup of G by $(G)^2$ and $\bar{t}_1 \bar{t}_2, \dots, \bar{t}_1 \bar{t}_n$.

Since only primes in S ramify in K/\mathbb{Q} , we have $G^{(2)} = \text{Gal}(K/\mathbb{Q}_S^{(2)} \cap K)$, hence

$$(7) \quad G^{(2)}L = \text{Gal}(K/k^{(\infty)} \cap \mathbb{Q}_S^{(2)}).$$

Now (2) implies $H^{(2,2)} = \text{Gal}(K/k^{(2,2)})$, and $k^{(2,2)} \subseteq K \cap k^{(\infty)}$ implies $L \subseteq H^{(2,2)}$. Thus

$$(8) \quad H^{(2,2)}L = \text{Gal}(K/k)^{(2,2)}.$$

Now we apply Lemma 1 to G . It follows from (7) and (8) that $k^{(2,2)} = \mathbb{Q}_S^{(2)} \cap k^{(\infty)} = K$.

Now put $s_\nu = t_\nu t_n$ for $\nu = 1, \dots, n-1$. Then a simple calculation transforms the relations (6) into (5). According to (2), we have $\text{Gal}(k^{(2,2)}/k)^{(2,2)} = 1$; this implies that $\text{Gal}(k^{(2,2)}/k)^{(2)} = \{1\}$, and the proof of Theorem 1 is complete. \square

According to Theorem 1, all invariants of the 2-class group of k in the strict sense are divisible by 4 if and only if $[p_\nu^*, p_\mu] = 0$ for all $\nu, \mu = 1, \dots, n$. In this case, all relations (5) vanish, and we have proved the following

Corollary 1. *Let k be a quadratic number field with discriminant $\Delta = p_1^* \cdots p_n^*$. Assume that the invariants of the 2-class group of k in the strict sense are all divisible by 4. Then the Galois group of $k^{(2,2)}/k$ is relative free, i.e., $\text{Gal}(k^{(2,2)}/k)$ is isomorphic to $F/F^{(2,2)}$, where F is a free group with $n - 1$ generators.*

Theorem 1 describes the structure of $\text{Gal}(k^{(2,2)}/k)$ completely. It is, however, interesting to find a more visible relation between the group structure of $\text{Gal}(k^{(2,2)}/k)$ and the values of $[\Delta, p]$. In this direction, L. Rédei and H. Reichardt have proved the following

Theorem 2. *Let Δ be the discriminant of a quadratic number field and $\Delta_1 \Delta_2 = \Delta$, $(\Delta_1, \Delta_2) = 1$ a factorization of Δ into discriminants. Then $\mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2})/\mathbb{Q}(\sqrt{\Delta})$ can be embedded into a cyclic unramified extension of degree 4 over $\mathbb{Q}(\sqrt{\Delta})$ if*

$$\left(\frac{\Delta_2}{p_1}\right) = \left(\frac{\Delta_1}{p_2}\right) = 1$$

for all primes $p_1 \mid \Delta_1$ and $p_2 \mid \Delta_2$.

Since $k^{(2,2)}/k$ is the compositum of fields whose Galois groups have two generators, an analogue of the theorem of Rédei and Reichardt will be based on a factorization of Δ into three discriminants which, however, need not be coprime. We then have to investigate in which cases the extension $\mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \sqrt{\Delta_3})/\mathbb{Q}(\sqrt{\Delta})$ with Klein's four group as Galois group can be embedded into an unramified extension with given Galois group G , where G has two generators and satisfies $G^{(2,2)} = \{1\}$. In this way, we get

Theorem 3. *Let k be a quadratic number field with discriminant Δ and let $\Delta_1 \Delta_2 \Delta_3 = \Delta \Delta'^2$ be a factorization of Δ into three discriminants with $\Delta_\nu = \Delta'_\nu \Delta'$, $(\Delta'_\nu, \Delta'_\mu) = 1$ for $\nu \neq \mu$. Moreover, let t_ν denote an automorphism of $k^{(2,2)}/\mathbb{Q}$ mapping $\sqrt{\Delta_\nu} \mapsto -\sqrt{\Delta_\nu}$ and fixing $\sqrt{\Delta_\mu}$ for $\mu \neq \nu$, $\mu, \nu = 1, 2, 3$.*

Then $\mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2})/k$ can be embedded into a field K with Galois group $G = \text{Gal}(K/k)$ if and only if the following conditions A are satisfied:

G	A
1. $G \simeq (4, 2)$ commutative $(t_1 t_2)^2 = 1$	$[\Delta_3, p_1] = [\Delta_3, p_2] = 0,$ $[\Delta_1 \Delta_2, p_3] = 0, [\Delta_1 \Delta_2, p'] = 0$
2. $G \simeq H_8$ quaternion	$[\Delta_2 \Delta_3, p_1] = [\Delta_1 \Delta_3, p_2] = [\Delta_1 \Delta_2, p_3] = 0$
3. G dihedral $(t_1 t_2)^2 = 1, (t_1 t_3)^2 = 1$	$[\Delta_3, p_2] = [\Delta_2, p_3] = 0$ $[\Delta_2 \Delta_3, p'] = 0$
4. G group of order 16 $(t_1 t_2)^2 = 1$	$[\Delta_3, p_1] = [\Delta_3, p_2] = 0,$ $[\Delta_1, p_3] = [\Delta_2, p_3] = 0,$ $[\Delta_1 \Delta_3, p'] = [\Delta_2 \Delta_3, p'] = 0$
5. G group of order 16 $(t_1 t_2)^2 = 1$	$[\Delta_1, p_2] = [\Delta_1, p_3] = 0,$ $[\Delta_3, p_2] = [\Delta_2, p_3] = 0,$ $[\Delta_2 \Delta_3, p_1] = [\Delta_2 \Delta_3, p'] = 0$
6. $G \simeq (4, 4)$ commutative	$[\Delta_i, p_j] = 0, i, j = 1, 2, 3$
7. G group of order 32, rel. free	$[\Delta_1 \Delta_2, p'] = [\Delta_1 \Delta_3, p'] = 0$

Here p_ν runs through all primes dividing $\Delta_\nu u'$, $\nu = 1, 2, 3$, and p' runs through the primes dividing Δ' .

Proof. Let $\Delta'_\nu = \prod_{t_\nu \in J_\nu} p_{\nu i_\nu}^*$ and $\Delta' = \prod_{i \in J} p_i'^*$ the factorizations into prime discriminants of Δ'_ν and Δ' , respectively. Let $t_{\nu i_\nu}$ be an automorphism of $k^{(2,2)}/\mathbb{Q}$ mapping $\sqrt{p_{\nu i_\nu}^*} \mapsto -\sqrt{p_{\nu i_\nu}^*}$ and leaving $\sqrt{p^*}$ fixed for all other prime divisors p^* of Δ . Define t'_i correspondingly. Then the restrictions of $t_{\nu i_\nu}$ and t_ν (t'_i and $t_1 t_2 t_3$) to $\mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \sqrt{\Delta_3})$ coincide. By (6), the group $\text{Gal}(K/\mathbb{Q})$ is therefore a group with generators t_1, t_2, t_3 and relations

$$\begin{aligned} \text{Gal}(K/\mathbb{Q})^{(2,2)} &= 1, \quad t_\nu^2 = 1, \quad \nu = 1, 2, 3, \\ [t_2, t_1]^{[\Delta_2, p_{1i_1}]} [t_3, t_1]^{[\Delta_3, p_{1i_1}]} &= 1, \quad i_1 \in J_1, \\ [t_1, t_2]^{[\Delta_1, p_{2i_2}]} [t_3, t_2]^{[\Delta_3, p_{2i_2}]} &= 1, \quad i_2 \in J_2, \\ [t_1, t_3]^{[\Delta_1, p_{3i_3}]} [t_2, t_3]^{[\Delta_2, p_{3i_3}]} &= 1, \quad i_3 \in J_3, \\ [t_1, t_2]^{[\Delta_1 \Delta_2, p'_i]} [t_1, t_3]^{[\Delta_1 \Delta_3, p'_i]} [t_2, t_3]^{[\Delta_2 \Delta_3, p'_i]} &= 1, \quad i \in J. \end{aligned}$$

Theorem 3 now follows by direct verification. \square

Remark. The cases 1–7 exhaust all possibilities for G and A up to permutations of $\Delta_1, \Delta_2, \Delta_3$.

5. APPLICATIONS

Theorem 4. *The Galois group of the 2-class field tower of $\mathbb{Q}(\sqrt{p_1^* p_2^* p_3^*})$ is Klein's four group if and only if*

$$(9) \quad \left(\frac{p_i^*}{p_j} \right) = 1, \quad \left(\frac{p_j^*}{p_i} \right) = \left(\frac{p_i^*}{p_l} \right) = \left(\frac{p_l^*}{p_j} \right) = -1$$

for some permutation $i j l$ of the numbers 1 2 3.

Proof. Put $k = \mathbb{Q}(\sqrt{p_1^* p_2^* p_3^*})$. According to Theorem 3, $\text{Gal}(k^{(2,2)}/k)$ is Klein's four group if and only if (9) holds. From $k^{(2,2)} = k^{(1,2)}$ we deduce by induction that $k^{(1,2)} = k^{(n,2)} = k^{(\infty)}$. \square

Theorem 5. *The Galois group of the 2-class field tower of $\mathbb{Q}(\sqrt{p_1^* p_2^* p_3^*})$ is the quaternion group of order 8 if and only if*

$$(10) \quad \left(\frac{p_i}{p_j} \right) = -1$$

for all $i, j = 1, 2, 3$ with $i \neq j$.

Proof. Let $k = \mathbb{Q}(\sqrt{p_1^* p_2^* p_3^*})$ and $G = \text{Gal}(k^{(2,2)}/k)$. According to Theorem 3, G is the quaternion group of order 8 if and only if (10) holds. Moreover, $\text{Gal}(k^{(2,2)}/k) = G/G^{(2,2)}$. Lemma 2 then implies $G = \text{Gal}(k^{(2,2)}/k)$, that is, $k^{(2,2)} = k^{(3,2)} = k^{(\infty)}$. \square

REFERENCES

- [1] A. Fröhlich, *On the absolute class group of Abelian fields*, J. London Math. Soc. **29** (1954), 211–217
- [2] A. Fröhlich, *A note on the class field tower*, Quart. J. Math. Oxford (2) **5** (1954), 141–144
1
- [3] H. Koch, *Über die Faktorengruppe einer absteigenden Zentralreihe*, Math. Nachr. **22** (1954), 141–144 3
- [4] L. Rédei, H. Reichardt, *Die durch vier teilbaren Invarianten der Klassengruppe eines quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1933), 69–74 1

Translation by Franz Lemmermeyer