

*Pacific
Journal of
Mathematics*

ON INFINITE UNRAMIFIED EXTENSIONS

CHRISTIAN MAIRE

Volume 192 No. 1

January 2000

ON INFINITE UNRAMIFIED EXTENSIONS

CHRISTIAN MAIRE

In this article we construct number fields k which have a trivial class group, but an infinite unramified extension.

1. Introduction.

Let k be a number field. A natural question is: Does k admit an infinite unramified extension?

The answer is no, if the root discriminant of k is less than Odlyzko's bounds.

The answer is yes, if k fails the test of Golod-Shafarevic for a prime number p . In that case, we know that there exists an infinite unramified p -extension L over k .

But generally it is fairly difficult to determine whether k admits an infinite unramified extension.

For this problem we introduce the following unramified extensions of k :

- i) k_∞ is the maximal unramified Galois extension of k .
- ii) $k^{(1)}$ denotes the Hilbert field of k , i.e., the maximal unramified abelian extension of k ; its Galois group over k is isomorphic to the class group of k via the Artin map. More generally, let $k^{(i)}$ be the Hilbert field of $k^{(i-1)}$, $i \geq 1$, where $k^{(0)} = k$. Write $k_H = \cup k^{(i)}$; k_H is the Hilbert tower of k . We say that the Hilbert tower is finite (or stops) if $[k_H/k] < \infty$, or infinite otherwise.
- iii) For a prime number p , k_p will be the p -Hilbert tower of k , that is to say the maximal p -extension of k contained in k_H .

We have the following inclusions:

$$k \subset k_p \subset k_H \subset k_\infty.$$

We recall two facts:

1) There exist fields k for which k_H is different from k_∞ . For instance, the field $k = \mathbb{Q}(\sqrt{3.883})$ has a trivial class group, but there exists an unramified A_5 -extension over k .

2) Yamamura [7] has shown that for all imaginary quadratic fields k with a discriminant less than 420 (or 729 under GRH), $k_\infty = k_H$, and k_∞/k is finite (the tower stops at the first, second or third floor).

Using some refinements of a theorem of Golod-Shafarevic or genus theory, it is possible to obtain sufficient criteria for the existence of an infinite unramified extension of a given number field k . However, these results generally imply that the Hilbert tower of the considered field k is infinite.

In Theorem 3.1 we give various examples of fields, such as the biquadratic field $\mathbb{Q}(\sqrt{17601097}, \sqrt{17380678572159893})$, with a trivial class group and an infinite unramified Galois extension: For each field k of Theorem 3.1, k_H/k is finite and k_∞/k is infinite.

Moreover, we prove that there exists infinitely many quadratic fields with a finite 2-Hilbert tower, together with an infinite unramified extension of degree 2^∞ (an extension of degree 2^∞ is an infinite extension which is the compositum of extensions of degree a power of 2).

Note that the calculations were performed using PARI [1].

Acknowledgements. The author wishes to thank X. Roblot for providing Example 4.1.2. He also thanks the referee for comments and for Example 3 in Remark 3.4.1.

2. Preliminaries.

In this section, we recall four propositions that will be used in the sequel.

Proposition 2.1 (Genus theory and theorem of Golod-Shafarevich, see [6]). *Let K/k be a cyclic extension of degree p , and ρ the number of places of k which are ramified in this extension. Denote by E_K (resp. E_k) the units group of K (resp. k).*

Suppose that

$$\rho \geq 3 + 2\sqrt{d_p E_K + 1} + d_p E_k,$$

then the p -Hilbert tower of K is infinite.

From then on, we shall write $r = \lceil 3 + 2\sqrt{d_p E_K + 1} + d_p E_k \rceil + \delta$, where $\lceil \cdot \rceil$ is the ceiling function and where $\delta = 0$ or 1 depending on whether $3 + 2\sqrt{d_p E_K + 1} + d_p E_k$ is an integer or not.

Proposition 2.2 (Kummer theory). *Let k/\mathbb{Q} be a cyclic extension of degree p unramified at p , and K/\mathbb{Q} an extension of degree n . Suppose that for all places \mathfrak{Q} of K , the ramification index of \mathfrak{Q} in K/\mathbb{Q} divides the ramification index of $\mathfrak{q} = \mathbb{Q} \cap \mathfrak{Q}$ in k/\mathbb{Q} .*

Then the extension Kk/k is unramified at the finite places. In particular, if C is the Galois closure of K , then Ck/k is unramified at the finite places.

Note that in this case, a place \mathfrak{Q} of K which is unramified over \mathbb{Q} will ramify in Kk/K whenever $\mathfrak{Q} \cap \mathbb{Q}$ is ramified in k/\mathbb{Q} .

A consequence of the above is the following well-known result (see [4]):

Proposition 2.3. *Let P be an irreducible real polynomial, with squarefree discriminant $D(P)$. Denote by C the Galois closure of P . Then $C/\mathbb{Q}(\sqrt{\text{Disc}(P)})$ is unramified.*

Proposition 2.4 (Class group of biquadratic fields). *Let $k_1 = \mathbb{Q}(\sqrt{d_1})$ and $k_2 = \mathbb{Q}(\sqrt{d_2})$ be two distinct quadratic fields. Let $k_3 = \mathbb{Q}(\sqrt{d_1 \cdot d_2})$ and $F = k_1 k_2$. Assume that:*

- 1) F/k_3 is unramified at all places;
- 2) The class groups of k_1 and k_2 are trivial;
- 3) The class group of k_3 is cyclic of order 2.

Then the Hilbert tower of k_3 stops at F ; in particular, the class group of F is trivial.

Proof. It is known that for $p \neq 2$ (see [5])

$$|cl_F(p)| = |cl_{k_1}(p)| |cl_{k_2}(p)| |cl_{k_3}(p)| = 1,$$

where $cl_M(p)$ denotes the p -primary component of the class group of a number field M .

Moreover, the 2-Hilbert tower of k_3 is exactly F because $cl_{k_3}(2)$ is cyclic of order 2. In addition $|cl_F(2)| = 1$, and $|cl_F| = 1$. \square

3. Main result.

We propose to construct *quadratic fields* with a finite Hilbert tower, such that they have an infinite unramified extension. Note that in all our examples the tower will stop at the first floor. This point will be proved with the help of Proposition 2.4.

3.1. Construction of infinite unramified extension. We consider the following situation:

- 1) K is a totally real field of degree n over \mathbb{Q} such that:
 - i) The discriminant of K is equal to a prime number l . Hence the Galois group of the closure of K is S_n (see [4]). Let P be a defining polynomial of K .
 - ii) There exist $n - 2$ unramified places above l in K/\mathbb{Q} .
- 2) q_1 and q_2 are two primes different from l such that:
 - i) $q_1 \equiv q_2 \equiv 3(4)$,
 - ii) q_1 splits completely in K ,
 - iii) there exist $n - 1$ places above q_2 in K/\mathbb{Q} .
- 3) We write $k = \mathbb{Q}(\sqrt{l \cdot q_1 \cdot q_2})$, and $M = Kk$.

Using Proposition 2.2, we have that all places above q_1 and q_2 plus $n - 2$ places above l are ramified in M/K . Therefore, in the notation of Proposition 2.1, in the extension M/K we have

$$\rho = n + (n - 1) + (n - 2).$$

Applying Proposition 2.1 to M/K , we conclude that M has an infinite 2-Hilbert tower, denoted by M_2 , if n is at least 7.

We have from Proposition 2.2 that the extension M/k is everywhere unramified. The above facts imply the following inclusions:

$$k = \mathbb{Q}(\sqrt{l \cdot q_1 \cdot q_2}) \subset M \subset M_2,$$

where M_2/k is an infinite unramified extension. Taking the Galois closure of M_2 over k , we obtain an infinite unramified Galois extension L over k . In particular, k_∞/k is infinite.

3.2. The finiteness of k_H/k . Suppose that we have found primes l , q_1 , q_2 and a field K of degree n satisfying all the hypotheses of paragraph 3.1. Let k_1 , k_2 , and $k = k_3$ be the quadratic fields of discriminant l , $l \cdot q_1$, and $l \cdot q_1 \cdot q_2$, respectively, and put $F = k_1 k_2$. Since $l \equiv q_1 q_2 \equiv 1 \pmod{4}$, F/k_3 is unramified. If, in addition, k_1 , k_2 have trivial class groups and k_3 has class number 2, then the Hilbert tower stops at F .

We remark that cl_F is trivial, and that the extension LF/F is an infinite unramified Galois extension, because F/k is unramified.

3.3. Finding a good polynomial. We want to find a polynomial of degree 7 verifying condition 1.i and 1.ii of paragraph 3.1. Such a polynomial does not exist in the PARI tables. Consequently, we use the following method:

Pick 7 reals around 0. Construct the monic polynomial P' of degree 7 whose roots are the considered reals, and take $P \in \mathbb{Z}[X]$ the nearest polynomial to P' . Then by choosing many families of 7 reals, we finally hope to find a good polynomial, i.e., such that:

- i) $\text{Disc}(P) = l$;
- ii) $P \equiv (X - \alpha_1)^2 \prod_{i=2,6} (X - \alpha_i) \pmod{l}$.

Indeed, we rapidly obtain the polynomial

$$P(X) = X^7 - 3X^6 - 13X^5 + 28X^4 + 42X^3 - 47X^2 - 31X + 12,$$

with

$$l = \text{Disc}(P) = 17380678572159893.$$

Conditions 1.i and 1.ii of paragraph 3.1 are verified.

3.4. Examples. We find one potential prime q_1 less than 300000 ($q_1 = 16747$), and 17 potential primes q_2 less than 100000.

Finally, eight of these primes q_2 are such that $(l, q_1 = 16747, q_2)$ satisfies the conditions of Proposition 2.4 (or paragraph 3.2).

Hence we have:

Theorem 3.1. *For the quadratic fields $\mathbb{Q}(\sqrt{17380678572159893 \cdot 16747 \cdot q_2})$, with $q_2 = 1051, 11863, 24659, 31583, 74527, 77339, 86579, 93491$, one has:*

- i) k_H/k is finite;
- ii) k_∞/k is infinite.

3.4.1. Remarks.

1) If we choose q_2 such that P is totally decomposed modulo q_2 , then q_2 is totally decomposed in the Galois closure of P , and so q_2 is decomposed in the extension $\mathbb{Q}(\sqrt{l})/\mathbb{Q}$. Consequently the class group of $\mathbb{Q}(\sqrt{l \cdot q_1 \cdot q_2})$ contains the cyclic group (4) [2]. In particular, the Hilbert field of this field is not a biquadratic field so it would be more difficult to control its class group.

2) For each field of Theorem 3.1, there exists an unramified infinite extension L over F with Galois group G such that we have the extension sequence:

$$1 \longrightarrow H \longrightarrow G \longrightarrow A_7 \longrightarrow 1,$$

where H is a non-analytic pro-2-group [3]. Note that $G = [G, G]$.

As a result, the 2-rank of the class group of any nested sequence of extensions M of F contained in L tends to infinity (see [3]). One shall bear in mind that $cl_F = (1)$.

3) It would be interesting to find the field of smallest discriminant satisfying the hypotheses of Theorem 3.1. The referee gives the following example:

$$P(X) = X^7 + 9X^6 + 13X^5 - 57X^4 - 86X^3 + 120X^2 - 1,$$

with $q_1 = 20411$ and $q_2 = 787$.

This example has the desired properties and the biquadratic field F has slightly smaller discriminant than the field in the introduction.

4. A remark.

One may try to apply Proposition 2.3 in order to find fields satisfying the conditions of Theorem 3.1.

More precisely, let P be an irreducible totally real polynomial with degree n such that the discriminant of P is equal to $l_1 \cdot l_2 \cdot l_3$ with $l_1 \equiv 1(4)$, and $l_2 \equiv l_3 \equiv 3(4)$, where l_1, l_2, l_3 are primes.

Let $K = \mathbb{Q}(\theta)$, where θ is a root of P , $k = \mathbb{Q}(\sqrt{l_1 \cdot l_2 \cdot l_3})$, and $M = Kk$. Assume that l_1, l_2 and l_3 are sufficiently decomposed in K/\mathbb{Q} . Then for larger n , using Propositions 2.1 and 2.3 we obtain that the field $k = \mathbb{Q}(\sqrt{l_1 \cdot l_2 \cdot l_3})$ has an infinite unramified Galois extension.

To show that the Hilbert tower of this field stops we can use an argument similar to the one involved in the previous section.

Yet, the problem becomes: How to find a polynomial satisfying the hypotheses above.

4.1. A method. Let $l_1 \equiv 1(4)$ and $l_2 \equiv 3(4)$ be two primes, and put

$$P(X) = X^2 \prod_{i=1}^{n-2} (X - \alpha_i) \pm l_1 \cdot l_2,$$

where α_i are different integers. Changing α_i, l_1 , and l_2 , we hope to find some polynomials P such that:

- 1) P is irreducible;
- 2) P is totally real;
- 3) $\text{Disc}(P) = l_1.l_2.l_3$, for some prime l_3 ;
- 4) P is sufficiently decomposed modulo l_3 ;
- 5) For $i = 2$ or 3 , $\left(\frac{l_1}{l_i}\right) = -1$.

Note that the last condition is necessary to get $cl_{k_3} = (2)$ [2].

4.1.1. Case $n = 17$; $r = 32$.

For the definition of r , see the paragraph of following Proposition 2.1. In that case, we should have at least two places above l_3 .

We have produced one polynomial:

$$\begin{aligned} P(X) = & X^{17} - 8X^{16} - 140X^{15} + 1120X^{14} + 7472X^{13} - 59696X^{12} \\ & - 191620X^{11} + 1532960X^{10} + 2475473X^9 - 19803784X^8 \\ & - 15291640X^7 + 122333120X^6 + 38402064X^5 \\ & - 307216512X^4 - 25401600X^3 + 203212800X^2 - 4819 \end{aligned}$$

with $\text{Disc}(P) = l_1.l_2.l_3$, where $l_1 = 61$, $l_2 = 79$ and

$$\begin{aligned} l_3 = & 66382900552793321010851526783904690431649057036670997212644 \\ & 289798588293426436298810789013190435989241744842371595711118731 \\ & 34668406985800955450434299964685089696459. \end{aligned}$$

Note that $\log(l_3)/\log(10) \approx 163$, and that

$$\begin{aligned} P(X) = & X^2(X-1)(X-2)(X-3)(X-4)(X-5)(X-6) \\ & \cdot (X-7)(X-8)(X+1)(X+2)(X+3)(X+4)(X+5) \\ & \cdot (X+6)(X+7) - 61.79 \end{aligned}$$

There are 5 places above l_3 which are ramified in K/k . So $\rho = 15+15+5 = 35 > r$.

4.1.2. Case $n = 11$; $r = 24$.

X. Roblot comes up with the polynomial:

$$P(X) = X^{11} - 45X^{10} + 870X^9 - 9450X^8 + 63273X^7 - 269325X^6 + 723680X^5 - 1172700X^4 + 1026576X^3 - 362880X^2 + 2483$$

with $\text{Disc}(P) = l_1.l_2.l_3$, where $l_1 = 13$, $l_2 = 191$ and

$$l_3 = 1975697671490152075520432855935517362161188018903.$$

Here $\rho = 9 + 9 + 7 = 25 > r$.

4.1.3. Case $n = 9$; $r = 21$.

We found three polynomials ; for all these cases $\rho = 7 + 7 + 7 = 21 \geq r$.

- $X^9 - 16X^8 - 122X^7 + 1100X^6 + 3709X^5 - 20524X^4 - 28068X^3 + 95760X^2 - 18467$
with $l_1 = 313$, $l_2 = 59$, and
 $l_3 = 26255115680330741686041335538501141687236954384684227$.
- $X^9 + 35X^8 + 51X^7 - 1535X^6 - 2476X^5 + 18660X^4 + 17424X^3 - 69120X^2 + 13067$
with $l_1 = 73$, $l_2 = 179$, and
 $l_3 = 7154637362578369142642781505295690026075933100681339$.
- $X^9 + 41X^8 + 69X^7 - 1805X^6 - 3046X^5 + 22044X^4 + 21096X^3 - 82080X^2 + 18511$
with $l_1 = 173$, $l_2 = 107$, and
 $l_3 = 95384503977834605133365739257008489233297152056661447$.

The problem is to calculate the class group of the fields $\mathbb{Q}(\sqrt{l_1})$ and $\mathbb{Q}(\sqrt{l_1.l_2.l_3})$.

5. Infinite non Galois unramified extension.

In this section, we prove:

Theorem 5.1. *There exists infinitely many quadratic fields (imaginary and real) with a finite 2-Hilbert tower, but with an infinite unramified extension of degree 2^∞ .*

Proof (only for the real case) and examples.

Let K be a totally real extension over \mathbb{Q} of degree 8, such that $\text{Disc}(K) = l$ where l is prime number. Let q_1 and q_2 be two primes, satisfying:

- 1) $q_1 \equiv q_2 \equiv 3(4)$;
- 2) q_1 and q_2 are totally decomposed in K/\mathbb{Q} .

Put $N = K\mathbb{Q}(\sqrt{l})$.

Then q_1 and q_2 are totally decomposed in the Galois closure of P , in particular in N/\mathbb{Q} . This extension is of degree 16.

Using Proposition 2.1 applied to the extension $N(\sqrt{q_1.q_2})/N$, we conclude that $E = N(\sqrt{q_1.q_2})$ has an infinite 2-Hilbert tower, noted E_2 .

Thus, we have the following inclusions:

$$\mathbb{Q}(\sqrt{l.q_1.q_2}) \subset \mathbb{Q}(\sqrt{l}, \sqrt{q_1.q_2}) \subset E \subset E_2,$$

where all extensions are unramified 2-extensions. Accordingly, $E_2/\mathbb{Q}(\sqrt{l.q_1.q_2})$ is an unramified extension of degree 2^∞ .

Moreover, the choice of q_1 and q_2 implies that the 2-part of class group of $\mathbb{Q}(\sqrt{l.q_1.q_2})$ is cyclic. As consequence the 2-Hilbert tower stops at the first floor.

If K/\mathbb{Q} exists, Chebotarev's density criterion asserts that there exist infinitely many such fields $\mathbb{Q}(\sqrt{l.q_1.q_2})$.

For the imaginary quadratic case, one may start with the same K and q_1 as above and take $q_2 = -1$. Then $\mathbb{Q}(\sqrt{l \cdot q_1 \cdot q_2})$ is an imaginary quadratic field with the desired properties.

5.1. Examples. Consider the following polynomial, found in the PARI tables (E-mail: megrez.math.u-bordeaux.fr, directory pub/numberfields):

$$P(X) = X^8 - X^7 - 7X^6 + 5X^5 + 14X^4 - 6X^3 - 9X^2 + X + 1,$$

where

$$\text{Disc}(P) = 1318279381.$$

Then the fields

$$\mathbb{Q}\left(\sqrt{1302839.4503991.1318279381}\right)$$

and

$$\mathbb{Q}\left(\sqrt{-643.1318279381}\right)$$

satisfy the conditions of Theorem 5.1.

References

- [1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's guide to PARI-GP*, 1997.
- [2] G. Gras, *Sur les classes d'idéaux dans les extensions cycliques relatives de degré premier l* , Ann. Inst. Fourier, **23**(4) (1973), 1-48.
- [3] F. Hajir, *On the growth of p -class groups in p -class field towers*, J. Algebra, **188** (1997), 256-271.
- [4] T. Kondo, *Algebraic number fields with the discriminant equal to that of a quadratic number field*, J. Math. Soc. Japan, **42** (1995), 31-36.
- [5] T. Kubota, *Über den Bizyklischen Biquadratischen Zahlkörper*, Nagoya Math. J., **10** (1955), 65-85.
- [6] J. Martinet, *Tours de corps de classes et estimations de discriminants*, Invent. Math., **44** (1978), 65-73.
- [7] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*, preprint, 1997.

Received April 15, 1998 and revised June 2, 1998.

LABORATOIRE A2X - UNIVERSITÉ BORDEAUX I
 351, COURS DE LA LIBÉRATION
 33405 TALENCE CEDEX
 FRANCE
 E-mail address: maire@math.u-bordeaux.fr