MATHEMATICS OF COMPUTATION
Volume 76, Number 260, October 2007, Pages 2127–2138
S 0025-5718(07)01964-3
Article electronically published on April 17, 2007

PRIME DECOMPOSITION IN THE ANTI-CYCLOTOMIC EXTENSION

DAVID BRINK

ABSTRACT. For an imaginary quadratic number field K and an odd prime number l, the *anti-cyclotomic* $\mathbb{Z}_l$-extension of K is defined. For primes $\mathfrak{p}$ of K, decomposition laws for $\mathfrak{p}$ in the anti-cyclotomic extension are given. We show how these laws can be applied to determine if the Hilbert class field (or part of it) of K is $\mathbb{Z}_l$-embeddable. For some K and l, we find explicit polynomials whose roots generate the first step of the anti-cyclotomic extension and show how the prime decomposition laws give nice results on the splitting of these polyniomials modulo p. The article contains many numerical examples.

I. INTRODUCTION

Let l be an odd prime number, and denote by $\mathbb{Z}_l$ the infinite pro-cyclic l-group $\varprojlim \mathbb{Z}/l^n$. Consider an imaginary quadratic number field K. As is well known, K has a unique $\mathbb{Z}_l$-extension which is pro-dihedral over $\mathbb{Q}$. We call it the *anti-cyclotomic* $\mathbb{Z}_l$-extension of K (for reasons later to be clear).

The purpose of this paper is to study the decomposition of primes $\mathfrak{p}$ of K in the anti-cyclotomic extension. Since this extension is pro-cyclic over K, the decomposition type of $\mathfrak{p}$ is completely determined by the number of *steps* of the anti-cyclotomic extension in which $\mathfrak{p}$ is unramified, and the number of steps in which $\mathfrak{p}$ splits totally. By the n^{th} *step* of a $\mathbb{Z}_l$-extension we understand the subextension of degree l^n over the ground field.

Such decomposition laws are given in Section III (Theorems 1 and 2). The laws involve representations of primes p or prime powers p^h by certain quadratic forms.

As we shall see, the decomposition laws also depend on how many steps of the anti-cyclotomic extension are unramified. This dependence may be turned around, meaning that if we know how certain primes decompose, then we can compute the number of unramified steps. In particular, we can answer whether the Hilbert class field of K is contained in the anti-cyclotomic extension and thus is $\mathbb{Z}_l$-embeddable.

In Section IV we show how to find explicit polynomials whose roots generate the first step of the anti-cyclotomic extension. When K is not l-rational (to be defined in Section II), this involves using the decomposition laws to identify the right polynomial f among a finite number of candidates. When this is done, one obtains nice laws for the splitting of f modulo p. For instance, we show that

Received by the editor October 21, 2005 and, in revised from, July 4, 2006.
2000 *Mathematics Subject Classification.* Primary 11R32.
Key words and phrases. Prime decomposition, imaginary quadratic number fields, ring class fields, pro-cyclic l-extensions, factorisation of polynomials modulo p.

$X^5 + 20X + 32$ splits into linear factors modulo a prime number $p \neq 2, 5$ iff p is of the form $x^2 + 125y^2$ or $2x^2 + 2xy + 63y^2$.

Throughout the article we use the following notation:

l:	an odd prime number
Δ:	a square–free natural number
K:	the imaginary quadratic number field $\mathbb{Q}(\sqrt{-\Delta})$
d_K:	the discriminant of K
h, μ, u:	we write the class number of K as $h = l^\mu u$ with $l \nmid u$
$\mathcal{O}$:	the ring of integral elements in K
$\mathfrak{p}$:	a prime of K, i.e. a prime ideal in $\mathcal{O}$
p:	the rational prime divisible by $\mathfrak{p}$
K_H:	the Hilbert class field of K
$K_{\max}$:	the maximal abelian extension of K unramified outside l
$K_{\text{anti}}^{(n)}$:	the n^{th} step of the anti-cyclotomic extension K_{anti}
ν:	the non-negative integer defined by $K_{\text{anti}} \cap K_H = K_{\text{anti}}^{(\nu)}$

II. The cyclotomic and the anti-cyclotomic extension

In Iwasawa [4] it is shown that any $\mathbb{Z}_l$-extension of K is unramified outside l. This result motivates the study of the maximal abelian extension $K_{\max}$ of K which is unramified outside l. If K^f denotes the ray class field over K of conductor f, then $K_{\max}$ is the union of the tower

$$K \subseteq K^1 \subseteq K^l \subseteq K^{l^2} \subseteq \dots .$$

Here, K^1 is the Hilbert class field of K which we also denote K_H.

Let τ denote complex conjugation. Clearly, $K_{\max}$ is normal over $\mathbb{Q}$, so τ operates on $\mathrm{Gal}(K_{\max}/K)$ by conjugation.

Main Lemma 1. *We may write $Gal(K_{\max}/K) = U \times W \times T \times T'$ such that*

(i) *U is isomorphic to $\mathbb{Z}_l$, and τ operates trivially on U,*

(ii) *W is isomorphic to $\mathbb{Z}_l$, and τ operates by inversion on W,*

(iii) *T is a finite l-group, and τ operates by inversion on T,*

(iv) *T' is finite of order prime to l.*

Furthermore, we may write $Gal(K_{\max}/K_H) = U \times V \times T^* \times S'$ where

(v) *V is isomorphic to $\mathbb{Z}_l$, contained in $W \times T$, and has $|V : W \cap V| \leq |T|$,*

(vi) *T^* is trivial unless $l = 3$, $\Delta \equiv 3 \mod 9$, and $\Delta \neq 3$; in this* exceptional case*, T^* has order 3 and is contained in T,*

(vii) *S' is contained in T' (and thus finite of order prime to l).*

Consider a conductor $f = l^e$ with $e \geq 1$. Then $Gal(K_{\max}/K^f) = U^f \times V^f$ where

(viii) *U^f is contained in U and has index $|U : U^f| = l^{e-1}$,*

(ix) *V^f is contained in V. If $l \nmid \Delta$, then $|V : V^f| = l^{e-1}$. If $l \mid \Delta$, then $|V : V^f| = l^e$ unless $l = 3$ and $\Delta \equiv 3 \mod 9$; in this case, $|V : V^f| = 3^{e-1}$.*

The subgroups U, $W \times T$, T, T', V, T^*, S', U^f, and V^f are unique with these properties.

A similar representation of $\mathrm{Gal}(K_{\max}/K)$ appears in Carroll and Kisilevsky [3], proved using idèles rather than ideals as here.

A proof will be given at the end of the section. At this point, we only note that the uniqueness statement is seen as follows: U is the maximal subgroup of the l-part of $\mathrm{Gal}(K_{\max}/K)$ on which τ operates trivially, $W \times T$ is the maximal

subgroup of the l-part of $\mathrm{Gal}(K_{\max}/K)$ on which τ operates by inversion, T is the l-torsion and T' is the non-l-part[1] (and the non-l-torsion) of $\mathrm{Gal}(K_{\max}/K)$, V equals $\mathrm{Gal}(K_{\max}/K_H) \cap (W \times T)$, T^* is the l-torsion, and S' is the non-l-part of $\mathrm{Gal}(K_{\max}/K_H)$. Note that W is not unique if T is non-trivial.

Proposition 1. (a) *K has a unique $\mathbb{Z}_l$-extension which is pro-cyclic over $\mathbb{Q}$. It is called the* **cyclotomic** *extension and is denoted K_{cycl}. Adjoin to $\mathbb{Q}$ all roots of unity of l-power-order, and let $\mathbb{Q}_{\mathrm{cycl}}$ be the l-part of this extension. Then K_{cycl} is the composite of K and $\mathbb{Q}_{\mathrm{cycl}}$.*

(b) *K has a unique $\mathbb{Z}_l$-extension which is pro-dihedral over $\mathbb{Q}$. It is called the* **anti-cyclotomic** *extension and is denoted K_{anti}.*

(c) *K_{cycl} and K_{anti} are the only absolutely normal $\mathbb{Z}_l$-extensions of K. They are linearly disjoint over K, and any $\mathbb{Z}_l$-extension of K is contained in the composite $K_{\mathrm{cycl}}K_{\mathrm{anti}}$. The l-part of the Hilbert class field K_H (or any other part of it) is embeddable in a $\mathbb{Z}_l$-extension of K iff it is contained in K_{anti}.*

(d) *The Galois group of the maximal abelian l-extension of K which is unramified outside l is isomorphic to $\mathbb{Z}_l \times \mathbb{Z}_l \times T$ where T is a finite l-group. If T is trivial, the l-part of K_H is cyclic and $\mathbb{Z}_l$-embeddable.*

Proof. Everything follows from the theorem: K_{cycl} is the fixed field of $W \times T \times T'$, and K_{anti} is the fixed field of $U \times T \times T'$. Any $\mathbb{Z}_l$-extension of K is contained in the fixed field of the torsion $T \times T'$, i.e. in $K_{\mathrm{cycl}}K_{\mathrm{anti}}$. K_{cycl} and K_{anti} are the only absolutely normal $\mathbb{Z}_l$-extensions of K since U and W are the only τ-invariant subgroups of $U \times W$ with quotient $\mathbb{Z}_l$. Since K_H is generalised dihedral over $\mathbb{Q}$, the maximal $\mathbb{Z}_l$-embeddable subfield of it is $K_H \cap K_{\mathrm{anti}}$. If T is trivial, the l-part of K_H is contained in K_{anti}. It is clear that $\mathbb{Q}_{\mathrm{cycl}}$ is a $\mathbb{Z}_l$-extension of $\mathbb{Q}$. Hence $K\mathbb{Q}_{\mathrm{cycl}}$ is a $\mathbb{Z}_l$-extension of K and a $(\mathbb{Z}_l \times \mathbb{Z}/2)$-extension of $\mathbb{Q}$. The uniqueness of K_{cycl} implies $K_{\mathrm{cycl}} = K\mathbb{Q}_{\mathrm{cycl}}$. □

The situation is particularly simple when the torsion T is trivial. If this is the case, K is called **l-rational**.

Lemma 2. (a) *Let X be an infinite abelian pro-l-group, and assume V and T^* are subgroups of X of which V is pro-cyclic with finite index, and T^* is finite. Then we may write $X = W \times T$ with W pro-cyclic, T finite containing T^*, and $|V : V \cap W| \leq |T|$.*

(b) *Let X be an abelian pro-l-group with a subgroup V. Assume τ is an automorphism of order 2 on X that operates by inversion both on V and on X/V. Then τ operates by inversion on X.*

(c) *Let X be an abelian pro-l-group with a subgroup U. Assume τ is an automorphism on X that operates trivially on U and by inversion on X/U. Then $X = U \times V$ where $V = \{x \in X \mid x^\tau = x^{-1}\}$.*

Proof. (a) Assume $V \times T^*$ has index l in X; the general case will then follow by induction. Pick an $x \in X \backslash (V \times T^*)$ and write $x^l = vt$ with $v \in V$ and $t \in T^*$. If v is an l^{th} power in V, then $X = V \times T$ with a T containing T^*. If v^l is not an l^{th} power in V, then $X = W \times T^*$ where W is the pro-cyclic group generated by x; from $x^{l \cdot |T^*|} = v^{|T^*|}$ it follows that $|V : W \cap V| \leq |T^*|$.

[1]The l-part of an abelian pro-finite group is its Sylow-l-subgroup, the "non-l-part" is the product of the l'-parts for $l' \neq l$. The l-part of an abelian field extension is the fixed field of the non-l-part of the Galois group, and vice versa.

(b) Let $x \in X$. Then $x^\tau = x^{-1}v$ for some $v \in V$. Hence $x = x^{\tau\tau} = x^{-\tau}v^\tau = xv^{-2}$ and therefore $v^2 = e$, $v = e$ (since X has no elements of order 2), and $x^\tau = x^{-1}$.

(c) Let $x \in X$. Then $x^\tau = x^{-1}u$ for a $u \in U$. Every element in X is a square, so there is a $u_0 \in U$ with $u_0^2 = u^{-1}$. Put $v = xu_0$. Then $v^\tau = x^\tau u_0 = x^{-1}uu_0 = v^{-1}$, i.e. $v \in V$. Hence $x = u_0^{-1}v \in U \times V$. □

Lemma 3. *Let $e \geq 1$. The group of units in the ring $\mathcal{O}/l^e$ may be written as $(\mathcal{O}/l^e)^* = U \times V \times S'$ such that the following hold:*

(a) *Complex conjugation τ operates trivially on U which is isomorphic to $\mathbb{Z}/l^{e-1}$.*

(b) *Complex conjugation τ operates by inversion on V, and*

$$V \cong \begin{cases} \mathbb{Z}/l^{e-1} & \text{if } l \nmid \Delta, \\ \mathbb{Z}/l^e & \text{if } l \mid \Delta, \text{ unless } l = 3 \text{ and } \Delta \equiv 3 \mod 9, \\ \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3 & \text{if } l = 3 \text{ and } \Delta \equiv 3 \mod 9. \end{cases}$$

(c) *S' is the non-l-part of $(\mathcal{O}/l^e)^*$ and has order*

$$|S'| = \begin{cases} (l-1)^2 & \text{if } (-\Delta/l) = 1, \\ l^2 - 1 & \text{if } (-\Delta/l) = -1, \\ l - 1 & \text{if } (-\Delta/l) = 0. \end{cases}$$

There is a subgroup S'' of S' of order $l-1$ such that $(\mathbb{Z}/l^e)^* = U \times S''$.

Proof. To begin with, note that each coset of $\mathcal{O}/l^e$ has a unique representative of the form $a + b\sqrt{-\Delta}$ with $a, b \in \{0, 1, \ldots, l^e - 1\}$.

The order of $(\mathcal{O}/l^e)^*$ depends on the decomposition of l in K as follows:

$$|(\mathcal{O}/l^e)^*| = \begin{cases} (l-1)^2 l^{2e-2} & \text{if } l \text{ splits}, \\ (l^2-1)l^{2e-2} & \text{if } l \text{ is inert}, \\ (l-1)l^{2e-1} & \text{if } l \text{ ramifies}. \end{cases}$$

This gives the order of S'.

The subgroups $U := \langle 1 + l \rangle$ and $V' := \langle 1 + l\sqrt{-\Delta} \rangle$ of $(\mathcal{O}/l^e)^*$ are both $\cong \mathbb{Z}/l^{e-1}$ and have trivial intersection. Clearly, τ operates trivially on U and by inversion on $(U \times V')/U$. So by Lemma 2(c), $U \times V' = U \times V$ for a group $V \cong \mathbb{Z}/l^{e-1}$ on which τ operates by inversion. This shows (a) and (b) when $l \nmid \Delta$.

When $l \mid \Delta$, the same arguments work for $V' := \langle 1 + \sqrt{-\Delta} \rangle$ unless $l = 3$ and $\Delta \equiv 3 \mod 9$. In the *exceptional case* $l = 3$ and $\Delta \equiv 3 \mod 9$, however, the 3-part of $(\mathcal{O}/9)^*$ is $\langle 1+3 \rangle \times \langle 1+3\sqrt{-\Delta} \rangle \times \langle 1+\sqrt{-\Delta} \rangle \cong (\mathbb{Z}/3)^3$, showing $V \cong \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3$. This finishes the proof of (b).

To see the last part of (c), note $U = \{u \in (\mathbb{Z}/l^e)^* \mid u \equiv 1 \mod l\}$. □

Proof of Main Lemma 1. Consider conductors $f = l^e$ with $e \geq 1$. Let J_K^f be the group of fractional ideals prime to f (i.e. prime to l) and let P_K^f be the subgroup generated by the principal ideals (α) with integral $\alpha \equiv 1 \mod f$. By class field theory, the *Artin symbol* is a surjective homomorphism

$$\left(\frac{K^f/K}{}\right) : J_K^f \to \mathrm{Gal}(K^f/K)$$

with kernel P_K^f. It maps the group P_K of principal ideals prime to l onto $\mathrm{Gal}(K^f/K_H)$ and behaves nicely with respect to restriction when e varies. Moreover, since $\tau = \tau^{-1}$, the Artin symbol satifies

$$\left(\frac{K^f/K}{\tau(\mathfrak{p})}\right) = \tau\left(\frac{K^f/K}{\mathfrak{p}}\right)\tau \ .$$

Assume for simplicity that $\Delta \neq 1, 3$. We then have the natural exact sequence

$$1 \to \{\pm 1\} \to (\mathcal{O}/l^e)^* \to P_K/P_K^f \to 1$$

where an $\alpha \in (\mathcal{O}/l^e)^*$ is sent to the principal ideal (α). The Artin symbol thus induces an isomorphism

$$\varprojlim (\mathcal{O}/l^e)^*/\{\pm 1\} \xrightarrow{\cong} \mathrm{Gal}(K_{\max}/K_H) \ .$$

We conclude from Lemma 3 that $\mathrm{Gal}(K_{\max}/K_H) = U \times V \times T^* \times S'$ with U, V, and T^* as in the theorem, and S' is finite of order

$$|S'| = \begin{cases} (l-1)^2/2 & \text{if } (-\Delta/l) = 1, \\ (l^2-1)/2 & \text{if } (-\Delta/l) = -1, \\ (l-1)/2 & \text{if } (-\Delta/l) = 0. \end{cases}$$

From Lemma 3 it also follows that $\mathrm{Gal}(K_{\max}/K^f) = U^f \times V^f$ with U^f and V^f as in the theorem.

The rest is group theory: Write $\mathrm{Gal}(K_{\max}/K) = X \times T'$ with l-part X and non-l-part T'. Then X contains $U \times V \times T^*$, and T' contains S' with index $|T' : S'| = u$. It is well known that K_H is a generalised dihedral extension of $\mathbb{Q}$, so that τ operates by inversion on $X/(U \times V \times T^*)$. It follows from Lemma 2(b) that τ operates by inversion on X/U. By Lemma 2(c), $X = U \times Y$ where $Y = \{x \in X \mid x^\tau = x^{-1}\}$. Clearly, Y contains $V \times T^*$ with finite index $|Y : V \times T^*| = l^\mu$. By Lemma 2(a), $Y = W \times T$ with $W \cong \mathbb{Z}_l$, T finite containing T^*, and $|V : W \cap V| \leq |V|$.

In the case $\Delta = l = 3$, the occurrence of a factor of order 3 in $\mathcal{O}^*$ causes T^* to vanish. So in this situation, we are *not* in the "exceptional case". □

III. Prime decomposition laws

Consider a prime ideal $\mathfrak{p}$ of K, and let p be the rational prime it divides. Our main objective is to give a law for the decomposition or factorisation of $\mathfrak{p}$ in K_{anti}. For the sake of completeness, we start with the cyclotomic extension in which the law has the simplest form possible.

Proposition 2. *If $p = l$, then $\mathfrak{p}$ is totally ramified in K_{cycl}. If $p \neq l$, then $\mathfrak{p}$ is unramified in K_{cycl}, and $\mathfrak{p}$ splits totally in the n^{th} step of K_{cycl} iff $p \equiv \pm 1 \mod l^{n+1}$.*

Proof. This is an immediate consequence of Proposition 1(a) and the law on decomposition of prime numbers in cyclotomic fields. □

Now we turn to the anti-cyclotomic extension. Recall that K_{anti}/K is unramified outside l by Iwasawa's result. Define $\nu \geq 0$ such that $K_{\mathrm{anti}} \cap K_H = K_{\mathrm{anti}}^{(\nu)}$. Then any prime $\mathfrak{P}$ of $K_{\mathrm{anti}}^{(\nu)}$ dividing l ramifies totally in K_{anti}.

The ring class field N^f over K of conductor f is the maximal subfield of the ray class field K^f being dihedral over $\mathbb{Q}$. So K_{anti} is contained in the union of the tower

$$K \subseteq N^1 \subseteq N^l \subseteq N^{l^2} \subseteq \dots.$$

If p is inert (resp. ramified) in $K/\mathbb{Q}$, then the ideal class of $\mathfrak{p}$ is trivial (resp. of order 2) in the ideal class group of K, and hence class field theory ([5, Theorem 7.3]) gives that $\mathfrak{p}$ splits totally in any ring class field N^f (resp. in a subfield L of N^f with $|N^f : L| = 2$) of conductor f prime to l. In particular, $\mathfrak{p}$ splits totally in K_{anti} if p is different from l and non-split in K (another proof of this is given in [3, Section III]). So the remaining problem is the case where $p \neq l$ splits in K. We treat first the easier situation where K is l-rational (as defined in Section II).

Theorem 1. *Assume K is l-rational, and consider a prime $p \nmid d_K l$ and an integer $n \geq 0$. Write the class number of K as $h = l^\mu u$ with $l \nmid u$. For $n \leq \mu$, p splits in $K_{\text{anti}}^{(n)}$ iff p is representable by a quadratic form of discriminant d_K whose order in the form class group is not divisible by $l^{\mu-n+1}$. For $n > \mu$, p splits in $K_{\text{anti}}^{(n)}$ iff p is representable by a quadratic form of discriminant*

$$\begin{cases} d_K \cdot l^{2(n-\mu+1)} & \text{if } l \nmid \Delta \text{ or } \Delta = l = 3, \\ d_K \cdot l^{2(n-\mu)} & \text{otherwise} \end{cases}$$

whose order in the form class group is prime to l.

Proof. First some general observations. Consider a ring class field N^f of K with arbitrary conductor f. The Galois group $\mathrm{Gal}(N^f/K)$ is isomorphic to the ring class group of conductor f via the Artin isomorphism. This ring class group is again isomorphic to the form class group $\mathscr{C}$ of discriminant $-d_K f^2$. Now let L be any field with $K \subsetneqq L \subsetneqq N^f$. By the main theorem of Galois theory and the above isomorphisms, there corresponds to L some subgroup H of $\mathscr{C}$. For a prime number p dividing neither d_K nor f, class field theory gives that p splits totally in L iff p is representable by a quadratic form f whose equivalence class $\mathfrak{k}$ belongs to H.

Assume $n \leq \mu$ and let N be the ring class field of K with conductor $f = 1$ (which equals the Hilbert class field). The l-part of N/K is $K_{\text{anti}}^{(\mu)}$ since K is l-rational. The subgroup H of the form class group $\mathscr{C}$ of discriminant d_K corresponding to $L := K_{\text{anti}}^{(n)}$ consists of the classes of forms of order not divisible by $l^{\mu-n+1}$. This proves the first claim.

Now assume $n > \mu$. We only prove the case $l \nmid \Delta$. Let N be the ring class field of K with conductor $f = l^{n-\mu+1}$. By the Main Lemma, the l-part of N/K is $K_{\text{anti}}^{(n)}$ since K is l-rational. The subgroup H of the form class group $\mathscr{C}$ of discriminant $d_K f^2$ corresponding to $L := K_{\text{anti}}^{(n)}$ consists of the classes of forms of order prime to l. This proves the second claim. □

Antoniadis [1] gives a prime decomposition law for ring class fields and their subfields involving coefficients of L-series.

Example 1. (i) Let $l = 3$ and $\Delta = 3$. We seek the primes $p \neq 3$ that split in $K_{\text{anti}}^{(1)}$. The form class group of discriminant $-3 \cdot 3^4 = -243$ has order 3. So p splits iff it is representable by the principal form $x^2 + xy + 61y^2$.

(ii) Let $l = 5$ and $\Delta = 5$. The form class group of discriminant $-20 \cdot 5^2 = -500$ has order 10. So for a prime $p \neq 2, 5$ splits in $K^{(1)}_{\text{anti}}$ iff it is representable by either the principal form $x^2 + 125y^2$ or the form $2x^2 + 2xy + 63y^2$ of order 2.

(iii) Let $l = 7$ and $\Delta = 1$. The form class group of discriminant $-4 \cdot 7^4 = -9604$ is cyclic of order 28. So a prime $p \neq 2, 7$ splits in $K^{(1)}_{\text{anti}}$ iff it is representable by either the principal form $x^2 + 2401y^2$, or the form $2x^2 + 2xy + 1201y^2$ of order 2, or the form $41x^2 + 20xy + 61y^2$ of order 4 (the other form of order 4 is $41x^2 - 20xy + 61y^2$ which represents the same numbers).

When K is not l-rational, the l-part of the ring class fields of l-power conductor are not contained in K_{anti}, and the problem lies in identifying their intersection.

Theorem 2. *Assume that p is different from l and splits in K. We may then write*

$$p^h = \begin{cases} a^2 + \Delta b^2 & \text{if } \Delta \not\equiv 3 \mod 4, \\ a^2 + ab + ((\Delta + 1)/4)b^2 & \text{if } \Delta \equiv 3 \mod 4, \end{cases} \tag{1}$$

with relatively prime $a, b \in \mathbb{Z}$. Put $\omega := \sqrt{-\Delta}$ if $\Delta \not\equiv 3 \mod 4$, otherwise $\omega := (1 + \sqrt{-\Delta})/2$. Let $n \geq 0$ be an integer.

(a) *Suppose l splits in K. Write $(a + b\omega)^{l-1} = a^* + b^*\omega$. Then $\mathfrak{p}$ splits totally in $K^{(n)}_{\text{anti}}$ iff $b^* \equiv 0 \mod l^{n+1+\mu-\nu}$.*

(b) *Suppose l is inert in K. Write $(a+b\omega)^{l+1} = a^*+b^*\omega$. Then the conclusion of (a) holds.*

(c) *Suppose l is ramified in K and we are not in the exceptional case (see below). Then $\mathfrak{p}$ splits totally in $K^{(n)}_{\text{anti}}$ iff $b \equiv 0 \mod l^{n+\mu-\nu}$.*

(d) *Suppose $l = 3$ and $\Delta \equiv 3 \mod 9$ (the exceptional case). Write $(a+b\omega)^3 = a^* + b^*\omega$. Then $\mathfrak{p}$ splits totally in $K^{(n)}_{\text{anti}}$ iff $b^* \equiv 0 \mod 3^{n+2+\mu-\nu}$.*

In all cases, $\mathfrak{p}$ only splits in a finite number of steps of K_{anti}.[2]

Proof. Write $(p) = \mathfrak{pq}$ with conjugate prime ideals $\mathfrak{p}, \mathfrak{q}$ of K. By definition of h, $\mathfrak{p}^h$ and $\mathfrak{q}^h$ are principal, i.e. $\mathfrak{p}^h = (a + b\omega)$ and $\mathfrak{q}^h = (a + b\bar{\omega})$ for some $a, b \in \mathbb{Z}$. When $\Delta \not\equiv 3 \mod 4$, we have $(p^h) = \mathfrak{p}^h\mathfrak{q}^h = (a + b\sqrt{-\Delta})(a - b\sqrt{-\Delta}) = (a^2 + \Delta b^2)$ and consequently $p^h = a^2 + \Delta b^2$. The representation of p^h in case $\Delta \equiv 3 \mod 4$ is similar. If a and b were not relatively prime, then $\mathfrak{p}^h = (a + b\omega)$ and $\mathfrak{q}^h = (a + b\bar{\omega})$ would not be relatively prime either, a contradiction.

Now assume a representation

$$p^h = (u + v\omega)(u + v\bar{\omega})$$

is given with relatively prime $u, v \in \mathbb{Z}$. Then $\mathfrak{p}^h\mathfrak{q}^h = (p^h) = (u + v\omega)(u + v\bar{\omega})$. If $(u + v\omega)$ and $(u + v\bar{\omega})$ were not relatively prime, then one of these ideals would be divisible by $\mathfrak{pq} = (p)$, which is not the case since u and v are relatively prime. Hence the ideal $(u + v\omega)$ equals either $\mathfrak{p}^h$ or $\mathfrak{q}^h$, say $(u + v\omega) = \mathfrak{p}^h = (a + b\omega)$.

The remainder of the proof relies on Main Lemma 1 whose notation we adopt. The different cases are now treated separately.

(a) Assume l splits in K. It follows immediately from the definition of ν that $\text{Gal}(K_{\max}/K^{(\nu)}_{\text{anti}}) = U \times V \times T \times T'$. Hence $l^\nu = |W \times T : V \times T|$ and $|T| = l^{\mu-\nu}$ since $|W \times T : V| = l^\mu$.

[2] I wish to thank the referee for calling my attention to this.

Consider the conductor $f = l^e$ with $e = n + 1 + \mu - \nu$. By Main Lemma 1(v) and (ix), V^f is contained in W and hence

$$\mathrm{Gal}(K^f/K) = \bar{U} \times \bar{W} \times T \times T'$$

where $\bar{U} = U/U^f$ is cyclic of order $l^{e-1} = l^{n+\mu-\nu}$, $\bar{W} = W/V^f$ is cyclic of order $l^{e-1+\nu} = l^{n+\mu}$, and T' has order prime to l. The fixed field of $\bar{U} \times T \times T'$ is $K_{\mathrm{anti}}^{(n+\mu)}$. It follows from Lemma 3 that the image of $(\mathbb{Z}/l^e)^*$ under the Artin symbol

$$\left(\frac{K^f/K}{}\right) : (\mathcal{O}/l^e)^* \to \mathrm{Gal}(K^f/K)$$

is $\bar{U} \times S''$ where S'' is a subgroup of T' with index $u(l-1)$.

Let W_0 be the subgroup of $\bar{W}$ of order l^μ. Then $K_{\mathrm{anti}}^{(n)}$ is the fixed field of $\bar{U} \times W_0 \times T \times T'$. Now class field theory yields (see Neukirch [5]),

$$\begin{aligned} \mathfrak{p} \text{ splits in } K_{\mathrm{anti}}^{(n)} \quad &\Leftrightarrow \quad \left(\frac{K^f/K}{\mathfrak{p}}\right) \in \bar{U} \times W_0 \times T \times T' \\ &\Leftrightarrow \quad \left(\frac{K^f/K}{\mathfrak{p}^{h(l-1)}}\right) \in \bar{U} \times S'' \\ &\Leftrightarrow \quad b^* \equiv 0 \mod l^e \end{aligned}$$

if we write $\mathfrak{p}^{h(l-1)} = (a^* + b^*\omega)$.

To show that $\mathfrak{p}$ only splits in a finite number of steps of K_{anti}, we must show that $b^* \neq 0$. But this follows from $(a^*, b^*) = 1$, which is seen in the same way as $(a, b) = 1$ above.

(b) If l is inert in K, everything goes the same way except that T' now has order $u(l^2-1)/2$.

(c) Suppose l ramifies in K and we are not in the exceptional case. Then T' has order $u(l-1)/2$, and everything goes as above using the conductor $f = l^e$ with $e = n + \mu - \nu$.

(d) Suppose we are in the exceptional case. Then $|T| = 3^{\mu-\nu+1}$ and $|T'| = u(l-1)/2$. Using the conductor $f = l^e$ with $e = n+2+\mu-\nu$, the same arguments hold if we write $\mathfrak{p}^{3h} = (a^* + b^*\omega)$. □

Remark. Everything goes the same way if one uses the exponent of K's class group instead of h.

Corollary 1. *No rational prime p splits completely in K_{anti}.*

Proof. The prime l is (infinitely) ramified in K_{anti}, since otherwise K_{anti} would be an infinite unramified extension of K, contradicting the finiteness of the class number. If p is different from l, the claim follows from the last statement of Theorem 2. □

When the l-Hilbert class field of K is non-trivial, the decomposition law depends on how much of it is contained in K_{anti}, expressed by the number ν. Since all primes trivially split in $K_{\mathrm{anti}}^{(0)} = K$, but not all primes split in $K_{\mathrm{anti}}^{(1)}$, we can give the following description of ν (here stated in the case where l splits in K, the other cases are similar): *Let p run through all primes $\neq l$ that split in K, and compute b^* as in Theorem 2(a). Then ν is the minimal integer such that $l^{1+\mu-\nu}$ divides all the b^*.* We illustrate this principle by three examples.

Example 2. Let $l = 5$ and $K = \mathbb{Q}(\sqrt{-599})$. The class group of K is cyclic of order 25. Thus $\mu = 2$ and $\nu = 0, 1$, or 2. The prime $p = 2$ splits in K since $(-599/2) = 1$. We therefore write $2^{25} = a^2 + ab + 150b^2$ with $a = 5737$ and $b = 49$ and find $b^* = 37079430566955$ (Theorem 2(a)). Since b^* is divisible by 5, but not by 25, we conclude $\nu = 2$. In other words: *the entire Hilbert class field K_H of K is contained in K_{anti}.*

Example 3. Let $l = 5$ and $K = \mathbb{Q}(\sqrt{-479})$. Again, the class group of K is cyclic of order 25, so $\mu = 2$ and $\nu = 0, 1$, or 2. Further, $p = 2$ again splits in K. Writing $2^{25} = a^2 + ab + 120b^2$ with $a = -56$ and $b = 529$ gives $b^* = -14765386940175$ which is divisible by 25, but not by 125. This shows $\nu \geq 1$, so K_H contains at least $K_{\text{anti}}^{(1)}$. Now class field theory gives a simple decomposition law for $K_{\text{anti}}^{(1)}$: *a prime ideal $\mathfrak{p}$ of K splits in $K_{\text{anti}}^{(1)}$ iff it has order 1 or 5 in the ideal class group.* Since 2^5 is not of the form $a^2 + ab + 120b^2$, a prime $\mathfrak{p}$ of K dividing 2 has order 25 in the class group, so it does not split in $K_{\text{anti}}^{(1)}$. If ν were equal to 2, Theorem 2(a) would contradict this. Hence ν equals 1, and we conclude: *K_{anti} contains the subfield of K_H of degree 5 over K, but not the entire K_H.*

Example 4. Let $l = 5$ and $K = \mathbb{Q}(\sqrt{-2887})$. The class group of K is cyclic of order 25. Writing $2^{25} = a^2 + ab + 722b^2$ with $a = 4771$ and $b = 119$ gives $b^* = -503658527236874547125$ which is divisible by 125. The same arguments as in Example 2 show that $p = 2$ is inert in H_K. This implies $\nu = 0$ and therefore: *K_H and K_{anti} are linearly disjoint over K.*

IV. The first step of the anti-cyclotomic extension

In this section we address the problem of finding the first step $K_{\text{anti}}^{(1)}$ of the anti-cyclotomic extension K_{anti}/K. By "finding" we understand displaying explicitly a polynomial f over $\mathbb{Q}$ of degree l having $K_{\text{anti}}^{(1)}$ as its splitting field. The decomposition laws from Section II then dictate the factorisation of f modulo p. In some cases we will actually use this knowledge of the factorisation to identify f among a number of candidates.

To begin with, recall that $K_{\text{anti}}^{(1)}$ is a dihedral extension of $\mathbb{Q}$ of degree $2l$ having K as its quadratic subfield, and that $K_{\text{anti}}^{(1)}/K$ is unramified outside l. If K is l-rational, $K_{\text{anti}}^{(1)}$ is unique with these properties. We state without proof a lemma that allows us easily to determine if a given dihedral extension is unramified, or unramified outside l, over its quadratic subfield.

Lemma 4. *Consider a dihedral extension $M/\mathbb{Q}$ of degree $2l$ having K as its quadratic subfield. Let L be one of the l subfields of M of absolute degree l. Then the cyclic extension M/K is unramified iff the field discriminants satisfy $d_L = d_K^{(l-1)/2}$. Further, M/K is unramified outside l iff $d_L = (\text{power of } l) \cdot d_K^{(l-1)/2}$.*

So when K is l-rational, we can find $K_{\text{anti}}^{(1)}$ by guessing a D_l-polynomial f whose splitting field contains K, and such that the discriminant condition of the lemma is satisfied. Some examples are given in the following table.

Δ	h	f (for $l=3$)	f (for $l=5$)
1	1	X^3-3X-4	$X^5+2500X+120000$
2	1	$X^3-3X-10$	$X^5+6875X+17500$
3	1	X^3-3	$X^5+10X^3-15X^2+10X-12$
5	2	X^3-3X-8	$X^5+20X+32$
6	2	X^3+3X-2	$X^5+15X^3-70X^2+60X-24$
7	1	X^3-3X-5	$X^5+15X^3-5X^2+35X-91$
10	2	$X^3-3X-22$	$X^5-5X+12$
11	1	X^3+6X-1	$X^5-15X^3-15X^2+110X+143$
13	2	$X^3+9X-36$	$X^5+25772500X-395460000$
14	4	$X^3-3X-26$	$X^5+10X^3-140X^2+585X-532$
15	2	X^3+3X-1	X^5+5X^2+3
17	4	$X^3+6X-28$	$X^5-35X^3-30X^2+1060X-2616$
19	1	X^3+6X-5	$X^5+35X^3-40X^2+160X-232$

Consider one of the polynomials f from the table, and let p be a prime not dividing the discriminant of f. If p is inert in K, then it splits in $K^{(1)}_{\text{anti}}$. It follows that f is the product of one linear and $(l-1)/2$ irreducible quadratic polynomials modulo p. If, on the other hand, p splits as $\mathfrak{pq}$ in K, then f is either irreducible modulo p, or f is the product of linear factors modulo p; this happens according to whether $\mathfrak{p}$ is inert or splits in $K^{(1)}_{\text{anti}}$.

For example, the result mentioned in the introduction about the factorisation of the polynomial $X^5+20X+32$ modulo p follows immediately from the above table and Example 1 in Section III.

When K is not l-rational, finding $K^{(1)}_{\text{anti}}$ is harder since it is no longer unique with the property of being dihedral over $\mathbb{Q}$ and unramified outside l over K. But this case can be dealt with by first finding all fields with that property, and then identifying $K^{(1)}_{\text{anti}}$ using our knowledge of which primes split in that field. This method always leads to a conclusive answer, for different Galois extensions have different sets of splitting primes by a theorem of Bauer (see Neukirch [5, page 572]). We illustrate by two examples.

Example 1. Let $l=3$ and consider $K=\mathbb{Q}(\sqrt{-21})$. This field is not 3-rational, indeed it has (two linearly disjoint and hence) four $\mathbb{Z}/3$-extensions which are unramified outside 3 and dihedral over $\mathbb{Q}$ (see Brink [2]). Using Lemma 4 and a computer, we easily find four polynomials $f_1,\dots,f_4$ whose splitting fields are the above-mentioned four dihedral fields. The polynomials are shown in the table below together with all primes <200 modulo which they split into linear factors. These prime lists are the "fingerprints" of the polynomials, and we shall use them to uncover the culprit among our four suspects.

i	f_i	primes <200 modulo which f_i splits
1	$X^3-3X+16$	17, 101, 107, 139, 179, 193
2	$X^3+9X+12$	11, 19, 89, 103, 191
3	$X^3+9X+30$	5, 71, 109, 199
4	$X^3+18X+12$	23, 31, 37, 41, 173

Now consider a prime p that splits in K, i.e. with $(-21/p)=1$. The class group of K has exponent 2, so we may write

$$p^2=a^2+21b^2$$

with relatively prime $a, b \in \mathbb{N}$. This is shown in the table below for all $p < 200$. We have

$$(a + b\sqrt{-21})^3 = (a^3 - 63ab^2) + (3a^2b - 21b^3)\sqrt{-21}\ .$$

Therefore, by Theorem 2(d), p splits in $K_{\text{anti}}^{(1)}$ iff $b^* = 3a^2b - 21b^3$ is divisible by 27. The primes for which this is the case are typed with bold in the table.

p	a	b	b^*	p	a	b	b^*
5	2	1	−9	101	74	15	175545
11	10	1	279	103	47	20	−35460
17	10	3	333	107	82	15	231705
19	5	4	−1044	109	59	20	40860
23	2	5	−2565	139	85	24	229896
31	25	4	6156	**173**	170	7	599697
37	5	8	−10152	179	10	39	−1233999
41	34	5	14715	191	170	19	1503261
71	50	11	54549	193	185	12	1195812
89	86	5	108315	199	185	16	1556784

Comparing the bold primes with the ones in the previous table reveals f_4 as the wanted polynomial.

Let us note additionally that p splits in the 3-part of K's ray class field of conductor 3 iff b is divisible by 3. The table shows that this is the case for the primes $17, 101, 107$ etc., i.e. the primes modulo which the polynomial f_1 splits. So this ray class field is the splitting field of f_1. Finally, all four polynomials f_i split modulo p iff b is divisible by 9.

Example 2. We now aim at finding the first step of the anti-cyclotomic extension of $K = \mathbb{Q}(\sqrt{-107})$ for $l = 3$. Again, there are four $\mathbb{Z}/3$-extensions of K which are unramified outside 3 and dihedral over $\mathbb{Q}$ (see Brink [2]), and we find four candidate polynomials:

i	f_i	primes < 200 modulo which f_i splits
1	$X^3 - X + 4$	$29, 47, 83, 137$
2	$X^3 + 6X - 17$	$23, 37, 47, 61, 79, 101, 149$
3	$X^3 + 15X - 28$	$11, 19, 47, 151, 163, 197$
4	$X^3 + 18X - 45$	$13, 41, 47, 53, 89, 193, 199$

The class number of K is 3, and since f_1 generates a cubic field with discriminant -107, the splitting field of f_1 is the Hilbert class field of K. The anti-cyclotomic decomposition law depends on whether this class field is contained in K_{anti} (and thus equals $K_{\text{anti}}^{(1)}$) or not.

Let $p \neq 3$ be a prime that splits in K. Since K has class number 3, we write

$$p^3 = a^2 + ab + 27b^2$$

with relatively prime $a, b \in \mathbb{Z}$. This representation is shown in the table below for all $p < 200$. We are in case (a) of Theorem 2 and must compute

$$(a + b\omega)^2 = (a^2 - 27b^2) + (2ab + b^2)\omega\ .$$

Thus, p splits in $K^{(1)}_{\text{anti}}$ iff $b^* = 2ab + b^2$ is divisible by $3^{3-\nu}$.

p	a	b	b^*
11	1	7	63
13	1	9	99
19	64	9	1233
23	89	11	2079
29	107	20	4680
37	163	27	9531
41	118	43	11997
47	253	34	18360
53	341	29	20619
61	442	27	24597
79	523	81	91287

p	a	b	b^*
83	109	142	51120
89	694	79	115893
101	962	47	92637
137	163	304	191520
149	953	281	614547
151	1412	207	627417
163	1360	279	836721
193	1189	441	1243179
197	2690	83	453429
199	316	531	617553

Now if the Hilbert class field were contained in K_{anti}, that is, if $\nu = 1$, then all the primes in the table would split in $K^{(1)}_{\text{anti}}$ since all the b^* are divisible by 9. Not only does this seem unlikely, it is also demonstrably false since none of the polynomials f_i splits modulo all these primes. Hence $\nu = 0$, and the Hilbert class field is not contained in K_{anti}. So the p's that split in $K^{(1)}_{\text{anti}}$ are the ones for which 27 divides b^*. These primes (typed bold in the table) are the ones in the second line of the previous table, thereby identifying f_2 as the polynomial whose splitting field is $K^{(1)}_{\text{anti}}$.

References

[1] J. A. Antoniadis, *Diedergruppe und Reziprozitätsgesetz*, J. Reine Angew. Math. **377** (1987), 197–209. MR887409 (88g:11081)

[2] D. Brink, *On $\mathbb{Z}_p$-embeddability of cyclic p-class fields*, C. R. Math. Acad. Sci. Soc. R. Can. **27** (2005), 48–53. MR2142958 (2006c:11128)

[3] J. E. Carroll, H. Kisilevsky, *Initial layers of $\mathbb{Z}_l$-extensions of complex quadratic fields,* Compositio Math. **32** (1976), no. 2, 157–168. MR0406970 (53:10755)

[4] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326. MR0349627 (50:2120)

[5] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.

Department of Mathematics, Universitetsparken 5, 2100 Copenhagen, Denmark

E-mail address: brink@math.ku.dk

Current address: Departamento de Matemática, Universidade de Brasília, 70910-900 Brasília-DF-Brazil