C. R. Math. Rep. Acad. Sci. Canada Vol. **27**, (2), 2005 pp. 48–53

ON $\mathbb{Z}_P$-EMBEDDABILITY OF CYCLIC P-CLASS FIELDS

DAVID BRINK

Presented by George A. Elliott, FRSC

ABSTRACT. It is investigated when a cyclic p-class field of an imaginary quadratic number field can be embedded in an infinite pro-cyclic p-extension.

RÉSUMÉ. On donne des conditions pour qu'un p-corps de classes cyclique d'un corps de nombres quadratique imaginaire soit plongeable dans une p-extension pro-cyclique infinie.

Consider an imaginary quadratic number field K. Let p be an odd prime number, and denote by $\mathbb{Z}_p$ the pro-cyclic pro-p-group $\varprojlim_n(\mathbb{Z}/p^n)$. As shown by Iwasawa, any $\mathbb{Z}_p$-extension of K is unramified outside p. The lower steps of such an extension might well be unramified also at p. In this article the following question is investigated: *If the p-class group of K is non-trivial and cyclic, is the p-Hilbert class field of K (or part of it) then embeddable in a $\mathbb{Z}_p$-extension of K?* In doing so, we are led to study the torsion subgroup of the Galois group over K of the maximal abelian p-extension of K which is unramified outside p. First fix some notation:

p :	an odd prime number
ζ :	a primitive p-th root of unity
Δ :	a square-free natural number
K :	the imaginary quadratic number field $\mathbb{Q}(\sqrt{-\Delta})$
$\mathcal{O}$:	the ring of integral elements in K
K_0 :	the p-Hilbert class field of K
K_e :	the p-part of K's ray class field with conductor p^e, $e \geqq 0$
K_∞ :	the union $\bigcup_{e=0}^{\infty} K_e$
T :	the torsion subgroup of $\mathrm{Gal}(K_\infty/K)$
K^{cycl} :	the cyclotomic $\mathbb{Z}_p$-extension of K
K^{anti} :	the anti-cyclotomic $\mathbb{Z}_p$-extension of K
I :	the group of fractional ideals of K prime to p
P :	the group of principal fractional ideals of K prime to p
P_e :	the ray modulo p^e, $e \geqq 0$.

Note that the ray class field with conductor 1 is exactly the Hilbert class field so that the notation is consistent. We have the tower

$$K \subseteqq K_0 \subseteqq K_1 \subseteqq K_2 \subseteqq \cdots \subset K_\infty$$

and note that the union K_∞ is the maximal abelian p-extension of K which is unramified outside p. Thus, by Iwasawa's result, any $\mathbb{Z}_p$-extension of K is

Received by the editors on January 21, 2005.
AMS subject classification: 11R32.

contained in K_∞. It is well known that K_∞ is the composite of three fields K^{cycl}, K^{anti}, and K^T which are linearly disjoint over K (see [1]). The cyclotomic extension K^{cycl} is the unique $\mathbb{Z}_p$-extension of K which is abelian over $\mathbb{Q}$. The anti-cyclotomic extension K^{anti} is the unique $\mathbb{Z}_p$-extension of K which is pro-dihedral over $\mathbb{Q}$. Finally, K^T is a finite extension of K with $\text{Gal}(K^T/K) \cong T$ and dihedral over $\mathbb{Q}$ (but not unique with these properties). As we shall see, we may usually for K^T take K_0 or a subfield of K_0. From the above discussion follows the isomorphism

$$\text{Gal}(K_\infty/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times T$$

which will be important in the following. It may also be noted that the composite $K^{\text{anti}}K^T$ is the maximal abelian p-extension of K which is unramified outside p and dihedral over $\mathbb{Q}$, and hence equals the union of all p-ring class fields over K with conductor a power of p.

THEOREM 1.

(i) *Assume $p > 3$ and that $K(\zeta)$ has the same p-class number as K. Then T is trivial, and K_0/K is cyclic (possibly trivial) and $\mathbb{Z}_p$-embeddable.*

(ii) *Assume $p = 3$, $\Delta \not\equiv 3 \pmod 9$, and that the class number of $\mathbb{Q}(\sqrt{3\Delta})$ is not divisible by 3. Then T is trivial, and K_0/K is cyclic (possibly trivial) and $\mathbb{Z}_p$-embeddable.*

PROOF. Since the p-Hilbert class field K_0 is dihedral over $\mathbb{Q}$, it is contained in $K^{\text{anti}}K^T$. So if we show $T = 0$, it will follow that K_0 is contained in K^{anti}.

Let r be the p-rank of $\text{Gal}(K_\infty/K)$. Shafarevich gives in [4] a formula for r which implies $r = 2$ if the completion $\mathbb{Q}_p(\sqrt{-\Delta})$ does not contain ζ, and K has no element x such that the radical extension $K(\zeta, \sqrt[p]{x})/K(\zeta)$ is non-trivial and unramified (such elements are called *hyperprimary*, see [2] for more details on this).

(i) For $p > 3$, $\mathbb{Q}_p(\sqrt{-\Delta})$ never contains ζ. The assumption on the class number of $K(\zeta)$ implies that $K_0(\zeta)$ is the p-Hilbert class field of $K(\zeta)$. In particular, $K_0(\zeta)/K$ is abelian. Assume for a contradiction that K has a non-trivial hyperprimary element x, *i.e.*, that $K(\zeta, \sqrt[p]{x})/K(\zeta)$ is an unramified $\mathbb{Z}/p$-extension. Then $\sqrt[p]{x}$ is contained in $K_0(\zeta)$. But $K(\sqrt[p]{x})$ is not normal over K, a contradiction. So we have shown $r = 2$ and hence $T = 0$.

(ii) The assumption $\Delta \not\equiv 3 \pmod 9$ implies $\zeta \notin \mathbb{Q}_3(\sqrt{-\Delta})$. The 3-class number of $K(\zeta) = K(\sqrt{-3})$ is the product of the 3-class numbers of K, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{3\Delta})$. So the assumption on the class number of $\mathbb{Q}(\sqrt{3\Delta})$ implies that $K_0(\zeta)$ is the 3-Hilbert class field of $K(\zeta)$. The rest of the proof is the same as in (i). ∎

In [3], Jaulent and Nguyen Quang Do show $T = 0$ under the assumptions of (ii). For $p > 3$, they show $T = 0$ if K has trivial p-class group.

For $p = 3$, this theorem applies for many values of Δ, for instance 23, 26, 29, 31, and 38. In all these cases, K_0/K is cyclic of degree 3 and $\mathbb{Z}_3$-embeddable.

The smallest values of Δ for which the theorem does not apply are 107 (because $\mathbb{Q}(\sqrt{3 \cdot 107})$ has class number 3) and 129 (which is $\equiv 3 \pmod 9$).

For $p = 5$, the theorem likewise applies for many Δ, for instance 47, 74, 79, and 86. In these cases, K_0/K is cyclic of degree 5 and $\mathbb{Z}_5$-embeddable. The smallest values of Δ for which the theorem does not apply are 127 and 166 (in both cases, K has 5-class number 5, whereas that of $K(\zeta)$ is 25 and 125, respectively).

It may be noted that the theorem never applies when p is an *irregular* prime, *i.e.*, when the class number of $\mathbb{Q}(\zeta)$ is divisible by p.

We shall now see how the remaining cases can be dealt with. Recall that the *ray group* modulo p^e is the subgroup P_e of P generated by the principal ideals (α) with integral $\alpha \equiv 1 \pmod{p^e}$. The *ray class group* modulo p^e is the quotient I/P_e. It is a central result in class field theory that there is an isomorphism, the *Artin symbol*, from the p-part of I/P_e to $\mathrm{Gal}(K_e/K)$. It maps the p-part of P/P_e onto $\mathrm{Gal}(K_e/K_0)$.

Lemma 2.

(i) *With notation as above, we have for $p > 3$,*

$$\mathrm{Gal}(K_e/K_0) \cong \begin{cases} \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e-1} & \text{if } p \nmid \Delta, \\ \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e} & \text{if } p \mid \Delta. \end{cases}$$

Taking the inverse limit gives $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. *In particular,* $T = 0$ *if* $K_0 = K$.

(ii) *For $p = 3$, the above remains valid when $\Delta \not\equiv 3 \pmod 9$. Assume $\Delta \equiv 3 \pmod 9$ and $\Delta \neq 3$. Then*

$$\mathrm{Gal}(K_e/K_0) \cong \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3.$$

Taking the inverse limit gives $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}/3$. *In particular,* $T \cong \mathbb{Z}/3$ *if* $K_0 = K$.

Proof. There is a natural exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow (\mathcal{O}/p^e)^* \longrightarrow P/P_e \longrightarrow 1.$$

The exclusion of the case $p = \Delta = 3$ ensures that $\mathcal{O}^*$ has trivial p-part. Hence $\mathrm{Gal}(K_e/K_0)$ is isomorphic to the p-part of $(\mathcal{O}/p^e)^*$ by the Artin symbol. So we compute the structure of $(\mathcal{O}/p^e)^*$.

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

The order of $(\mathcal{O}/p^e)^*$, *i.e.*, the norm of the ideal $p^e\mathcal{O}$, depends on the prime ideal decomposition of p in K. More precisely, the order of the p-part is

$$|p\text{-part of } (\mathcal{O}/p^e)^*| = \begin{cases} p^{2e-2} & \text{if } p \nmid \Delta, \\ p^{2e-1} & \text{if } p \mid \Delta. \end{cases}$$

We note the following two facts:

(∗) Let $x \in \mathcal{O}$ and write $(1+x)^p = 1+x'$. If $p^i \parallel x$ for some $i \geqq 1$ (meaning that $p^i \mid x$, but $p^{i+1} \nmid x$), then $p^{i+1} \parallel x'$.

(∗∗) Let a and b be integers with $a \equiv 1 \pmod p$ and $p^i \parallel b$ for some $i \geqq 1$. Write $(a+b\sqrt{-\Delta})^p = a' + b'\sqrt{-\Delta}$. Then $a' \equiv 1 \pmod p$ and $p^{i+1} \parallel b'$.

It follows from (∗) that the cyclic subgroups $U := \langle 1+p \rangle$ and $V := \langle 1+p\sqrt{-\Delta} \rangle$ of $(\mathcal{O}/p^e)^*$ both have order p^{e-1}. It follows from (∗∗) that they have trivial intersection. So for $p \nmid \Delta$,

$$(p\text{-part of } (\mathcal{O}/p^e)^*) = U \times V \cong \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e-1}.$$

Assume $p \mid \Delta$. Then $U \times V$ has index p in the p-part of $(\mathcal{O}/p^e)^*$. If $p > 3$, or $p = 3$ and $\Delta \not\equiv 3 \pmod 9$, the same argument shows

$$(p\text{-part of } (\mathcal{O}/p^e)^*) = U \times V' \cong \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^e$$

for $V' := \langle 1+\sqrt{-\Delta} \rangle$. In case $p = 3$ and $\Delta \equiv 3 \pmod 9$, the 3-part of $(\mathcal{O}/9)^*$ is $\langle 4 \rangle \times \langle 1+3\sqrt{-\Delta} \rangle \times \langle 1+\sqrt{-\Delta} \rangle \cong (\mathbb{Z}/3)^3$, and therefore

$$(3\text{-part of } (\mathcal{O}/3^e)^*) = U \times V \times (\text{group of order } 3) \cong \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e-1} \times \mathbb{Z}/3.$$

This finishes the proof of the lemma. ∎

The question of $\mathbb{Z}_p$-embeddability in the case where the p-class field is cyclic of degree p can now be answered.

THEOREM 3. *Assume K_0/K is cyclic of degree p. Pick a prime $\mathfrak{q} \nmid p$ of K of order p in the class group, and write $\mathfrak{q}^p = (\alpha)$ with $\alpha \in \mathcal{O}$.*

(i) *Suppose $p > 3$.*

  (a) *If α is not a p-th power in $(\mathcal{O}/p^2)^*$, then K_0/K is $\mathbb{Z}_p$-embeddable (in fact K_0 is contained in K^{anti}), and $T = 0$.*

  (b) *If α is a p-th power in $(\mathcal{O}/p^2)^*$, then K_0/K is not embeddable in $\mathbb{Z}/p^2$-extension unramified outside p, and $T \cong \mathbb{Z}/p$.*

(ii) *Now suppose $p = 3$. If $\Delta \not\equiv 3 \pmod 9$, all the above remains valid. Assume $\Delta \equiv 3 \pmod 9$, and write $\alpha \equiv a + b\sqrt{-\Delta} \pmod 9$ with $a, b \in \mathbb{Z}$.*

  (c) *If $(a,b) \equiv (\pm 1, 0)$ modulo 3, but not modulo 9, then K_0/K is $\mathbb{Z}_3$-embeddable (in fact K_0 is contained in K^{anti}), and $T \cong \mathbb{Z}/3$.*

  (d) *If $(a,b) \not\equiv (\pm 1, 0)$ modulo 3, then K_0/K is embeddable in a $\mathbb{Z}/9$-extension unramified outside 3, but not in a $\mathbb{Z}/27$-extension unramified outside 3, and $T \cong \mathbb{Z}/9$.*

  (e) *If $(a,b) \equiv (\pm 1, 0)$ modulo 9, then K_0/K is not embeddable in a $\mathbb{Z}/9$-extension unramified outside 3, and $T \cong \mathbb{Z}/3 \times \mathbb{Z}/3$.*

PROOF. (i) Assume $p > 3$. By Lemma 2, $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Since $\mathrm{Gal}(K_0/K) \cong \mathbb{Z}/p$, there are two possibilities for T: either 0 or $\mathbb{Z}/p$.

(a) If $T = 0$, *i.e.*, $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p$, then K_0 is contained in $K^{\mathrm{cycl}}K^{\mathrm{anti}}$. Since K_0 is dihedral over $\mathbb{Q}$, it is in fact contained in K^{anti}. Both I/P_2 and P/P_2

have p-rank 2. Therefore, $\mathfrak{q}^p = (\alpha)$ is *not* a p-th power in P/P_2. So α is not a p-th power in $(\mathcal{O}/p^2\mathcal{O})^*$.

(b) If $T \cong \mathbb{Z}/p$, *i.e.*, $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}/p$, then K_0 is linearly disjoint from $K^{\mathrm{cycl}}K^{\mathrm{anti}}$. So we may for K^T take K_0. Hence no $\mathbb{Z}/p^2$-extension of K inside K_∞ contains K_0. Now the p-part of P/P_2 is a direct summand in the p-part of I/P_2. Therefore, $\mathfrak{q}^p = (\alpha)$ *is* a p-th power in P/P_2. So α is a p-th power in $(\mathcal{O}/p^2\mathcal{O})^*$.

(ii) Now assume $p = 3$. If $\Delta \not\equiv 3 \pmod 9$, everything goes as above. Henceforth assume $\Delta \equiv 3 \pmod 9$. Then $(\mathcal{O}/9)^* \cong \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3$ (see the proof of Lemma 2), so that $\alpha = a + b\sqrt{-\Delta}$ is a cube in $(\mathcal{O}/9)^*$ iff $(a, b) \equiv (\pm 1, 0)$ modulo 9. Further, $(\mathcal{O}/3)^* \cong \mathbb{Z}/2 \times \mathbb{Z}/3$, so that α is a cube in $(\mathcal{O}/3)^*$ iff $(a, b) \equiv (\pm 1, 0)$ modulo 3. By Lemma 2, $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}/3$. Since $\mathrm{Gal}(K_0/K) \cong \mathbb{Z}/3$, there are three possibilities for T: $\mathbb{Z}/3$, $\mathbb{Z}/9$, or $\mathbb{Z}/3 \times \mathbb{Z}/3$.

(c) If $T \cong \mathbb{Z}/3$, *i.e.*, $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}/3$, then K_0 is contained in $K^{\mathrm{cycl}}K^{\mathrm{anti}}$ and therefore also in K^{anti}. Both I/P_2 and P/P_2 have 3-rank 3. Therefore, $\mathfrak{q}^3 = (\alpha)$ is *not* a cube in P/P_2. So α is not a cube in $(\mathcal{O}/9)^*$. On the other hand, the 3-part of P/P_1 is a direct summand in the 3-part of I/P_1. Therefore, $\mathfrak{q}^3 = (\alpha)$ *is* a cube in P/P_1. So α is a cube in $(\mathcal{O}/3)^*$. This shows the claims about a and b.

The cases (d) where $T \cong \mathbb{Z}/9$ and (e) where $T \cong \mathbb{Z}/3 \times \mathbb{Z}/3$ are treated in a similar manner, so their proofs are omitted. ∎

The same arguments give a description of the torsion subgroup T in the general case where K_0/K is not necessarily cyclic: If $p > 3$, or $p = 3$ and $\Delta \not\equiv 3 \pmod 9$, then $K_\infty = K^{\mathrm{cycl}}K^{\mathrm{anti}}K_0$, and therefore $T \cong \mathrm{Gal}(K_0/K_0 \cap K^{\mathrm{anti}})$, *i.e.*, T is isomorphic to a subgroup of $\mathrm{Gal}(K_0/K)$ with cyclic quotient. If $p = 3$ and $\Delta \equiv 3 \pmod 9$, then K_∞ has degree 3 over $K^{\mathrm{cycl}}K^{\mathrm{anti}}K_0$, and therefore T has a subgroup of index 3 which is isomorphic to $\mathrm{Gal}(K_0/K_0 \cap K^{\mathrm{anti}})$.

The following examples answer the questions regarding $\mathbb{Z}_p$-embeddability from the beginning of the article (*i.e.*, for $p = 3$, $\Delta = 107, 129$ and $p = 5$, $\Delta = 127, 166$) and show that all cases of Theorem 4 occur.

Examples. (i) Let $p = 5$ and $\Delta = 127$. The class number of K is 5. The prime number 2 is divisible by a non-principal prime ideal $\mathfrak{q}$ of K. Further, $\mathfrak{q}^5 = (\alpha)$ with $\alpha = (1 + \sqrt{-127})/2$ since $2^5 = \alpha\bar{\alpha}$. Since α is not a fifth power in $(\mathcal{O}/25)^*$, we are in case (a).

(ii) Let $p = 5$ and $\Delta = 166$. The class number of K is 10. Here 7 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^5 = (\alpha)$ is principal, $\alpha = (129 + \sqrt{-166})/2$. Modulo 25 we have $\alpha \equiv \alpha^5$ and conclude that we are in case (b).

(iii) Let $p = 3$ and $\Delta = 107$. The class number of K is 3. Here 11 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = (9 + 7\sqrt{-107})/2$. Modulo 9 we have $\alpha \equiv \alpha^3$ and conclude that we are in case (b).

(iv) Let $p = 3$ and $\Delta = 237$. The class number of K is 12. Here 13 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = 8 + 3\sqrt{-237}$.

We are in case (c).

(v) Let $p = 3$ and $\Delta = 129$. The class number of K is 12. Here 13 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = 41+2\sqrt{-129}$. We are in case (d).

(vi) Let $p = 3$ and $\Delta = 3387$. The class number of K is 12. Here the prime 43 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = (209 + 9\sqrt{-3387})/2 \equiv 1 \pmod 9$. We are in case (e).

As is the case for the ideal class group, there is numerical evidence that the torsion subgroup T "prefers" having small rank, so that case (e) occurs quite rarely.

Finally a criterion for $\mathbb{Z}_p$-embeddability of a cyclic p-class field (or part of it) of arbitrary degree is given.

THEOREM 4. *Assume K_0/K is cyclic of degree $p^n > 1$, and let F/K be some subextension.*

(i) *Suppose $p > 3$. Then F/K is $\mathbb{Z}_p$-embeddable if it is embeddable in a $\mathbb{Z}/p^{n+1}$-extension unramified outside p.*

(ii) *Suppose $p = 3$. If $\Delta \not\equiv 3 \pmod 9$, the above holds. Assume $\Delta \equiv 3 \pmod 9$. Then F/K is $\mathbb{Z}_3$-embeddable if it is embeddable in a $\mathbb{Z}/3^{n+2}$-extension unramified outside 3.*

PROOF. Only (i) is proved since the proof of (ii) is very similar. Put $F' := K_0 \cap K^{\mathrm{cycl}} K^{\mathrm{anti}} = K_0 \cap K^{\mathrm{anti}}$, and let p^i be the degree of F'/K. It is the maximal $\mathbb{Z}_p$-embeddable subextension of K_0/K. Then $T \cong \mathbb{Z}/p^{n-i}$. Assume F/K is not $\mathbb{Z}_p$-embeddable, *i.e.*, that F is a proper extension of F'. Assume that F/K is embedded in a cyclic extension L/K inside K_∞. Then $F' = L \cap K^{\mathrm{cycl}} K^{\mathrm{anti}}$. Therefore $[L : F'] = [K^{\mathrm{cycl}} K^{\mathrm{anti}} L : K^{\mathrm{cycl}} K^{\mathrm{anti}}] \leqq p^{n-i}$ and we conclude that $[L : K] \leqq p^n$. ∎

REFERENCES

1. J. E. Carroll and H. Kisilevsky, *Initial layers of $\mathbb{Z}_l$-extensions of complex quadratic fields.* Compositio Math. (2) **32** (1976), 157–168.
2. K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields.* Ann. of Math. (2) **98** (1973), 246–326.
3. J.-P. Jaulent and T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers, et ramification restreinte.* J. Théor. Nombres Bordeaux **5** (1993), 343–363.
4. I. R. Shafarevich, *Extensions with prescribed ramification points.* Publ. Math. Inst. Hautes Etudes Sci. **18** (1963), 71–95 (Russian); translation in: Collected mathematical papers, Springer, Berlin, 1989, pp. 245–316.

Department of Mathematics
University of Copenhagen
Universitetsparken 5
2100 Copenhagen
Denmark
email: brink@math.ku.dk