ACTA ARITHMETICA
LXXVIII.4 (1997)

On normal integral bases in ray class fields over imaginary quadratic fields

by

Cornelius Greither (Ste-Foy, P.Q.)

1. Introduction. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. A lot of interesting and deep work has been done on the Galois module structure of integers in ray class fields of K, notably by Cassou-Noguès and Taylor [1] and Schertz [9]. Let us recall that the first question in general Galois module theory is: If E/F is a tame abelian G-Galois extension of number fields, when is the projective $\mathcal{O}_F[G]$-module $\mathcal{O}_E$ actually free? In other words, does E/F admit a *normal integral basis* (NIB for short)? However, the ray class field extensions considered in [1] and [9] are mostly wild, and one has to replace $\mathcal{O}_F[G]$ by a suitable order in $F[G]$ in order to get freeness results. Moreover, this line of work deals with a very relative situation, that is, already the base field F is a rather large ray class field over K. When one insists that E/F be tame, and F be as close as possible to K, one is naturally led to the question: Does the ray class field $K(\mathfrak{p})$ have NIB over the Hilbert class field $K(1)$ of K? This question, about which not too much seems to be known, is the subject of this paper. We restrict ourselves to the case $h_K = 1$, i.e. $K(1) = K$. This restricts d to the nine-element set $D = \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

Gómez Ayala and Schertz [5] have shown that the question in the strictness and generality as just formulated has a negative answer, by means of exhibiting quadratic subfields of $K(\mathfrak{p})$ without normal basis over K. On the positive side, Gómez Ayala [4] proved the existence of a NIB for $\mathfrak{p} = (2)$ for d = 11,19,43,67,163. Here, $K(2)/K$ is a cubic extension. (The four other values $d \in D$ are irrelevant here for various reasons.) Thus one may optimistically hope that the failure shown in [5] is only due to the existence of subextensions of degree 2, and one might conjecture a positive result for odd-degree subextensions. There is also a very reasonable weakened version of the NIB property, called WNIB (see below; basically one replaces the group ring of G by its maximal order), and one might conjecture that there exists at least a WNIB for $K(\mathfrak{p})/K$.

We show in this paper that neither of these optimistic conjectures would be correct. Quite to the contrary: we prove, using subfields of odd prime degree l, that infinitely often for each $d \in D$, $K(\mathfrak{p})/K$ does not even have WNIB. The crucial tools which we use are Stickelberger ideals and explicit computations using the system PARI in class groups. While we do not explicitly use McCulloh's beautiful theory of realizable classes [7, 8], it is certainly the main motivation for our constructions. At the end of the paper, we discuss cubic extensions of K with prime conductor, extending Gómez Ayala's affirmative results and complementing them with some negative ones. We also offer some heuristics concerning the question just *how often* $K(\mathfrak{p})/K$ might fail to have a WNIB. These heuristics may be unsound, but our results certainly allow us to say that in general, $K(\mathfrak{p})/K$ fails in a serious and systematic fashion to have normal integral basis. The main results to this effect are Theorem 1.6 and Theorem 3.3 in this paper.

Let us just give a few examples. For $d = 43$, $K(23)/K$ has no WNIB; this is proved using a subextension of degree 11 of $K(23)$ over K. For $d = 67$, $K(41)/K$ has no WNIB; this is shown using the degree 7 subextension. The reader will find some tables in Section 3. We also briefly summarize our results on cubic extensions: Exclude $d = 3$ for simplicity, and suppose $\mathfrak{p}$ is a prime of K over p, such that either p is inert in K and $p \equiv 2 \pmod 3$, or p is split in K and $p \equiv 1 \pmod 3$. Let L be the (!) cubic subfield of $K(\mathfrak{p})$ over K. Then first of all, L/K always has weak normal integral basis. If p is inert, L/K always has NIB; if p is split, L/K has NIB "half of the time" in a precise sense for $d \neq 2, 11$, and always for $d = 2, 11$.

1. Preliminaries, and Kummer descent (I).

Let G be abelian and E/F be a tame G-Galois extension of number fields. Let $\mathfrak{M}$ be the maximal order in $\mathcal{O}_F[G]$. Define E/F to have *weak normal integral basis* if the projective $\mathfrak{M}$-module $\mathfrak{M} \otimes_{\mathcal{O}_F[G]} \mathcal{O}_E$ is free. Note that we may identify $\mathfrak{M} \otimes_{\mathcal{O}_F[G]} \mathcal{O}_E$ with $\mathfrak{M}\mathcal{O}_E \subset E$. There is a standard short exact sequence

$$0 \to D_F(G) \to \mathrm{Cl}(\mathcal{O}_F[G]) \to \mathrm{Cl}(\mathfrak{M}) \to 0,$$

where one may call $D_F(G)$ the kernel group of G over F. For $F = \mathbb{Q}$, one gets the usual kernel group. $\mathfrak{M}$ is canonically isomorphic to a direct product of rings of integers in cyclotomic extensions of F: $\mathfrak{M} \cong \bigoplus_\chi \mathcal{O}_{F(\chi)}$, with χ running through the set of F-conjugacy classes of linear characters of G. Thus, the class group of $\mathfrak{M}$ is just $\bigoplus_\chi \mathrm{Cl}(\mathcal{O}_{F(\chi)})$. On the other hand, the kernel group tends to be large and hard to calculate.

Now let l be a prime, $\zeta = \zeta_l \in F$, and $G = \langle \sigma \rangle$ a cyclic group of order l. For $i \in \mathbb{Z}$ let $E^{(i)} = \{x \in E : \sigma(x) = \zeta^i x\}$ the ith Kummer eigenspace; of course, $E^{(i)}$ only depends on i mod l. We have $E = E^{(0)} \oplus \ldots \oplus E^{(l-1)}$. Define $A_i = \mathcal{O}_E \cap E^{(i)}$; then A_i is projective of rank 1 over $\mathcal{O}_F$. Note that

$A_0 = \mathcal{O}_F$. The maximal order $\mathfrak{M}$ in $F[G]$ is now $\bigoplus_{i=0}^{l-1} \mathcal{O}_F\varepsilon_i$, where ε_i acts as ith projection $E \to E^{(i)} \subset E$.

LEMMA 1.1. (a) *$\varepsilon_i(\mathcal{O}_E) = l^{-1}A_i$ for $i = 0, \ldots, l-1$.*

(b) *$\mathfrak{M}\mathcal{O}_E$ is free over $\mathfrak{M}$ iff $A_1, \ldots, A_{l-1}$ are $\mathcal{O}_F$-free.*

Proof. Part (a) implies part (b) since $\mathfrak{M}\mathcal{O}_E = \bigoplus_{i=0}^{l-1} \varepsilon_i\mathcal{O}_E$. So let us prove (a); we do this by localizing at an arbitrary prime $\mathfrak{p}$ of F. If $\mathfrak{p}$ is not over l, then $\mathcal{O}_{E,\mathfrak{p}} = \bigoplus_i A_{i,\mathfrak{p}}$ and $\varepsilon_i\mathcal{O}_{E,\mathfrak{p}} = A_{i,\mathfrak{p}} = (l^{-1}A_i)_\mathfrak{p}$, as claimed. Suppose now $\mathfrak{p}$ divides l. Then $E_\mathfrak{p}/F_\mathfrak{p}$ is unramified (since E/F was tame), so there exists (see Childs [2]) an element $x \in A_{1,\mathfrak{p}}$ with $x^l \in \mathcal{O}_{F,\mathfrak{p}}^*$ such that $\mathcal{O}_{E,\mathfrak{p}}$ has an $\mathcal{O}_{F,\mathfrak{p}}$ basis $1, z, \ldots, z^{l-1}$ where we let $z = (x-1)/\lambda$, $\lambda = 1 - \zeta$. This shows that $\varepsilon_i(\mathcal{O}_{E,\mathfrak{p}}) = \mathcal{O}_{F,\mathfrak{p}}x^i/\lambda^{l-1} = l^{-1}\mathcal{O}_{F,\mathfrak{p}}x^i$. On the other hand, we have $\mathcal{O}_{F,\mathfrak{p}}x^i = A_{i,\mathfrak{p}}$ because x is a unit of $\mathcal{O}_{E,\mathfrak{p}}$, and (a) follows. ■

Now let $\mathfrak{A}_i = A_i^l$; for any i, this is a nonzero ideal in $\mathcal{O}_F$. From the definition of A_i it easily follows that $\mathfrak{A}_i$ is l-power free, i.e. not divisible by the lth power of a proper ideal. Since E/F is tame, the $\mathfrak{A}_i$ are all prime to l. By localizing one also sees easily that a prime $\mathfrak{p}$ of F ramifies in E iff it divides one of the $\mathfrak{A}_i$. Recall in this context that the index i runs mod l, and $\mathfrak{A}_0 = \mathcal{O}_F$. From the definition it is clear that $A_i^j \subset A_{ij}$ for any i and j, and therefore $\mathfrak{A}_i^j$ equals the product of $\mathfrak{A}_{ij}$ with the lth power of some ideal of F. Let us put this on record:

LEMMA 1.2. *For any $i, j \in \mathbb{Z}/l$, $\mathfrak{A}_{ij}$ equals the l-power free part of $\mathfrak{A}_i^j$.*

We now turn to descent theory. Suppose K is a number field disjoint with $\mathbb{Q}(\zeta_l)$; let $F = K(\zeta_l)$ and $\varDelta = \mathrm{Gal}(F/K)$. As usual, we fix the isomorphism $(\mathbb{Z}/l)^* \xrightarrow{\sim} \varDelta$ by mapping j to σ_j which is characterized by $\sigma_j(\zeta_l) = \zeta_l^j$. Suppose L/K is a G-extension with G cyclic of order l as before; put $E = FL$. Thus, the action of $\varDelta$ on F extends to an action of $\varDelta$ on E inducing the trivial action on L. The following observation is well known.

LEMMA 1.3. *For all $j \in (\mathbb{Z}/l)^*$, $i \in \mathbb{Z}/l$ we have $\sigma_jA_i = A_{ij}$, and also $\sigma_j\mathfrak{A}_i = \mathfrak{A}_{ij}$.*

Proof. From the definition of E_i and the formula $\sigma_j\zeta = \zeta^j$ one finds that $\sigma_jE^{(i)} = E^{(ij)}$; the first formula of the lemma follows, and the second formula is an immediate consequence obtained by raising to the lth power. ■

Let us now impose the additional hypothesis that L/K is tame, and ramified exactly in the prime $\mathfrak{p}$. (We make the latter assumption to keep things simple.) From global class field theory one sees that the absolute norm of $\mathfrak{p}$ is congruent 1 mod l, otherwise L could not exist; this implies that $\mathfrak{p}$ is totally split in F. Let us write

$$\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_{l-1},$$

where $\mathfrak{P}_j = \sigma_j^{-1}\mathfrak{P}_1$. Then we can write

$$\mathfrak{A}_i = \mathfrak{P}_1^{a_{i,1}} \cdot \ldots \cdot \mathfrak{P}_{l-1}^{a_{i,l-1}},$$

with $a_{i,k} \in \{0, 1, \ldots, l-1\}$.

Lemma 1.2 gives, on comparing prime decompositions, that $a_{ij,k} = [ja_{i,k}]$, where $[\cdot]$ denotes the smallest nonnegative residue modulo l. But Lemma 1.3 also gives that $a_{ij,k}$, the exponent of $\mathfrak{P}_k$ in $\mathfrak{A}_{ij}$, equals $a_{i,jk}$, the exponent of $\sigma_j^{-1}\mathfrak{P}_k$ in $\mathfrak{A}_i$. Therefore $a_{i,k} = [ika_{1,1}]$ for all $i, k \in \mathbb{Z}/l$. This shows that $a_{1,1}$ cannot be zero (otherwise all $\mathfrak{A}_i$ would be the unit ideal which contradicts the condition that E/F does ramify), and after changing our numbering of the $\mathfrak{P}_k$, we may even assume that $a_{1,1} = 1$. Let us rewrite this slightly:

Proposition 1.4. *With the above notation and hypotheses we have*

$$\mathfrak{A}_1 = \mathfrak{P}_1 \cdot \mathfrak{P}_2^2 \cdot \ldots \cdot \mathfrak{P}_{l-1}^{l-1} = \mathfrak{P}_1^{l\theta},$$

where $l\theta = \sum_{i=1}^{l-1} i \cdot \sigma_i^{-1} \in \mathbb{Z}[\Delta]$ *is the "standard lth Stickelberger element without denominator". For any i we have* $\mathfrak{A}_i = \mathfrak{P}_1^{\sigma_i l\theta}$.

Corollary 1.5. *We have* $\mathfrak{A}_1^i = \mathfrak{A}_i \cdot \mathfrak{P}_1^{(i-\sigma_i)l\theta}$, *and therefore* $A_1^i = A_i \cdot \mathfrak{P}_1^{(i-\sigma_i)\theta}$. *(Note here that* $(i-\sigma_i)\theta$ *really is in* $\mathbb{Z}[\Delta]$, *so the last expression makes sense.)*

The following theorem is the main tool in settling the existence of a WNIB in a given situation.

Theorem 1.6. *Assume that* L/K *is tame, cyclic of degree* l, *and ramified exactly in the prime* $\mathfrak{p}$ *of* K. *Let* $\mathfrak{P}$ *be a prime over* $\mathfrak{p}$ *in* $F = K(\zeta_l)$. *If* L/K *has WNIB, then the class* $[\mathfrak{P}] \in \mathrm{Cl}(\mathcal{O}_F)$ *is annihilated by the Stickelberger ideal* $J = \mathbb{Z}\Delta \cap \theta(\mathbb{Z}\Delta)$. *The converse implication holds if* l *does not divide* h_F.

Proof. Recall $E = FL$. Using $\mathcal{O}_E = \mathcal{O}_F\mathcal{O}_L$ we see that if L/K has WNIB, then so has E/F. (Similarly for NIB, as is very well known.) Suppose L/K has WNIB. Applying the preceding remarks and Lemma 1.1, we find that $A_1, \ldots, A_{l-1}$ are free over $\mathcal{O}_F$. Hence $\mathfrak{A}_1 = A_1^l$ is a principal $\mathcal{O}_F$-ideal. By Proposition 1.4, $\mathfrak{A}_1 = \mathfrak{P}_1^{l\theta}$, and $\mathfrak{P}$ is a conjugate of $\mathfrak{P}_1$, so $\mathfrak{P}^{l\theta}$ is principal. By Corollary 1.5, all $\mathfrak{P}^{(i-\sigma_i)\theta}$ are principal as well. Now J is generated by $l\theta$ and the elements $(i-\sigma_i)\theta$ as a $\mathbb{Z}\Delta$-module, and hence $\mathfrak{P}^\alpha$ is principal for all $\alpha \in J$.

Suppose for the converse that J annihilates $[\mathfrak{P}]$. Then for one thing, $\mathfrak{P}_1^{l\theta}$ is principal. Write $A_1 = \mathfrak{A}x$ where $\mathfrak{A}$ is some fractional ideal of F. Then $\mathfrak{A}^l$ is principal since it is isomorphic to $\mathfrak{A}_1 = A_1^l = \mathfrak{P}_1^{l\theta}$. Since h_F is by hypothesis not divisible by l, we see that $\mathfrak{A}$ is principal, and hence A_1 is free. Then all A_i are free since $A_i = \mathfrak{P}_1^{(\sigma_i-i)l\theta}A_1$ and the first factor on the right hand side is principal since the exponent $(\sigma_i - i)l\theta$ is in J. By Lemma 1.1, we conclude that E/F has WNIB, and it remains to descend to L/K.

Let $\mathfrak{M}$ be the maximal order in $K[G]$, $\mathfrak{M}'$ the maximal order in $F[G]$. The augmentation epimorphism induces splittings $\mathfrak{M} = \mathcal{O}_K \times \mathfrak{M}_0$ and $\mathfrak{M}' = \mathcal{O}_F \times \mathfrak{M}'_0$. The classes $[\mathfrak{M}\mathcal{O}_L] \in \mathrm{Cl}(\mathfrak{M})$ (respectively, $[\mathfrak{M}'\mathcal{O}_E] \in \mathrm{Cl}(\mathfrak{M}')$) are automatically already in $\mathrm{Cl}_0(\mathfrak{M}) = \ker(\mathrm{Cl}(\mathfrak{M}) \to \mathrm{Cl}(\mathcal{O}_K)) = \mathrm{Cl}(\mathfrak{M}_0)$ (respectively, in $\mathrm{Cl}_0(\mathfrak{M}') = \mathrm{Cl}(\mathfrak{M}'_0)$). We thus know from the last paragraph that the class of $\mathfrak{M}'\mathcal{O}_E$ is zero in $\mathrm{Cl}_0(\mathfrak{M}')$. Consider the canonical embedding $\iota_0 : \mathrm{Cl}_0(\mathfrak{M}) \to \mathrm{Cl}_0(\mathfrak{M}')$. Using $\mathcal{O}_E = \mathcal{O}_F\mathcal{O}_L$, one sees that $\mathrm{Cl}(\iota_0)$ maps $[\mathfrak{M}\mathcal{O}_L]$ to $[\mathfrak{M}'\mathcal{O}_E]$. Observe now that the algebra inclusion $\mathfrak{M}_0 \to \mathfrak{M}'_0$ is split. (In fact, $\mathfrak{M}_0$ is isomorphic to $\mathcal{O}_F$, and $\mathfrak{M}'_0$ is isomorphic to a product of $l-1$ copies of $\mathcal{O}_F$.) Hence ι_0 is a (split) monomorphism, which finally shows that the class of $\mathfrak{M}\mathcal{O}_L$ is trivial, as we wanted to show. ■

2. Kummer descent (II). In this section we keep the general scenario, this time with $l = 3$, and we now discuss finer criteria, i.e. we are interested in the existence of NIB's, not only WNIB's. To a great extent, we build on the work of Gómez Ayala [3, 4]. We have the following result ([3], Thm. 2.1, [4], Prop. 1.4):

Theorem 2.1 (Gómez Ayala). *Suppose $\zeta = \zeta_3 \in F$ and E/F is a tame cyclic cubic extension. Then E/F has NIB if and only if there exist ideals $\mathfrak{b}, \mathfrak{c}$ in $\mathcal{O}_F$, a generator x of $\mathfrak{b}\mathfrak{c}^2$ with $x \equiv 1 \pmod{3\sqrt{-3}}$, and a generator y of $\mathfrak{c}$ with $y \equiv 1 \pmod 3$ such that with $\alpha^3 = x$ one has the following $\mathcal{O}_F$-basis for $\mathcal{O}_E$:*

$$1,\quad \frac{1-\alpha}{\sqrt{-3}},\quad \frac{1+\alpha+y^{-1}\alpha^2}{3};$$

in this case, the third of these three basis elements also gives a generator of an normal integral basis. Furthermore, $\mathfrak{b}$ and $\mathfrak{c}$ are square-free and coprime.

We shall combine this result with descent theory. Observe first that exactly the divisors of $\mathfrak{b}$ or $\mathfrak{c}$ ramify in E/F; in particular, $\mathfrak{b}$ and $\mathfrak{c}$ are prime to 3. In the notation set up in Section 1, we also have $A_0 = \mathcal{O}_F$ (as always), $A_1 = \alpha\mathcal{O}_F$, $A_2 = y^{-1}\alpha^2\mathcal{O}_F$; consequently, $\mathfrak{A}_1 = \mathfrak{b}\mathfrak{c}^2$ and $\mathfrak{A}_2 = \mathfrak{b}^2\mathfrak{c}$. The last two formulas determine two coprime square-free ideals $\mathfrak{b}$, $\mathfrak{c}$ uniquely, for *any* cyclic cubic tame extension E/F. More precisely, from Lemma 1.2 we know that $\mathfrak{p}$ occurs once in the prime decomposition of $\mathfrak{A}_1$ iff it occurs twice in $\mathfrak{A}_2$ and vice versa; thus $\mathfrak{b}$ is the product of all primes dividing $\mathfrak{A}_1$ exactly once, and $\mathfrak{c}$ is the product of all primes dividing $\mathfrak{A}_1$ exactly twice. We will call $\mathfrak{b}$ and $\mathfrak{c}$ the *characteristic ideals* of the cyclic cubic extension E/F.

Now suppose $F = K(\zeta_3) \neq K$; we want to understand when exactly a tame cubic cyclic extension E/F descends, i.e. can be written $E = LF$ with L/K cyclic cubic (and automatically tame). It is easy and well known that this is the case iff the nontrivial automorphism τ of F/K can be extended to an involutory automorphism, also written τ, of E, the field L then being just the fixed field of τ. Some cases of our next result are already implicit in [4]; see also Greither and Miranda [6].

Theorem 2.2. *Let E/F be a tame cyclic cubic extension with characteristic ideals $\mathfrak{b}$ and $\mathfrak{c}$; let $\alpha \in E^{(1)}$ be an arbitrary Kummer generator, $0 \neq x = \alpha^3 \in F$. Suppose in* (b) *and* (c) *that* 3 *does not ramify in K.*

(a) *The extension E/F descends to K iff $\mathfrak{c} = \mathfrak{b}^\tau$ and there exists $z \in F$ with $z^{2+\tau} = x^{-1}$.*

(b) *If E/F has NIB, and descends to an extension L/K, then the descended extension L/K has NIB, too.*

(c) *If we fix $\mathfrak{b}$ and $\mathfrak{c}$ such that $\mathfrak{c} = \mathfrak{b}^\tau$, then the following two statements are equivalent*: (i) *There exists E/F having characteristic invariants $\mathfrak{b}$ and $\mathfrak{c}$ and satisfying* (a) *and* (b); (ii) *$\mathfrak{c}$ has a generator* $y \equiv 1 \pmod 3$.

Proof. (a) Suppose τ can be extended to an involutory automorphism of E. Since τ interchanges the eigenspaces A_1 and A_2 by virtue of Lemma 1.3, we can write $\tau(\alpha) = z\alpha^2$ with some $z \in F^*$. The property $\tau^2 = \mathrm{id}$ evaluated in α gives the condition $\alpha = \tau(z\alpha^2) = z^{2+\tau}\alpha^4$, or equivalently $z^{2+\tau} = x^{-1}$. If on the other hand this formula holds, setting $\tau(\alpha) = z\alpha^2$ gives a well-defined involutory automorphism extending $\tau \in \mathrm{Gal}(F/K)$.

(b) We take a Kummer generator α as in Theorem 2.1. Then (a) holds for this particular choice, so $x = z^{-2-\tau}$. Recall that $x\mathcal{O}_F = \mathfrak{b}\mathfrak{c}^2 = \mathfrak{c}^{2+\tau}$. From this it follows easily that $z^{-1}\mathcal{O}_F = \mathfrak{c}$. (The endomorphism $2+\tau$ of the ideal group of $\mathcal{O}_F$ is injective, for example because $(2+\tau)(2-\tau) = 3$.)

Sublemma. *For $u \in \mathcal{O}_F$ we have*:

$$u \equiv 1 \pmod 3 \Leftrightarrow u^{2+\tau} \equiv 1 \pmod{3\sqrt{-3}}.$$

Proof. Note first that $a^\tau \equiv a \pmod{\sqrt{-3}}$ for all $a \in \mathcal{O}_F$, and $\tau(\sqrt{-3}) = -\sqrt{-3}$. Suppose $u = 1 + 3a$. Then $u^{2+\tau} \equiv 1 + 3(2a + a^\tau) \pmod{3\sqrt{-3}}$, and $2a + a^\tau \equiv 3a \equiv 0 \pmod{\sqrt{-3}}$, which gives one implication. For the other, let $v = u^{2+\tau} = 1 + 3\sqrt{-3}b$. Then $u^3 = v^{2-\tau} \equiv 1 + 3\sqrt{-3}(2b + b^\tau) \equiv 1 \pmod 9$. The implication $u^3 \equiv 1 \pmod 9 \Rightarrow u \equiv 1 \pmod 3$ is well known.

Back to the proof of (b): Since we chose α according to Theorem 2.1, we know that $x = \alpha^3$ is congruent to 1 modulo $3\sqrt{-3}$, and now the sublemma tells us that $z^{-1} \equiv 1 \pmod 3$. We may therefore replace y by z^{-1} in the basis element $\frac{1}{3}(1 + \alpha + y^{-1}\alpha^2)$ in Theorem 2.1, so we obtain the following generator of an normal integral basis for E/F:

$$T = \tfrac{1}{3}(1 + \alpha + z\alpha^2).$$

One checks immediately that $\tau(T) = T$; therefore $T \in \mathcal{O}_L$, and T also generates an normal integral basis of L/K, just by faithfully flat descent and since $\mathcal{O}_E = \mathcal{O}_F\mathcal{O}_L$.

(c) We have already seen in the sublemma that (a) and (b) imply condition (ii). Conversely, if $y \equiv 1 \pmod 3$ generates $\mathfrak{c}$, define $x = y^{2+\tau}$. Again by the sublemma, $x \equiv 1 \pmod{3\sqrt{-3}}$, and the extension $E = K(\sqrt[3]{x})$ has all the required properties. ∎

Remark 2.3. The preceding theorem is particularly useful if h_F is prime to three. For in this case, the characteristic ideals determine E/F uniquely. This can be seen as follows: Two extensions E and E' with the same characteristic ideals give rise to two elements x and x' of $\mathcal{O}_F$, generating the same ideal, and congruent modulo $3\sqrt{-3}$. The quotient $u = x/x'$ would therefore be a unit congruent 1 modulo $3\sqrt{-3}$, so $F(\sqrt[3]{u})$ would be cyclic cubic and unramified over F unless u is already a cube, but in that case E equals E'. Moreover, we do not have to worry about the order in which we write the two characteristic ideals: changing the roles of $\mathfrak{b}$ and $\mathfrak{c}$ just amounts to replacing the original choice of the generator σ by σ^2, and the extension E/F just considered as a field (without fixing the G-action) does not change.

Corollary 2.4. *Suppose K is imaginary quadratic, $d_K \neq -3$ and 3 does not divide h_F. Let $\mathfrak{p}$ be a prime of K such that $3 \mid \mathrm{N}(\mathfrak{p}) - 1$. Then $K(\mathfrak{p})$ contains exactly one cubic subfield L, and L/K has an NIB iff the primes $\mathfrak{P}_1$, $\mathfrak{P}_2$ over $\mathfrak{p}$ in F are principal with generator congruent to 1 modulo 3.*

Proof. If L/K has NIB, then so has E/F. By looking at the ramification we see that the characteristic ideals of E/F are $\mathfrak{P}_1$ and $\mathfrak{P}_2$ for some numbering. Furthermore E/F descends, so by Theorem 2.2(c), $\mathfrak{P}_2$ has a generator $\equiv 1 \pmod 3$. If conversely $\mathfrak{P}_2$ has a generator $\equiv 1 \pmod 3$, then there exists by Theorem 2.2(c) some E'/F which descends to L'/K with NIB, and which has the right characteristic ideals. By Remark 2.3, the compositum $E = FL$ is the unique tame cyclic cubic extension of F with characteristic ideals $\mathfrak{b} = \mathfrak{P}_1$ and $\mathfrak{c} = \mathfrak{P}_2$. Therefore $E' = E$ and $L' = L$, which shows what we want. ∎

3. Applications I: Ray class fields without WNIB.

Let $K = \mathbb{Q}(\sqrt{-d})$, $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Let $3 < l \equiv 3 \pmod 4$ be a fixed prime. We are interested in finding primes $\mathfrak{p}$ of K with l dividing $\mathrm{N}(\mathfrak{p}) - 1$ such that the unique subfield L of degree l of the ray class field $K(\mathfrak{p})$ does not have WNIB over K. Note two things: first, L exists and is unique by global class field theory; second, $K(\mathfrak{p})$ will not have WNIB over K either if L does not. We impose the mild restriction that $\mathfrak{p}$ and l are unramified in $K/\mathbb{Q}$.

Let p be the rational prime over which $\mathfrak{p}$ lies. We have seen in Section 1 that $\mathfrak{p}$ is totally split in $F = K(\zeta_l)$, whether p is inert or split in K. Note, however, that the case p inert, $p \equiv +1 \pmod l$ is uninteresting since then

L is equal to the composite of K with the unique degree l subfield of $\mathbb{Q}(\zeta_p)$, so it certainly admits NIB. Let us therefore assume henceforward: If p is inert in K, then $p \equiv -1 \pmod{l}$. (In the case p split in K, we only have the one possibility $p \equiv 1 \pmod{l}$.)

Write $\mathrm{Gal}(F/K) = \Delta = \{\sigma_1, \ldots, \sigma_{l-1}\}$ and $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_{l-1}$ as in Section 1. Recall that J is the Stickelberger ideal in $\mathbb{Z}\Delta$. By Theorem 1.6 we have the criterion:

If the class $[\mathfrak{P}_1] \in \mathrm{Cl}(\mathcal{O}_F)$ *is not annihilated by* J, *then* L, *and consequently* $K(\mathfrak{p})$, *does not have a weak normal integral basis over* K.

Before embarking on calculations, we discuss some technical reduction steps which make it easy to use this criterion. Let $C_3(M)$ be the 3-primary part of $\mathrm{Cl}(M)$ for any number field M. Denote the projection of $[\mathfrak{A}] \in \mathrm{Cl}(M)$ to $C_3(M)$ by $[\mathfrak{A}]_3$. The automorphism $j = \sigma_{-1}$ acts semi-simply on $C_3(F)$, and $C_3(F) = C_3^+(F) \oplus C_3^-(F)$, where j acts as ± 1 on $C_3^{\pm}(F)$. The following is motivated by the well-known principle that "the Stickelberger ideal lives mainly in the minus part". Denote the projection of $[\mathfrak{A}]_3 \in C_3(F)$ to $C_3^-(F)$ by $[\mathfrak{A}]_3^-$. The abelian group $C_3^-(F)$ is in a canonical way a module over $\mathbb{Z}_3\Delta$, and also over the minus quotient $(\mathbb{Z}_3\Delta)_- = \mathbb{Z}_3\Delta/(1+j)$. We then have an obvious lemma:

Lemma 3.1. *If* $[\mathfrak{P}_1]_3^- \in C_3^-(F)$ *is nontrivial*, *and if the image of* $\mathbb{Z}_3 \otimes_{\mathbb{Z}} J$ *in* $(\mathbb{Z}_3\Delta)_-$ *is the unit ideal*, *then* $[\mathfrak{P}_1] \in \mathrm{Cl}(F)$ *is not annihilated by* J.

The point of this lemma is that we have an easy handle on the Stickelberger ideal in the minus quotient of the 3-completion. By Theorem 6.2 in [10], the image of $\mathbb{Z}_3 \otimes_{\mathbb{Z}} J$ in $(\mathbb{Z}_3\Delta)_-$ is all of $(\mathbb{Z}_3\Delta)_-$ iff 3 does not divide $h_l^- = h^-(\mathbb{Q}(\zeta_l))$. (Comment: In using this result, we have identified $(\mathbb{Z}_3\Delta)_-$ with $(\mathbb{Z}_3\Delta)^-$, and the image of $\mathbb{Z}_3 \otimes_{\mathbb{Z}} J$ with $\mathbb{Z}_3 \otimes_{\mathbb{Z}} J^-$. We are working 3-adically, not 2-adically, just in order to be able to make these canonical identifications.)

We can give a still simpler criterion for the first condition in Lemma 3.1 to hold, using quadratic fields. Observe that p splits in $F_0 = \mathbb{Q}(\sqrt{ld})$. (Distinguish the two cases p inert/split in K and correspondingly $p \equiv +1/-1 \pmod{l}$.) Let $p\mathcal{O}_{F_0} = \mathfrak{q}\mathfrak{q}'$.

Proposition 3.2. *Keep the notation of Lemma* 3.1 *and suppose that the order of* $[\mathfrak{q}]$ *in* $\mathrm{Cl}(F_0)$ *is divisible by* 3. *Then*

(a) $x = [\mathfrak{P}_1]_3^-$ *is nontrivial in* $C_3^-(F)$.

(b) *Let* $\Delta^+ = \mathrm{Gal}(F/K(\sqrt{-l}))$. *Then* $\Delta^+ = \left\{\sigma_i : 0 < i < l, \left(\frac{i}{l}\right) = +1\right\}$. *Let* $\nu = \sum_{\sigma \in \Delta^+} \sigma$. *Then* x^ν *is nontrivial in* $C_3^-(F)$ *provided* l *is not congruent to* 1 *modulo* 3.

Proof. (a) The norm map N from $\mathrm{Cl}(F)$ to $\mathrm{Cl}(F_0)$ induces first of all a homomorphism $\mathrm{N}_3 : C_3(F) \to C_3(F_0)$. Since j induces the *nontrivial* automorphism τ of $F_0/\mathbb{Q}$, and since τ acts as -1 on $C_3(F_0)$, it follows that for any $[\mathfrak{A}]_3 \in C_3(F)$, the images of $[\mathfrak{A}]_3$ and $[\mathfrak{A}]_3^-$ under N_3 are the same. Furthermore, $\mathrm{N}([\mathfrak{P}_1])$ gives (up to exchanging $\mathfrak{q}$ with $\mathfrak{q}'$) either $[\mathfrak{q}]$ or its square, depending on whether p is split or inert in K. Thus, $\mathrm{N}_3([\mathfrak{P}_1]_3^-)$ gives $[\mathfrak{q}]_3$ or the square of this; by hypothesis, these are nonzero elements of $C_3(F_0)$, and part (a) of the proposition follows.

(b) The operator ν acts invertibly (more precisely: as multiplication by $(l-1)/2$) on $C_3(F_0)$ since $l-1$ is coprime to 3. Thus the proof goes through as in (a) after replacing x by x^ν and $[\mathfrak{q}]$ by $[\mathfrak{q}]^\nu$; the point is that the latter is still nontrivial. ■

Now we can state:

Theorem 3.3. *Let K and l be as above, and p a prime with either $p \equiv 1 \pmod{l}$ and p split in K, or $p \equiv -1 \pmod{l}$ and p inert in K. Suppose that*:

(i) *the classes of the primes over p in $\mathrm{Cl}(\mathbb{Q}(\sqrt{ld}))$ have order divisible by three*; *and*

(ii) *either* 3 *does not divide h_l^-, or $l \equiv 2 \pmod 3$ and* 3 *does not divide $h(-l)$.* (*Here $h(-l)$ denotes the class number of $\mathbb{Q}(\sqrt{-l})$. Note that "*3 *does not divide h_l^-" implies "*3 *does not divide $h(-l)$", which means that we get by with a weaker hypothesis in the case $l \equiv 2 \pmod 3$.*)

Then $K(\mathfrak{p})$ does not even have WNIB over K, where $\mathfrak{p}$ is any prime over p in K.

Proof. If the first clause in (ii) holds, then we get the conclusion immediately on combining Lemma 3.1, Proposition 3.2(a), and the criterion stated at the beginning of the section. If we only know that 3 does not divide $h(-l)$ and we are in the case $l \equiv 2 \pmod 3$, a little argument is needed. By the criterion it suffices to show $Jx \neq 0$ (we switch to additive notation); we know $\nu x \neq 0$ by Proposition 3.2(b). Therefore if we can show that $\nu \cdot (\mathbb{Z}_3 \otimes_{\mathbb{Z}} J)_-$ equals $\nu \cdot (\mathbb{Z}_3 \Delta)_-$, we are done. This will be established with the help of the following claim:

$$\nu\theta = l^{-1}\nu(R + N\sigma_{-1}),$$

where R (resp. N) is the sum of all quadratic residues (resp. nonresidues) modulo l among $1, \ldots, l-1$. Proof of this claim: Let P (resp. Q) denote the set of residues (nonresidues) modulo l among $\{1, \ldots, l-1\}$. Then $l\theta = \sum_{a\in P} a\sigma_a^{-1} + \sum_{a\in Q} a\sigma_a^{-1}$. Observe now that $ai \in P \Leftrightarrow \sigma_a \in = \Delta^+$, and that $a \in Q \Leftrightarrow \sigma_a \in \sigma_{-1}\Delta^+$. Thus, $\nu l\theta = \sum_{a\in P} a\nu + \sum_{a\in Q} a\nu\sigma_{-1} = \nu(R + N\sigma_{-1})$.

From the claim we obtain $(\nu\theta)_- = \nu \cdot (R-N)/l$, and it is well known that $(R-N)/l = h(-l)$, so $(R-N)/l$ is a 3-adic unit if 3 does not divide $h(-l)$. ■

The following examples in which the hypotheses of the preceding theorem are all satisfied were obtained using some tables and the number theory program system PARI. One thing is clear: If we have *one* example (K, l, p_0) with (i) and (ii), then there will be infinitely many values p which work instead of p_0. Reason: By the generalized Dirichlet theorem, one finds infinitely many p such that $\mathfrak{q}$ (a degree one prime over p in $\mathbb{Q}(\sqrt{ld})$) is in the same class as $\mathfrak{q}_0$ (a degree one prime over p_0); this assures (i), and (ii) does not depend on p at all. Therefore the point is to find values of l for given K; it is nice but quite unessential to have a long list of values p for given K and l.

The procedure is obvious: we fix $d \in D$ and find primes $l \equiv 3 \pmod 4$ such that $3 \mid h(\mathbb{Q}(\sqrt{ld}))$, i.e. there *exist* primes p satisfying (i); one finds such values p just by exhaustive search up to some arbitrary limit; before doing so, one makes sure there is no "obstacle", i.e. (ii) is satisfied. This happened rarely in our calculations. However, for $l \geq 521$ (that is, l is not covered by the table of Lehmer and Masley) and $l \equiv 1 \pmod 3$ one has to work a bit. Of course we did not calculate the number h_l^-, we just wrote a program to check whether $h_l^- \equiv 0 \pmod 3$, using the Stickelberger element modulo 3.

We begin with $d = 11$ because this was the case we considered first, and where we calculated most. In the leftmost column of Table 1, we give all primes $l < 1100$ with $l \equiv 3 \pmod 4$ such that 3 divides $h(11 \cdot l)$. The second column tells whether condition (ii) holds or not. The final column contains all the values of p satisfying (i), inert in K, $p \equiv -1 \pmod{11}$, up to the limit 10000 (first row), 25000 (second row), and 50000 (all other rows). As indicated above, it is easy to find many more p; we did some tests to see whether the density of p which work was close to the density predicted by Dirichlet, and indeed it was.

It is gratefully acknowledged here that the main tool in the calculation, apart from some class number tables, was the number theory package PARI, developed by H. Cohen and collaborators at Bordeaux.

Table 1

l	(ii)?	Values of p inert in K satisfying (i)
43	yes	601, 1117, 1289, 2837, 3181, 4127, 4729, 8513, 8599
191	yes	10313, 17189, 20627, 21391
271	yes	36313, 37397, 39023
619	yes	22283, 30949, 40853, 48281
647	yes	15527, 21997, 29761, 42701, 45289
659	yes	30313, 34267
691	yes	1381, 8291, 12437, 42841
743	no	—
1091	yes	4303, 10909, 24001, 45821

This example is typical, so we will be brief about the other seven values of $d \neq 3$, and the cases where p splits in K. Sticking with the case p inert for a moment, we give Table 2, where the second column contains the *first* value of l satisfying (ii) and "3 divides $h(\mathbb{Q}(\sqrt{ld}))$"; the third column contains some values of p (inert in K) satisfying (i).

Table 2

d	First l	p inert in $K = \mathbb{Q}(\sqrt{-d})$ satisfying (i)
1	79	631, 947, 1579
2	71	709
7	67	937
19	103	4943, 7621
43	11	131
67	7	41
163	167	2671

Note the rather small numbers in the example $(d, l, p) = (67, 7, 41)$. So we are saying here that the abelian extension of $K = \mathbb{Q}(\sqrt{-67})$ with degree 7 and conductor 41 does not have WNIB.

In the same way one obtains values p which are split in K and satisfy (ii) starting with one of the eight values $d \in D$, $d \neq 3$, and a value l already obtained for d. We just give a few values:

Table 3

d	First l	p split in $K = \mathbb{Q}(\sqrt{-d})$ satisfying (i)
11	43	947, 1549, 1727
43	11	23, 67
67	7	29, 71

Thus we obtain two more examples with fairly small numbers: $(d, l, p) = (43, 11, 23)$ or $(67, 7, 29)$. Let us remark that the value $l = 7$ is in the present approach the lowest you can hope for, since 5 is not congruent 3 mod 4, and $l = 3$ will not work, see Section 4. This does not at all exclude the existence of quintic examples, but a different approach would be needed.

As the reader has noticed, we have been excluding $d = 3$. This has a very good reason: Using Scholz' theorem, one can show that $3 \mid h(3l)$ implies $3 \mid h(-l)$ and hence $3 \mid h_l^-$, so (ii) will always be violated. The solution here is to do the same as in a famous recent paper by A. Wiles: we replace 3 by 5 consistently in Lemma 3.1 and Proposition 3.2. One finds the prime $l = 547$ with the property $5 \mid h(3 \cdot 547)$, and 5 does not divide h_{547}^-; furthermore the prime $p = 13127$ has the property that the order of the classes above p in $\mathbb{Q}(\sqrt{3 \cdot 547})$ is a multiple of (in fact, equal to) 5. Exactly as in 3.1–3.3, one shows that this implies: The degree 547 subfield of $K(13127)$ has no WNIB over $K=\mathbb{Q}(\sqrt{-3})$. Again, there are infinitely many other values of p.

The natural question arises: Given d, are there infinitely many values of l which work? This should be true, but it seems very hard to prove. In fact, there is a close link with the Cohen–Lenstra heuristics, but if we insist on including the case $l\equiv 1 \pmod 3$, the situation is worse here since we also need a nondivisibility statement for minus class numbers of full cyclotomic fields, not quadratic fields. (We already mentioned that if 3 divides $h(-l)$, then it divides h_l^-; the converse is not true, the smallest example being $l=131$, but such instances of l seem to be relatively rare. In fact, we checked all primes $l\equiv 3 \pmod 4$, $l<5500$, and we found only six such cases, and there are 133 values l in this interval with $3\mid h(-l)$.) We were led to the following speculative hypothesis: When $p\to\infty$ (always p inert in K), then the probability that $K(p)/K$ has WNIB should actually converge to 0. However, the convergence to 0 should be so slow that it is quite out of the question to test this guess by numerical experiments.

How did we arrive at this hypothesis? For $p\to\infty$, the number of prime divisors $l\equiv 3 \pmod 4$ of $p+1$ should also go to infinity, perhaps like $\log\log p$. For any $l\mid p+1$ one can ask whether Theorem 3.3 applies or not to disprove WNIB for $K(p)/K$. If one is willing to accept that Theorem 3.3 applies with a certain positive probability c (the more sceptical reader should perhaps impose the extra condition $l\equiv 2 \pmod 3$), and also that the prime divisors $l\equiv 3 \pmod 4$ of $p+1$ are "random", then one is led to the above speculative hypothesis.

4. Applications II: The cubic case. In this section we will be concerned with integral normal bases in the original sense, not in the weak sense. Gómez Ayala proved in [4] that $K(2)/K$ does have a NIB for the five fields $K=\mathbb{Q}(\sqrt{-d})$, $d\in D$, for which $K(2)/K$ is cubic and tame. We are going to generalize this and try to understand the underlying principle.

Note first of all: Any tame cubic extension of $K=\mathbb{Q}(\sqrt{-d})$, $d\in D$, has a WNIB, since the maximal order in $K[\mathbb{Z}/3]$ is $\mathcal{O}_K\times\mathcal{O}_F$ with $F=K(\zeta_3)$, and one checks that for all nine values of d, the field F has class number one. What might therefore happen is that a tame cubic extension of K has WNIB but no NIB, and we shall see that this does occur.

In the sequel we *exclude* $d=3$, since we know thanks to [3], 2.14, that all tame cubic extensions of $\mathbb{Q}(\sqrt{-3})$ have NIB.

Now let $\mathfrak{p}$ be a prime of K whose norm is 1 modulo 3, and L the cubic subfield of $K(\mathfrak{p})$. Let p be the rational prime under $\mathfrak{p}$. If p splits in K, then $p\equiv 1 \pmod 3$. If p is inert, then $p\equiv \pm1 \pmod 3$, but in the case $p\equiv +1 \pmod 3$ we know that L/K has NIB (see beginning of Section 3), so we exclude this case. In any case we have $\mathfrak{p}\mathcal{O}_F=\mathfrak{P}_1\mathfrak{P}_2$. For any integral ideal $\mathfrak{A}$ of F, let $S(\mathfrak{A})$ be the ray class group modulo $\mathfrak{A}$, that is, $S(\mathfrak{A}) = (\mathcal{O}_F/\mathfrak{A})^*/\mathrm{Im}(\mathcal{O}_F^*)$. This is the correct definition since $h_F = 1$. Every ideal $\mathfrak{b}$ of F gives an element of $S(\mathfrak{A})$, to wit, the class of some (and therefore any) generator of $\mathfrak{b}$. Corollary 2.4 tells us:

L/K has NIB iff the class of $\mathfrak{P}_1$ in $S(3)$ is trivial.

We will exploit this criterion now.

LEMMA 4.1. *The canonical epimorphism $S(3) \to S(\sqrt{-3})$ is an isomorphism, and $S(\sqrt{-3})$ is trivial if 3 splits in K, and of order two with $1+\sqrt{-d}$ representing the nontrivial element if 3 is inert in K.*

Proof. For the first statement one has to show that if $a \in \mathcal{O}_F$, then there exists a unit $u \in \mathcal{O}_F$ with $u \equiv 1+a\sqrt{-3} \pmod 3$. There are 9 residue classes $1+a\sqrt{-3}$ modulo $3\mathcal{O}_F$. Let $\varepsilon = \eta^4$, where η is the fundamental unit of F. (For $d \geq 11$, see [4], p. 378; for $d = 1, 2, 7$ we have $\eta = 2 + i\sqrt{-3}$, $5 + 2\sqrt{-2}\sqrt{-3}$, and $\frac{1}{2}(5 + \sqrt{-7}\sqrt{-3})$ respectively.) Modulo 3, one has $\varepsilon = 1 + b\sqrt{-d}\sqrt{-3}$ with $b \in \mathbb{Z}$ and $b \equiv \pm 1 \pmod 3$ in all cases. This shows that the nine units $\varepsilon^r\zeta_3^s$ $(0 \leq r, s < 3)$ are all different mod $3\mathcal{O}_F$, and all of the form $1 + a\sqrt{-3}$, so we are done.

The group $S(\sqrt{-3})$ equals $(\mathbb{F}_3^* \times \mathbb{F}_3^*)/\langle -1, \overline{\eta}\rangle$ if 3 splits, and it equals $\mathbb{F}_9^*/\langle -1, \overline{\eta}\rangle$ if 3 is inert in K. In the first case one sees that the image $\overline{\eta}$ of η is $\pm(+1, -1)$, so $S(\sqrt{-3})$ is trivial. In the other case, $\overline{\eta}$ is the class of $\pm\sqrt{-d}$, an element of order 4 in $\mathbb{F}_9^* = (\mathcal{O}_F/(\sqrt{-3}))^*$, and the class of $1 + \sqrt{-d}$ is a generator of $\mathbb{F}_9^*$. This proves the lemma. ■

COROLLARY 4.2. *If $d = 2$ or $d = 11$, then L, the cubic subfield of $K(\mathfrak{p})$, always has NIB.*

Proof. By Lemma 4.1 we clearly have that $S(3)$ is trivial. Apply the criterion stated just above. ■

PROPOSITION 4.3. *If p is inert in K, i.e. $\mathfrak{p} = p\mathcal{O}_F$, then L/K always has NIB.* (*Note that this gives the result of* [4] *when one sets $p = 2$.*)

Proof. As said earlier, we may assume $p \equiv -1 \pmod 3$. Thus, $\mathfrak{P}_1$ is induced from an ideal of the real quadratic field $F_0 = \mathbb{Q}(\sqrt{3d})$, because p splits already in that field. Hence $\mathfrak{P}_1$ has a generator of the form $y = \frac{1}{2}(a + b\sqrt{-d}\sqrt{-3})$ with $a, b \in \mathbb{Z}$ (the factor $\frac{1}{2}$ being needed only in case $3d \equiv 1 \pmod 4$), and obviously a is prime to 3. In other words, $y \equiv \pm 1 \pmod{\sqrt{-3}}$, so the class of $\mathfrak{P}_1$ in $S(\sqrt{-3})$ is trivial. By Lemma 4.1, and our criterion, the proposition follows. ■

The only case which remains is: 3 is inert in K, and p is split in K, hence totally split in F. Here the situation is different:

Proposition 4.4. *Under the conditions just stated*, *let*

$$P = \{\mathfrak{p} \text{ prime in } K \text{ of degree } 1 \text{ with } N(\mathfrak{p}) \equiv 1 \pmod 3\};$$

$L^{(\mathfrak{p})}$ *the cubic subfield of* $K(\mathfrak{p})$; $P^+ = \{\mathfrak{p} \in P : L^{(\mathfrak{p})}$ *has NIB over* $K\}$, *and finally* $P^- = P \setminus P^+$. *Then* P^+ *and* P^- *have the same Dirichlet density* (*equal to* $1/4$). *In particular*, *both sets are infinite.*

Proof. We know that P is exactly the set of degree one primes which split in F/K. Thus, the norm defines a 2-to-1 map $P' \to P$, where P' is the set of degree one primes in F. If $\mathfrak{P}$ goes to $\mathfrak{p} \in P$, then $\mathfrak{p}$ is in P^+ iff $\mathfrak{P}$ gives the trivial element of the ray class group $S(3)$, by our criterion. By Lemma 4.1 and the generalized Dirichlet theorem, the proposition follows. ∎

Example. Let $d = 19$. If we take $\mathfrak{P} = z\mathcal{O}_F$, with

$$z = \frac{1}{4}((-5 + \sqrt{-19}) + (3 + \sqrt{-19})\sqrt{-3}),$$

then $\mathfrak{p} = \mathrm{N}_{F/K}\mathfrak{P}$ is a prime in K with norm 7, and $\mathfrak{P}$ represents the nontrivial class in $S(3)$ since $z \equiv 1 + \sqrt{-19}$ modulo $\sqrt{-3}$. Thus, $\mathfrak{p}$ belongs to P^-. On the other hand, if we replace z by $\sqrt{-19} + (7 + \sqrt{-19})\sqrt{-3}$, then $\mathfrak{p}$ is this time a prime with norm 38557, and it belongs to P^+.

References

[1] P. Cassou-Noguès and M. Taylor, *Elliptic Functions and Rings of Integers*, Progr. Math. 66, Birkhäuser, 1986.

[2] L. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. 35 (1995), 407–422.

[3] E. J. Gómez Ayala, *Bases normales d'entiers dans les extensions de Kummer de degré premier*, J. Théor. Nombres Bordeaux 6 (1994), 95–116.

[4] —, *Structure galoisienne et corps de classes de rayon de conducteur* 2, Acta Arith. 72 (1995), 375–383.

[5] E. J. Gómez Ayala und R. Schertz, *Eine Bemerkung zur Galoismodulstruktur in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, J. Number Theory 44 (1993), 41–46.

[6] C. Greither and R. Miranda, *Galois extensions of prime degree*, J. Algebra 124 (1989), 354–366.

[7] L. McCulloh, *A Stickelberger condition on Galois module structure for Kummer extensions of prime degree*, in: Algebraic Number Fields (Durham Proceedings), A. Fröhlich (ed.), Academic Press, London, 1977, 561–588.

[8] —, *Galois module structure of elementary abelian extensions*, J. Algebra 82 (1983), 102–134.

[9] R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory 39 (1991), 285–326.

[10] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, 1982.

Département de Mathématiques et de Statistique
Université Laval et CICMA
Ste-Foy, P.Q.
Canada G1K 7P4
E-mail: greither@mat.ulaval.ca

Received on 9.2.1996 (2920)