Relative ideal classes of arbitrary order

David L. Pincus · Lawrence C. Washington

Received: 28 December 2022 / Accepted: 11 February 2023 / Published online: 21 March 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
We adapt a technique for searching for ideal classes of arbitrary order and apply it to three families of number fields. We show that a family of cyclic sextic number fields has infinitely many fields in it that contain a relative ideal class of order $r$, where $r$ is a positive integer relatively prime to the degree of the extension. We then show that the same holds true for a family of cyclic quartic number fields. Though the technique is traditionally applied to Galois extensions, we show how it may be adapted to handle a family of non-Galois cubic number fields and prove that this family contains infinitely many fields with an ideal class of arbitrary order relatively prime to three.

Keywords   Ideal class group · Relative ideal class · Sextic field · Quartic field · Cubic field

Mathematics Subject Classification Primary 11R29; Secondary 11R16

1 Introduction

Let $\mathcal{F} := \{K_n\}$ denote an indexed family of number fields and let $r$ be a positive integer. Let $\mathcal{I}_{K_n}$ denote the group of fractional ideals of $K_n \in \mathcal{F}$. Can we find a field $K_n \in \mathcal{F}$ that contains an ideal class of order $r$? We may answer in the affirmative if the following criteria are satisfied.

1. We can find an index $n$ and a principal ideal $w\mathcal{O}_{K_n} \in \mathcal{I}_{K_n}$ that factors as $w\mathcal{O}_{K_n} = J^r$ for some fractional ideal $J \in \mathcal{I}_{K_n}$.
2. We can show that no smaller power of $J$ is principal.

This sort of approach has been used by authors going back at least as far as Nagell [8].
A method for meeting Criterion (1) begins by looking for solutions to the equation

\[ Y^r = f_n(X), \quad (1.1) \]

where \( f_n(X) \in \mathbb{Z}[X] \) is the minimal polynomial of a primitive element for \( K_n/\mathbb{Q} \). Indeed if \( K_n/\mathbb{Q} \) is Galois with primitive element \( \rho \), then a solution \((x, y) \in \mathbb{Z}^2\) to Eq. (1.1) gives

\[ y^r = f_n(x) = \prod_{i=0}^{[K:\mathbb{Q}]-1} (x - \rho_i), \quad (1.2) \]

where the \( \rho_i \) run over the Galois conjugates of \( \rho := \rho_0 \). If one can show that the exact power of a prime ideal that divides, say, \((x - \rho_i)\mathcal{O}_K\) is also the exact power of the same prime ideal that divides \( y^r\mathcal{O}_K \), then one may conclude that \((x - \rho_i)\mathcal{O}_{K_n} = J^r\) for some ideal \( J \in \mathcal{I}_{K_n} \).

A method for meeting Criterion 2 is then to assume the contrary and suppose that \((x - \rho_i)\mathcal{O}_{K_n}\) is the \( p \)th power of a principal ideal, where \( p \) is a prime dividing \( r \). Element-wise this implies that there is a \( z \in K_n^\times \) and a unit \( u \in \mathcal{O}_{K_n}^\times \) such that

\[ x - \rho_i = u z^p. \quad (1.3) \]

By restricting our consideration to those solutions \((x, y) \in \mathbb{Z}^2\) that have the property that, for each prime divisor \( p \) of \( r \), the prime divisors of \( y \) satisfy certain \( p \)th power residue conditions, we can ensure that for each prime \( p \mid r \), Eq. (1.3) fails to hold.

Our focus in this paper is not on the examples themselves per se, but rather on the technique just introduced. This technique is constructive in the sense that it proves the existence of a field \( K_n \in \mathcal{F} \) with class number divisible by \( r \) by providing a recipe for producing an ideal class of order \( r \). If we were solely concerned with producing such an ideal class, then we could simply apply the general technique to the proper subfields of the fields in \( \mathcal{F} \). Our interest, however, is in constructing ideal classes that are ‘new’ in the sense that they have trivial norm down to each proper subfield. Thus the recipe that we provide in this paper produces ideal classes of order \( r \) whose representatives are not obtained from ideal classes of a proper subfield. This involves extra complications, for example the use of Hilbert’s Irreducibility Theorem [5].

In somewhat more detail we extend the general technique outlined prior to the preceding paragraph in the following three ways.

A. If several of the (ideal) factors \((x - \rho_i)\mathcal{O}_{K_n}\) on the right hand side of Eq. (1.2) factor as \( r \)th powers of ideals, then do so products and quotients of these ideals. By taking appropriate products and quotients of such factors, we may obtain a principal ideal that has trivial norm down to each proper subfield of \( K_n \) and which also factors as an \( r \)th power, say as \( J^r \). The ideal class of \( J \) then has trivial norm down to each proper subfield of \( K_n \) and is called a relative ideal class. We use this technique in Sect. 2 (resp. Sect. 3) below to search for relative ideal classes of order \( r \) in a family of sextic (resp. quartic) number fields. The qualifier relative is important. Had we simply been interested in searching for ideal classes of order \( r \), then it would have sufficed to look for a principal fractional ideal belonging to any of the proper subfields of \( K_n \) that factors as an \( r \)th power. The fact that the ideal classes we detect are relative ideal
Relative ideal classes of arbitrary order 821

B. If $K_n/\mathbb{Q}$ is non-Galois with primitive element $\rho \in \mathcal{O}_{K_n}$ and $(x, y) \in \mathbb{Z}^2$ is such that $y^r = f_n(x)$, then Eq. (1.2) no longer holds in $K_n$. It is still true, however, that for each prime ideal $\mathfrak{P}$ dividing $(x - \rho)|\mathcal{O}_{K_n}$, we have $q(x) \not\equiv 0 \mod \mathfrak{P}$, then we still have that $(x - \rho)|\mathcal{O}_{K_n} = J^r$ for some ideal $J \in \mathcal{I}_{K_n}$. We use this technique in Sect. 4 to search for ideal classes of order $r$ in a family of non-Galois cubic number fields.

C. Congruence conditions are not always sufficient to guarantee that for each prime $p$ dividing $r$, $(x - \rho)/u$ doesn’t have a $p$th root in $K_n$. Likewise, congruence conditions don’t always suffice to guarantee that for each prime $p \mid r$, there is no $p$th root of $w/u$ in $K_n$, where $w$ is a product of powers of the $(x - \rho)$. What the congruences can do, however, is limit the possibilities for $u \in \mathcal{O}_{K_n}^\times$. Eliminating the possibility that there is a prime $p \mid r$ such that $w/u$ has a $p$th root in $K_n$ can then be reduced to showing that the polynomial $\varphi(x^r)$ is irreducible in $\mathbb{Q}[X]$, where $\varphi(X) \in \mathbb{Q}[X]$ is the minimal polynomial of $w/u$. Since $\varphi(x^r)$ depends on both $r$ and the parameter $n$ indexing our families of number fields, proving irreducibility is not easy. In Sects. 2 and 3 we make use of Hilbert’s Irreducibility Theorem [5] to do so.

Using these techniques we show that each of the families mentioned above has infinitely many fields that contain an ideal class of order $r$. In the case of the sextic and quartic families, these are relative ideal classes. In all cases $r$ is a positive integer relatively prime to the degree of the extension, but otherwise arbitrary. Although the methods we employ may be extended to handle some cases where $(r, [K : \mathbb{Q}]) > 1$, we have been unable to obtain complete results. Thus our presentation sticks to the case $(r, [K : \mathbb{Q}]) = 1$. We could use genus theory to produce relative classes of order 3 in the sextic case, for example. But this method does not work as well when a higher power of 3 divides $r$.

The three families we study were chosen because they have explicit relative units. The Brauer–Siegel theorem tells us to expect large class numbers, but the above techniques are needed to obtain arithmetic properties rather than just information about the magnitude. Of course, knowledge of the units is vital when proving an ideal is non-principal. It is interesting to note that for both the sextic and the quartic fields we consider, we do not have explicit expressions for the fundamental units of the quadratic subfields, and this information is not needed for obtaining the desired relative ideal classes.

2 A family of sextic number fields

Let $n \in \mathbb{Z} \setminus \{0, \pm 6, \pm 26\}$ and let $K_n = \mathbb{Q}(\rho)$, where $\rho$ is a root of

$$f_n(X) := X^6 - \left(\frac{n - 6}{2}\right) X^5 - 5 \left(\frac{n + 6}{4}\right) X^4$$

$$- 20 X^3 + 5 \left(\frac{n - 6}{4}\right) X^2 + \left(\frac{n + 6}{2}\right) X + 1.$$  \hfill (2.1)
**Theorem 2.1** Let $r > 0$ be an integer with $(6, r) = 1$. There are infinitely many fields $K_n$ containing a relative ideal class of order $r$.

It is clear that $K_n = K_{-n}$, since the zeros of $\varphi_n(X)$ serve as primitive elements for $K_n/\mathbb{Q}$ and since $\varphi_n(X) = \varphi_{-n}(X)$. As we make no additional assumptions regarding the injectivity of the parametrization of $\mathcal{J}$ given by $n \mapsto K_n$, it would be insufficient for us to show that there are infinitely many $n$ for which $K_n$ contains a relative ideal class of order $r$. Instead we put most of our effort into first proving

**Proposition 2.2** Let $r > 0$ be an integer with $(6, r) = 1$ and let $q \in \mathbb{Z}$ be a prime such that

$$P(X) := (X^r + 143 - 30\sqrt{108})(X^r + 143 + 30\sqrt{108}) \in \mathbb{Z}[X],$$

splits into linear factors $\pmod{q}$. Assume that $q \nmid 210r$. There is a field $K \in \mathcal{J}$ that satisfies the following three conditions:

(i) There is an ideal $J \in \mathcal{I}_K$ whose ideal class, $[J]$, has order $r$.
(ii) $N_{K|\mathbb{Q}}(J)$, $(i = 2, 3)$ is a principal ideal.
(iii) $q$ ramifies in $k_2$.

Once Proposition 2.2 is established we have the following.
Proof of Theorem 2.1 There are infinitely many primes $q \mid 210r$ for which $\mathcal{P}(X)$ splits into linear factors $\pmod{q}$. Hence there are infinitely many primes $q$ that ramify in the quadratic subfield of some $K \in \mathfrak{K}$ (depending on $q$) for which $\mathcal{I}_K$ contains a relative ideal class of order $r$. Since only finitely many primes can ramify in the quadratic subfields of a finite subcollection of $\mathfrak{K}$, we conclude that the collection of $K \in \mathfrak{K}$ for which $\mathcal{I}_K$ contains a relative ideal class of order $r$ is infinite. □

We remark that we could have proved Theorem 2.1 using the argument given in the proof of Theorem 4.1 below. That proof finds infinitely many fields containing a class of order $r$ by finding cyclic subgroups of the class group of orders that are increasingly higher powers of $r$. Since the proof we’ve given above doesn’t rely on such an argument, it reveals slightly more about this family of fields.

To provide some insight into the motivation behind Proposition 2.2, we note that when $\mathcal{P}(X)$ splits into linear factors $\pmod{q}$, there is a root of the equation

$$X^r = 30n - 143 = f_n(-3), \quad (2.4)$$

in the field $\mathbb{Z}/q\mathbb{Z}$, where $n^2 + 108 \equiv 0 \pmod{q}$.

Let

$$w := \frac{(3 + \rho_1)(3 + \rho_2)}{(3 + \rho_3)(3 + \rho_5)}.$$ 

Proposition 2.3 Let $n \equiv 2 \pmod{4}$ be an integer. If there is a $y \in \mathbb{Z}$ with $7 \nmid y$ and such that $y^r = 30n - 143 = f_n(-3)$, then $w\mathcal{O}_{K_n} = J^r$ for some ideal $J \in \mathcal{I}_{K_n}$.

For the proof of this proposition we require the following easy lemma:

Lemma 2.4 If a prime $p$ is a common divisor of $30n - 143$ and $\text{disc}(f_n)$, then $p = 7$.

Proof The congruences $30n - 143 \equiv 0 \pmod{p}$ and $\text{disc}(f_n) = 3^6(n^2 + 108)^5/2^{14} \equiv 0 \pmod{p}$ hold simultaneously only if $p = 7$. □

Proof of Proposition 2.3 It suffices to prove that for each index $i$, the ideal $(3 + \rho_i)\mathcal{O}_K$ is an $r$th power. Since $n \equiv 2 \pmod{4}$, each $\rho_i$ is an algebraic integer of $K$. Since $7 \nmid y$, no prime dividing $y$ also divides $\text{disc}(f_n)$. If a prime $p \mid y$ and $\mathfrak{P} \mid p\mathcal{O}_K$ is a prime ideal then $\prod_{i=0}^5(3 + \rho_i) = f_n(-3) \in \mathfrak{P}$. Hence $3 + \rho_i \in \mathfrak{P}$ for some $0 \leq i \leq 5$. Each of the six Galois conjugates of $3 + \rho_i$ is contained in a Galois conjugate of $\mathfrak{P}$, but since $p \nmid \text{disc}(f_n)$, no two distinct conjugates of $3 + \rho_i$ can be contained in the same Galois conjugate of $\mathfrak{P}$. Hence the prime ideals $\mathfrak{P}^{\sigma_i}$, $(i = 0, \ldots, 5)$, are all distinct and each contains exactly one of the Galois conjugates of $3 + \rho_i$. So for each prime $p \mid y$, let $\mathfrak{P}_i$ denote the unique prime common divisor of $p\mathcal{O}_K$ and $(3 + \rho_i)\mathcal{O}_K$, $(i = 0, \ldots, 5)$. If $p^{v(p)}$ is the exact power of $p$ dividing $y$, then $\mathfrak{P}_i^{v(p)}$ is the exact power of $\mathfrak{P}_i$ dividing $(3 + \rho_i)\mathcal{O}_K$. Hence $(3 + \rho_i)\mathcal{O}_K = \left(\prod_{p\mid y} \mathfrak{P}_i^{v(p)}\right)^r$. □

The goal of the following subsections is to produce conditions under which the ideal class of $J$ has order exactly $r$. 

Springer
2.1 A unit index

Let $\epsilon$ denote the fundamental unit of $k_2$, let $\mu_0, \mu_1$ be a fundamental system of units for $k_3$ and let $U := \langle -1, \epsilon, \mu_0, \mu_1, \rho_0/\rho_3, \rho_1/\rho_4 \rangle \subseteq O_K^\times$. Since $\text{rk} O_K^\times = 5$, it will suffice to prove the following.

**Lemma 2.5** The subset $S := \{\epsilon, \mu_0, \mu_1, \rho_0/\rho_3, \rho_1/\rho_4\} \subseteq O_K^\times$ is multiplicatively independent.

**Proof** Suppose

$$
\epsilon^a \mu_0^b \mu_1^c (\rho_0/\rho_3)^d (\rho_1/\rho_4)^e = 1,
$$

where $a, b, c, d, e$ are integers. Note that

$$
(\rho_0/\rho_3)^{1-\sigma + \sigma^2} = (\rho_1/\rho_4)^{1-\sigma + \sigma^2} = 1.
$$

Also,

$$
\epsilon^{1-\sigma + \sigma^2} = \pm \epsilon \text{ and } \mu_i^{1-\sigma + \sigma^2} = \pm \mu_i^{-2\sigma}.
$$

Therefore,

$$
\epsilon^a \mu_0^{-2b\sigma} \mu_1^{-2c\sigma} = \pm 1.
$$

Since no nontrivial power of $\epsilon$ is in $k_3$, we must have $a = 0$. The independence of $\mu_0$ and $\mu_1$ yields $b = c = 0$. Therefore,

$$
(\rho_0/\rho_3)^{d+e\sigma} = (\rho_0/\rho_3)^d (\rho_1/\rho_4)^e = \pm 1.
$$

Since $e^2(\sigma^2 - \sigma + 1) - (e\sigma + d)(e\sigma - e - d) = e^2 + de + d^2$, we obtain

$$
(\rho_0/\rho_3)^{e^2+de+d^2} = \pm 1,
$$

hence $d = e = 0$. \qed

Having shown that the index of $U$ in $O_K^\times$ is finite, we want to choose $n$ so as to prevent certain primes from dividing this index. We need the following technical lemma. We employ the notation $(a | \ell)_p = 1$ (resp. $(a | \ell)_p \neq 1$) to mean that $a$ is a $p$th power residue $(\text{mod } \ell)$ (resp. $a$ is a $p$th power nonresidue $(\text{mod } \ell)$.) When the subscript $p = 2$, the notation is the Legendre symbol.

**Lemma 2.6** Let $q$ be as in Proposition 2.2. There is a constant $c_r$ with $c_r^r \equiv 71^{-r} \pmod{30}$ and $(210q, c_r) = 1$ and which is such that for each prime $p | r$ there are primes $\ell_i | c_r$, $(i = 1, 2)$, for which

1. $(2 | \ell_1)_p = (3 | \ell_1)_p = 1$ and $(5 | \ell_1)_p \neq 1$. \hfill \qed

\text{Springer}
(2) \((3 \mid \ell_2)_p = (5 \mid \ell_2)_p = 1\) and \((2 \mid \ell_2)_p \neq 1\).

**Proof** Let \(L_1 = \mathbb{Q}(\zeta_p, 2^{1/p}, 3^{1/p})\) and \(L_2 = \mathbb{Q}(\zeta_{2p}, 5^{1/p})\), where \(\zeta_n\) denotes a primitive \(n\)th root of unity. A prime \(\ell\) totally splits in \(L_1\) if and only if \(\ell \equiv 1 \pmod{p}\) and \((2 \mid \ell)_p = (3 \mid \ell)_p = 1\). Likewise a prime \(\ell\) totally splits in \(L_2\) if and only if \(\ell \equiv 1 \pmod{2p}\) and \((5 \mid \ell)_p = 1\).

Bauer’s Theorem [9, Chapter VII, Prop. 13.9] states that if \(K_1\) and \(K_2\) are finite Galois extensions of \(\mathbb{Q}\), then \(K_1 \subseteq K_2\) if and only if the set of primes that split completely in \(K_2\) is contained (modulo a finite set) in the set of primes that split completely in \(K_1\) (this is also a consequence of Chebotarev’s Density Theorem). Since \(L_2 \not\subseteq L_1\), we conclude that there are infinitely many primes \(\ell\) that totally split in \(L_1\) but not in \(L_2\). Hence there are infinitely many primes \(\ell\) such that \((2 \mid \ell)_p = (3 \mid \ell)_p = 1\) and \((5 \mid \ell)_p \neq 1\). Choose such a prime \(\ell_1\) and use the infinitude of such primes to ensure that \((\ell_1, 210q) = 1\). Similarly, choose \(\ell_2\) with \((\ell_2, 210q) = 1\), and such that \((3 \mid \ell_2)_p = (5 \mid \ell_2)_p = 1\) and \((2 \mid \ell_2)_p \neq 1\). Repeat this procedure for each prime \(p | r\). Choose \(a, b \in \mathbb{Z}\) such that \(ra + 4b = 1\) and choose \(s \in \mathbb{N}\) with \((s, 7q) = 1\) and such that \(s \left( \prod_{p | r} \ell_1(p)^2 \ell_2(p) \right) \equiv 7^{(1-r)a} \pmod{30}\). Setting \(c_r = s^{r} \left( \prod_{p | r} \ell_1(p)^2 \ell_2(p) \right)^r \equiv 7^{(1-r)ar} \equiv (7^{1-r})^{ra+4b} = 7^{1-r} \pmod{30}\). □

**Proposition 2.7** Let \(n \equiv 2 \pmod{4}\) be an integer. Let \(\ell_1, \ell_2\) be primes not equal to 7. If \(n\) is such that \(\ell_1 \ell_2 | 30n - 143 = f_n(-3)\) and \(p \neq 2, 3\) is a prime such that

1. \((2 \mid \ell_1)_p = (3 \mid \ell_1)_p = 1\) and \((5 \mid \ell_1)_p \neq 1\),
2. \((3 \mid \ell_2)_p = (5 \mid \ell_2)_p = 1\) and \((2 \mid \ell_2)_p \neq 1\),

then \(p \nmid [\mathcal{O}_K^\times : U]\).

**Proof** If \(p \mid [\mathcal{O}_K^\times : U]\), then there is a \(u \in \mathcal{O}_K^\times \setminus U\) such that \(u^p = \pm \varepsilon^a \mu_0^b \mu_1^c (\rho_0/\rho_3)^d (\rho_1/\rho_4)^e\). Without loss of generality, we may take \(u^p = \varepsilon^a \mu_0^b \mu_1^c (\rho_0/\rho_3)^d (\rho_1/\rho_4)^e\) with \(0 \leq a, b, c, d, e < p\). Taking field norms, we find that \((N_{K|\mathbb{Q}}(u))^p = \pm \varepsilon^{3a}\). Hence \(p \mid a\) and \(a = 0\). Likewise the fact that \((N_{K|\mathbb{Q}}(u))^p = \pm \mu_0^b \mu_1^c \) implies that \(p\) divides both \(b\) and \(c\) and hence that \(b = c = 0\). Choose prime ideals \(L_i \subset \mathbb{O}_K, (i = 1, 2)\), with \(L_i \cap \mathbb{Z} = \ell_i \mathbb{Z}\) and such that \(\rho_0 \equiv -3 \pmod{L_i}\). Then \(\rho_0/\rho_3 \equiv 15 \pmod{L_i}\), and \(\rho_1/\rho_4 \equiv 6 \pmod{L_i}\), and we deduce that \(u^p \equiv (-1)^e 2^e 3^d 5^e 7^e \pmod{L_i}\). Note that every Galois conjugate ideal \(L_i\) contains a conjugate of \(3 + \rho_0\), but that no two such ideals can contain the same conjugate since this would imply that \(\ell_i\) was a common divisor of \(30n - 143\) and \(\text{disc}(f_n)\) and so would contradict Lemma 2.4. Hence \(\ell_i\) completely splits in \(K\) and the residual degree of \(L_i\) is equal to 1. Applying our power residue hypotheses we conclude that \(d = e = 0\). But then \(u^p = 1\) and so \(u = 1 \in U\); contradiction. Hence \(p \nmid [\mathcal{O}_K^\times : U]\). □
2.2 A consequence of Hilbert’s Irreducibility Theorem

To apply Proposition 2.11 below, we will need a condition sufficient to guarantee that \( w_{\rho_4}/\rho_1 \) fails to have a \( p \)th root in \( K_n \) for each prime \( p | r \). The next proposition provides us with such a condition.

Proposition 2.8 Let

\[
p_{n,r}(X) := \sum_{k=0}^{6} a_k X^{rk},
\]

where

\[
\begin{align*}
a_0 &= a_6 = (30n - 143)^2 \\
a_1 &= a_5 = 6(30n - 143)^2 \\
a_2 &= a_4 = -104149n^2 - 128700n - 12399357 \\
&= -104149 \frac{(30n - 143)^2}{900} - \frac{16823807}{450} (30n - 143) - \frac{13841287201}{900} \\
a_3 &= -253298n^2 + 171600n - 25821164 \\
&= -253298 \frac{(30n - 143)^2}{900} - \frac{16823807}{225} (30n - 143) - \frac{13841287201}{450}.
\end{align*}
\]

If \( p_{n,r}(X) \) is irreducible in \( \mathbb{Q}[X] \), then for each \( p | r \), \( w_{\rho_4}/\rho_1 \) fails to have a \( p \)th root in \( K_n \).

Proof If there is a \( z \in K_n^\times \) such that \( z^p = w_{\rho_4}/\rho_1 \) with \( p \) a prime dividing \( r \), then \( X^r - w_{\rho_4}/\rho_1 \) factors non-trivially in \( K_n[X] \). Let \( m(X) \in \mathbb{Q}[X] \) denote the minimal polynomial of \( w_{\rho_4}/\rho_1 \) over \( \mathbb{Q} \).

We claim that \( \deg m(X) = 6 \), and \( w_{\rho_4}/\rho_1 \) is a primitive element for \( K_n/\mathbb{Q} \). Note that \( w_{\rho_4}/\rho_1 \) has trivial norm down to each proper subfield of \( K_n \). If \( w_{\rho_4}/\rho_1 \) was contained in such a proper subfield we would be forced to conclude that \( w = \pm \rho_1/\rho_4 \). Using Eq. (2.2), we rewrite this as a non-trivial polynomial relation in \( \rho \) of degree less than 6. Since \( \rho \) is a primitive element for \( K_n/\mathbb{Q} \) we’ve reached a contradiction and so conclude that \( w_{\rho_4}/\rho_1 \) is not contained in any proper subfield of \( K_n \) and so is a primitive element for the extension.

Let \( \zeta \) be a zero of \( X^r - w_{\rho_1}/\rho_4 \). Since \( X^r - w_{\rho_1}/\rho_4 \) is reducible in \( K_n[X] \) and since \( \zeta^r = w_{\rho_1}/\rho_4 \), we deduce that \( [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : K_n][K_n : \mathbb{Q}] < 6r \).

But since \( m(\zeta^r) = 0 \), we deduce that \( m(X^r) \) factors non-trivially in \( \mathbb{Q}[X] \) (because otherwise \( [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg m(X^r) = 6r \)). A straightforward calculation reveals that \( p_{n,r}(\zeta) = 0 \), so \( m(X^r) \) is a constant times the polynomial \( p_{n,r}(X) \). Thus we have shown that the existence of a prime \( p | r \) such that \( w_{\rho_4}/\rho_1 \in (K_n^r)^p \) implies that \( p_{n,r}(X) \) admits a non-trivial factorization in \( \mathbb{Q}[X] \).
Hilbert’s Irreducibility Theorem [5] states that if \( g(X, Y) \) is an irreducible polynomial in \( \mathbb{Z}[X, Y] \), then there are infinitely many \( m \in \mathbb{Z} \) such that \( g(X, m) \) is irreducible in \( \mathbb{Z}[X] \). In particular, if \( g(X, Y) \) is an irreducible polynomial in \( \mathbb{Z}[X, Y] \) and if for each \( m \in \mathbb{Z} \) there is an \( n_m \in \mathbb{Z} \) such that

\[
g(X, m) = p_{n_m,r}(X),
\]

then Hilbert’s Irreducibility Theorem implies that there are infinitely many \( m \in \mathbb{Z} \) such that \( p_{n_m,r}(X) \) is irreducible in \( \mathbb{Q}[X] \). We turn now to the construction of such a polynomial \( g(X, Y) \in \mathbb{Z}[X, Y] \).

**Proposition 2.9** Let \( r > 0 \) be an integer with \((r, 6) = 1\) and let \( y_0, c_r \in \mathbb{Z} \), where the latter is chosen such that \((-143c_r)^r \equiv -143 \pmod{30}\). Let

\[
g(X, Y) := \sum_{k=0}^{6} g_k(Y)X^{rk},
\]

where

\[
g_0(Y) = g_6(Y) = (c_r(30(y_0 + 8q^2Y) - 143))^{2r}
\]
\[
g_1(Y) = g_5(Y) = -6g_0(Y)
\]
\[
g_2(Y) = g_4(Y) = -\frac{104149}{900}g_0(Y) - \frac{16823807}{450}\sqrt{g_0(Y)} - \frac{13841287201}{900}
\]
\[
g_3(Y) = -\frac{253298}{900}g_0(Y) - \frac{16823807}{225}\sqrt{g_0(Y)} - \frac{13841287201}{450}.
\]

Then \( g(X, Y) \) is irreducible in \( \mathbb{Q}[X, Y] \) and for each \( m \in \mathbb{Z} \), \( g(X, m) = p_{n_m,r}(X) \), where \( n_m \) is the unique integer satisfying

\[
(c_r(30(y_0 + 8q^2m) - 143))^r = 30n_m - 143.
\]

To establish the proposition, we first need the following

**Lemma 2.10** Let \( t \in \mathbb{Q} \) be such that \( c_r(30(y_0 + 8q^2t) - 143) = 1 \). Then \( g(X, t) \) is irreducible in \( \mathbb{Q}[X] \).

**Proof** Note that \( g(X, t) = h(X^r) \), where

\[
h(X) = X^6 - 6X^5 - \frac{385417749}{25}X^4 - \frac{770836748}{25}X^3 - \frac{385417749}{25}X^2 - 6X + 1.
\]

Since \( 25h(X + 1) \) is Eisenstein at 13, \( h(X) \) is irreducible in \( \mathbb{Q}[X] \). Let \( v \) be a zero of \( h(X) \). If \( g(X, t) = h(X^r) \) has a non-trivial factorization in \( \mathbb{Q}[X] \), then \( X^r - v \) has a non-trivial factorization in \( \mathbb{Q}(v)[X] \). So it suffices to show that \( X^r - v \) is irreducible in \( \mathbb{Q}(v)[X] \). By [6, Chapter VI, §9, Theorem 9.1], it suffices to show that \( v \notin (\mathbb{Q}(v))^p \) for each prime \( p \mid r \). Towards this end, we note that \( 5^6 h \left( \frac{X}{5} \right) \) is a monic polynomial

\[\square\] Springer
in \(\mathbb{Z}[X]\) that has 5\(v\) as a zero. Hence 5\(v\) is an algebraic integer in \(\mathbb{Q}(v)\). Since \(v\) is not an algebraic integer in \(\mathbb{Q}(v)\) it has some prime ideals in its denominator. But since 5\(v\) is an algebraic integer in \(\mathbb{Q}(v)\) and since 5 splits completely in \(\mathbb{Q}(v)\) (as is easily checked using PARI [10], for example), \(v\) must have the first power of some ideal in its denominator. Hence \(v \notin (\mathbb{Q}(v))^p\) for every prime \(p \mid r\).

**Proof of Proposition 2.9** Suppose that \(g(X, Y) = k(X, Y) j(X, Y)\) is a non-trivial factorization of \(g(X, Y)\) in \(\mathbb{Q}[X, Y]\). If \(k\) and \(j\) each have degree \(\geq 1\) in \(X\), then choosing \(t \in \mathbb{Q}\) such that \(c_r(30(\gamma_0 + 8q^2t) - 143) = 1\) implies that \(g(X, t) = k(X, t) j(X, t)\) is a non-trivial factorization of \(g(X, t)\) in \(\mathbb{Q}[X]\); a contradiction to Lemma 2.10. We conclude that if \(g(X, Y)\) factors non-trivially in \(\mathbb{Q}[X, Y]\), then one of the factors must have degree 0 in \(X\); i.e., \(g(X, Y) = k(Y) j(X, Y)\). Without loss of generality we may assume that \(k(Y)\) is irreducible in \(\mathbb{Q}[X, Y]\). Hence \(k(Y)\) divides each \(g_i(Y)\) as well as \(\sqrt{g_0}(Y)\). We conclude that \(k(Y)\) divides 900\(g_2(Y) + 104149g_0(Y) + 2(16823807)\sqrt{g_0}(Y) = -712^2\). But \(k(Y)\) is a non-trivial factor of \(g(X, Y)\) in \(\mathbb{Q}[X, Y]\) and so must have degree greater than 0 in \(Y\). This contradiction reveals that \(g(X, Y)\) is irreducible in \(\mathbb{Q}[X, Y]\).

Note that for each \(m \in \mathbb{Z}\), \((c_r(30(\gamma_0 + 8q^2m) - 143))^{r} = (-143c_r)^{r} = -143 (mod 30)\). Hence for each \(m \in \mathbb{Z}\) there is an \(n_m \in \mathbb{Z}\) such that \((c_r(30(\gamma_0 + 8q^2m) - 143))^{r} = 30n_m - 143\) and hence such that \(g(X, m) = p_{n_m,r}(X)\). The uniqueness of \(n_m\) is clear.

**2.3 The ideal classes**

**Proposition 2.11** Let \(n \equiv 2 \pmod{4}\) be an integer. If there is an integer \(y\) not divisible by 7 satisfying \(y^r = 30n - 143 = f_n(-3)\), and if for each prime \(p \mid r\) the following conditions hold:

1. there are primes \(\ell_i \mid 30n - 143\) \((i = 1, 2)\), such that
   
   a. \((2 \mid \ell_1)p = (3 \mid \ell_1)p = 1\) and \((5 \mid \ell_1)p \neq 1\)
   
   b. \((3 \mid \ell_2)p = (5 \mid \ell_2)p = 1\) and \((2 \mid \ell_2)p \neq 1\)

2. \(w \rho_4/\rho_1\) fails to have a \(p\)th root in \(K_n\),

then \(w \mathcal{O}_K = J^r\) where \([J]\) has order \(r\).

**Proof** From Proposition 2.3 we deduce that \(w \mathcal{O}_K = J^r\) for some ideal \(J \in \mathcal{I}_K\) and so the order of \([J]\) is \(\leq r\). If it is strictly \(< r\), then \(w \mathcal{O}_K\) is a prime power of a principal ideal for some prime \(p \mid r\). Supposing this to be the case and writing \(w \mathcal{O}_K = (z \mathcal{O}_K)^p\), for some \(z \in K^*\), we have that \(w = uz^p\) for some \(u \in \mathcal{O}_K^*\). Since \(p \mid [\mathcal{O}_K^* : U]\), we may assume \(u \in U\). Since \(p\) is odd, we may ignore any factor of \(-1\) and assume that

\[
u = e^a \mu_0 b \mu_1 c (\rho_0/\rho_3)^d (\rho_1/\rho_4)^e.
\]

By absorbing any \(p\)th powers into \(z^p\), we may further assume that \(a, b, c, d,\) and \(e\) are integers in the interval \([0, p)\). Since \(N_{K|k_2}(w) = 1\), we deduce that \(N_{K|k_2}(1/z)^p = N_{K|k_2}(u) = \pm e^{3u}\). Recalling that \(p \mid r\) and that \((r, 6) = 1\), we find that \(p \mid a\) and so conclude that \(a = 0\). Since \(N_{K|k_3}(w) = 1\), we deduce that \(N_{K|k_3}(1/z)^p = N_{K|k_3}(u) = \pm e^{3r}\).

\(\text{Springer}\)
$ \pm \mu_0^{2\nu} \mu_1^{2c}$. Hence $p \mid b$ and $p \mid c$ and so $b = c = 0$. Thus $w = (\rho_0 / \rho_3)^d (\rho_1 / \rho_4)^e z^p$. Choose prime ideals $L_i \subset \mathcal{O}_K$, $(i = 1, 2)$, with $L_i \cap \mathbb{Z} = \ell_i \mathbb{Z}$ and such that $\rho_0 \equiv -3 (\text{mod } L_i)$, $\rho_3 / \rho_0 \equiv 1/5 (\text{mod } L_i)$, and $\rho_4 / \rho_1 \equiv -1/6 (\text{mod } L_i)$, and we deduce that $z^p \equiv (-1)^e 2^{1-e} 3^{1-d-e} 5^{-d} (\text{mod } \ell_i)$. Applying our power residue hypotheses we conclude that $d = 0$, $e = 1$ and thereby deduce that $w \rho_2 / \rho_1$ has a $p$th root in $K$. Since this contradicts our hypotheses $w \mathcal{O}_K$ is not a prime power of a principal ideal for any prime $p \mid r$ and $[J]$ has order $r$. \hfill \Box

We now prove

**Proposition 2.12** There is a $y \in \mathbb{Z}$ for which Proposition 2.11 holds and hence a field $K_n \in \mathcal{F}$ for which

(i) there is an ideal $J \in \mathcal{I}_{K_n}$ whose ideal class, $[J]$, has order $r$.

(ii) $N_{K | k_i}(J)$, $(i = 2, 3)$ is a principal ideal.

**Proof of Proposition 2.12** Choose $c_r$ according to Lemma 2.6, let $y_0 \in \mathbb{Z}$, and let $y := dc_r(30(y_0 + 8q^2 m) - 143)$, where $d$ satisfies the system of congruences $d \equiv 5/(c_r(30y_0 - 143)) (\text{mod } 8)$ and $d \equiv 1 (\text{mod } 30)$. Then $y_r \equiv (-143 c_r)^r \equiv (7c_r)^r \equiv 7 (\text{mod } 30)$. Hence $y_r \equiv 30n - 143$ for some $n \in \mathbb{Z}$. Furthermore, since $r$ is odd and since $y \equiv 5 (\text{mod } 8)$, the congruence $5 \equiv y_r \equiv 30n - 143 (\text{mod } 8)$ implies that $n \equiv 2 (\text{mod } 4)$. According to Lemma 2.6, for each prime $p \mid r$ there are primes dividing $c_r$, and hence dividing $30n - 143$, that satisfy condition (1) of Proposition 2.11. Since $(dc_r(30y_0 - 143))^r \equiv -143 (\text{mod } 30)$, Proposition 2.9 and the discussion of Hilbert’s Irreducibility Theorem preceding it reveal that $p_{n,r}(X)$ is irreducible in $\mathbb{Q}[X]$ for infinitely many $m \in \mathbb{Z}$. Choose such a pair $(m, n_m)$. Proposition 2.8 reveals that $w \rho_2 / \rho_1$ fails to have a $p$th root in $K_{n_m}$ for each prime $p \mid r$. We see that for such a pair $(m, n_m)$ all of the hypotheses of Proposition 2.11 are satisfied and we conclude that there is a field $K := K_{n_m} \in \mathcal{F}$ for which $w \mathcal{O}_K = J^r$ where $[J]$ has order $r$. Finally, since $J^r = w \mathcal{O}_K$ and since $N_{K | k_i}(w) = 1$ $(i = 2, 3)$, it is clear that $N_{K | k_i}(J) = \mathcal{O}_{k_i}$ $(i = 2, 3)$.

At this point we have found a field $K \in \mathcal{F}$ that satisfies conditions (i) and (ii) of Proposition 2.2. All that remains to establish this proposition is to show that $q$ ramifies in $k_2$. This is accomplished through a judicious choice of $y_0$ in the following proof.

**Proof of Proposition 2.2** Since $\mathcal{P}(X)$ splits into linear factors (mod $q$), we deduce that $(-108 \mid q)^2 = 1$. Choose $n_0 \in \mathbb{Z}$ such that $n_0^2 + 108 \equiv 0 (\text{mod } q)$ and $n_0^2 + 108 \not\equiv 0 (\text{mod } q^2)$. Use the fact that $\mathcal{P}(X)$ splits into linear factors (mod $q$) to choose $b_0 \in \mathbb{Z}$ such that $b_0^r \equiv 30n_0 - 143 (\text{mod } q)$. Note that $q \not\equiv 7$ implies that $q \not\mid b_0$, since otherwise $q$ would be a prime common divisor of $30n_0 - 143$ and $n_0^2 + 108 \mid \text{disc}(f_{n_0}(X))$. Since $q \not\mid b_0$ and since $q \not\mid r$, we conclude that we may lift $b_0$ to an $r$th root of $30n_0 - 143 (\text{mod } q^2)$. Choose $c_r$ according to Lemma 2.6 and note that since $q \not\mid 30c_r$, we may choose $y_0 \in \mathbb{Z}$ such that $b_0 \equiv c_r(30y_0 - 143) (\text{mod } q^2)$.

Let $m \in \mathbb{Z}$ and let $y := dc_r(30(y_0 + 8q^2 m) - 143)$, where $d$ satisfies the system of congruences $d \equiv 5/(c_r(30y_0 - 143)) (\text{mod } 8)$ and $d \equiv 1 (\text{mod } 30q^2)$. Then $y_r \equiv b_0^r \equiv 30n_0 - 143 (\text{mod } q^2)$. Since $y_r \equiv -143 (\text{mod } 30)$, we have $y_r = 30n_m - 143$, for some $n_m \in \mathbb{Z}$. Since $n_m \equiv n_0 (\text{mod } q^2)$, we deduce that $n_m^2 + 108 \equiv 0 (\text{mod } q)$.
and \( n_m^2 + 108 \not\equiv 0 \pmod{q^2} \). This implies that \( q \) ramifies in \( k_2 = \mathbb{Q}(\sqrt{n_m^2 + 108}) \subset K_{n_m} \), since \( q \) divides the square-free part of \( \text{disc}(X^2 - (n_m^2 + 108)) \) and so divides \( \text{disc}(\mathcal{O}_{k_2}/\mathbb{Z}) \).

We conclude that for each \( m \in \mathbb{Z} \), the prime \( q \) ramifies in \( K_{n_m} \). To prove that one of these fields satisfies conditions \((i)\) and \((ii)\) of Proposition 2.2, one may copy the proof of Proposition 2.12 verbatim beginning with the fourth sentence.

\( \square \)

3 A family of quartic number fields

In this section we apply the method introduced in the previous section to a family of quartic number fields. Since the results and proofs of this section are highly similar to those presented in the previous section, much of this section will be abridged.

Let \( n \in \mathbb{Z} \setminus \{0, \pm 3\} \) and let \( K_n = \mathbb{Q}(\rho) \), where \( \rho \) is a root of

\[
fn(X) := X^4 - nX^3 - 6X^2 + nX + 1. \tag{3.1}
\]

\( K_n/\mathbb{Q} \) is a real cyclic quartic extension and was studied by M.-N. Gras in [3]. Let \( G := \text{Gal}(K_n/\mathbb{Q}) \). Then \( G = \langle \sigma \mid \sigma^4 = 1 \rangle \), where \( \sigma : \rho \mapsto (\rho - 1)/(\rho + 1) \). The images of \( \rho \) under \( G \), denoted \( \rho_i := \sigma^i(\rho) \), \( (i = 0, \ldots, 3) \), are given by

\[
\rho_0 = \rho, \quad \rho_1 = (\rho - 1)/(\rho + 1),
\rho_2 = -1/\rho, \quad \rho_3 = -(\rho + 1)/(\rho - 1). \tag{3.2}
\]

Let \( \mathfrak{F} := \{ K_n \mid n \neq 0, \pm 3 \} \). Let \( \mathcal{I}_K \) denote the group of fractional ideals of \( K \in \mathfrak{F} \) and for a fractional ideal \( J \in \mathcal{I}_K \), let \( [J] \) denote its ideal class. Let \( k_2 = \mathbb{Q}(\sqrt{n^2 + 16}) \) denote the unique quadratic subfield of \( K \). Then \( [J] \) is said to be a relative ideal class if it has trivial norm down to \( k_2 \).

Note that the \( \rho_i \) \( (i = 0, \ldots, 3) \) are algebraic integers and, in fact, relative units of \( K_n \).

Our primary result is

**Theorem 3.1** Let \( r > 0 \) be an odd integer. There are infinitely many fields \( K \in \mathfrak{F} \) containing a relative ideal class of order \( r \).

It is straightforward to see that \( K_n = K_{-n} \). However, the parametrization of \( \mathfrak{F} \) given by \( n \mapsto K_n \) fails to be injective even when we restrict to \( n > 0 \). For example Lazarus [7] notes that \( K_2 = K_{22} \). Hence in proving Theorem 3.1 it is insufficient to simply show that there are infinitely many \( n \) such that \( K_n \) contains a relative ideal class of order \( r \). Instead we put most of our effort into first proving

**Proposition 3.2** Let \( r > 0 \) be an odd integer. Let \( q \in \mathbb{Z} \) be a prime such that

\[
P(X) := (X^r + 7 - 6\sqrt{-16})(X^r + 7 + 6\sqrt{-16}) \in \mathbb{Z}[X],
\]

splits into linear factors \( \pmod{q} \). Assume that \( q \nmid 5r \). There is a field \( K \in \mathfrak{F} \) that satisfies the following three conditions:

\( \square \) Springer
(i) There is an ideal \( J \in \mathcal{I}_K \) whose ideal class, \([J]\), has order \( r \).

(ii) \( N_{K|k_2}(J) \) is a principal ideal.

(iii) \( q \) ramifies in \( k_2 \).

Once Proposition 3.2 is established we have the following

**Proof of Theorem 3.1** Replace \( q \not| 210r \) with \( q \not| 5r \) in the proof of Theorem 2.1.

Let

\[ w := \frac{2 + \rho_1}{2 + \rho_3}. \]

**Proposition 3.3** If there is a \( y \in \mathbb{Z} \) with \( 5 \not| y \) and such that \( y^r = 6n - 7 = f_n(-2) \), then \( w \mathcal{O}_{K_n} = J^r \) for some ideal \( J \in \mathcal{I}_{K_n} \).

For the proof of this proposition we require the following easy lemma:

**Lemma 3.4** If a prime \( p \) is a common divisor of \( 6n - 7 \) and \( \text{disc}(f_n) \), then \( p = 5 \).

**Proof** The congruences \( 6n - 7 \equiv 0 \) (mod \( p \)) and \( \text{disc}(f_n) = 4(n^2 + 16)^3 \equiv 0 \) (mod \( p \)) hold simultaneously only if \( p = 5 \).

**Proof of Proposition 3.3** In the proof of Proposition 2.3 above, replace \( 7 \not| y \) with \( 5 \not| y \). Also restrict the indices \( 0 \leq i \leq 3 \) and replace \( (3 + \rho_i) \) with \( (2 + \rho_i) \) and \( f_n(-3) \) with \( f_n(-2) \). Finally note that no restriction on the congruence class of \( n \) is required, because \( \rho \) and its conjugates are algebraic integers.

3.1 A unit index

Let \( \varepsilon \) denote the fundamental unit of \( k_2 \) and let \( U := \langle -1, \varepsilon, \rho_0, \rho_1 \rangle \leq \mathcal{O}_K^\times \). We will need to know that \([\mathcal{O}_K^\times : U]< \infty \). It suffices to prove the following.

**Lemma 3.5** The set \( S := \{ \varepsilon, \rho_0, \rho_1 \} \subset \mathcal{O}_K^\times \) is multiplicatively independent.

**Proof** Suppose

\[ 1 = e^a \rho_0^b \rho_1^c = e^a \rho_0^{b+c}. \]

Since \( \rho_0^{1+\sigma^2} = \pm 1 \), applying \( 1 + \sigma^2 \) yields \( \varepsilon^{2a} = \pm 1 \), so \( a = 0 \). The relation

\[ c^2(\sigma^2 + 1) - (b + c\sigma)(c\sigma - b) = b^2 + c^2, \]

yields \( \rho_0^{b^2+c^2} = \pm 1 \), hence \( b = c = 0 \).

We remind the reader that the notation (introduced in Sect. 1 above) \( (a \mid \ell)_p = 1 \) (resp. \( (a \mid \ell)_p \neq 1 \)) means that \( a \) is a \( p \)th power residue (mod \( \ell \)) (resp. \( a \) is a \( p \)th power nonresidue (mod \( \ell \)).

We need a technical result analogous to the one used for sextic fields.
Lemma 3.6 Let $q$ be as in Proposition 3.2. There is a constant $c_r \equiv 1 \pmod{6}$ with $(c_r, 5q) = 1$ and which is such that for each prime $p \mid r$ there are primes $\ell_i \mid c_r$, $(i = 1, 2)$, for which

(i) $(2 \mid \ell_1)_p = 1$ and $(3 \mid \ell_1)_p \neq 1$.

(ii) $(3 \mid \ell_2)_p = 1$ and $(2 \mid \ell_2)_p \neq 1$.

Proof Let $L_1 = \mathbb{Q}(\xi_p, 2^{1/p})$ and $L_2 = \mathbb{Q}(\xi_{2p}, 3^{1/p})$, and then for each prime $p$ dividing $r$ use Bauer’s Theorem as in the proof of Lemma 2.6 to choose primes $\ell_1(p)$ (resp. $\ell_2(p)$) satisfying condition (1) (resp. condition (2)) of the lemma with each $\ell_i \nmid 30q$. Then set $c_r = s\left(\prod_{p \mid r} \ell_1(p)\ell_2(p)\right)$, where $s$ is chosen to ensure that $c_r \equiv 1 \pmod{6}$.

\[ \Box \]

Proposition 3.7 Let $n$ be an integer, and let $\ell \neq 5$ be a prime such that $\ell \mid 6n - 7 = f_n(-2)$. If $p$ is an odd prime such that $(2 \mid \ell)_p = 1$ and $(3 \mid \ell)_p \neq 1$, then $p \nmid [O_K : U]$.

Proof If $p \mid [O_K : U]$, then there is a $u \in O_K \setminus U$ such that $u^p = \pm e^a \rho_0^b \rho_1^c$. Without loss of generality we may take $u^p = e^a \rho_0^b \rho_1^c$ with $0 \leq a, b, c < p$. Since $\ell$ divides $f_n(-2) = \prod_{i=0}^3 (2 + \rho_i)$, any prime ideal $L$ dividing $\ell O_K$ must contain one of the conjugates $2 + \rho_0$. Furthermore every conjugate $2 + \rho_0$ must be contained in some prime ideal over $\ell$, since the Galois group acts transitively on the set of conjugates of $2 + \rho_0$ and since it takes prime ideals of $O_K$ to prime ideals of $O_K$. Since $\ell \neq 5$ and $\ell \nmid 6n - 7$, we know that $\ell \nmid \text{disc}(f_n)$, and so we deduce that every conjugate of $2 + \rho_0$ is contained in a unique prime ideal over $\ell$. Let $L$ denote the unique prime ideal $L \mid \ell O_K$ such that $-2 \equiv \rho_0 \pmod{L}$. Modulo $L$ this forces $\rho_1 \equiv 3$, $\rho_2 \equiv 1/2$, and $\rho_3 \equiv -1/3$. Hence

\[ (uu^a)^p = (\pm 1)^a (\rho_0 \rho_1)^b (\rho_1 \rho_2)^c \equiv (\pm 1)^a (-1)^b 2^{b-c} 3^{b+c} \pmod{L}, \]

and

\[ (u^a u^{a_2})^p = (\pm 1)^a (\rho_1 \rho_2)^b (\rho_2 \rho_3)^c \equiv (\pm 1)^a (-1)^c 2^{-(b+c)} 3^{b-c} \pmod{L}. \]

Applying the power residue hypotheses to these two congruences we find that $b \equiv c$ and $b \equiv -c \pmod{p}$. Hence $b \equiv c \equiv 0 \pmod{p}$ and so $b = c = 0$. Therefore $u^p = e^a = (e^a)^{a^2} = (u^p)^{a^2}$. Hence $u = u^{a^2}$. But then $u \in O_K^\times \cap k_2 \subset U$. We’ve reached a contradiction, and so are forced to conclude that $p \nmid [O_K^\times : U]$. \[ \Box \]

### 3.2 An application of Hilbert’s Irreducibility Theorem

To apply Proposition 3.11 below, we will need a condition sufficient to guarantee that $w/\rho_1 \notin (K_n^\times)^p$ for each prime $p \mid r$. The next proposition provides us with such a condition.

Proposition 3.8 Let

\[ p_{n,r}(X) := \sum_{k=0}^{4} a_k X^{rk}, \]
where

\[ a_0 = a_4 = -a_2/6 = 6n - 7 \]
\[ a_1 = -a_3 = 7n + 96. \]

If \( p_{n,r}(X) \) is irreducible in \( \mathbb{Q}[X] \), then \( w/\rho_1 \) fails to have a \( p \)th root in \( K_n \) for every prime \( p \mid r \).

**Proof** If there is a \( z \in K_n^\times \) such that \( z^p = w/\rho_1 \) with \( p \) a prime dividing \( r \), then \( X^r - w/\rho_1 \) factors non-trivially in \( K_n[X] \). Let \( m(X) \in \mathbb{Q}[X] \) denote the minimal polynomial of \( w/\rho_1 \) over \( \mathbb{Q} \). We note that \( \deg m(X) = 4 \), since \( w/\rho_1 \) is a primitive element for \( K_n/\mathbb{Q} \). (Note that \( N_{K_n/\mathbb{Q}}(w/\rho_1) = -1 \), so the real number \( w/\rho_1 \) can’t be contained in a proper subfield of \( K_n \).) Let \( \xi \) be a zero of \( X^r - w/\rho_1 \). Since \( X^r - w/\rho_1 \) is reducible in \( K_n[X] \) and since \( \xi^r = w/\rho_1 \), we deduce that \( [\mathbb{Q}(\xi) : \mathbb{Q}] = [\mathbb{Q}(\xi) : K_n][K_n : \mathbb{Q}] < 4r \). But since \( m(\xi^r) = 0 \), we deduce that \( m(X^r) \) factors non-trivially in \( \mathbb{Q}[X] \) (because otherwise \( [\mathbb{Q}(\xi) : \mathbb{Q}] = \deg m(X^r) = 4r \).) Since \( p_{n,r}(X) = a_0 m(X^r) \), we deduce that \( p_{n,r}(X) \) factors non-trivially in \( \mathbb{Q}[X] \). Thus we have shown that the existence of a prime \( p \mid r \) such that \( w/\rho_1 \in (K_n^\times)^p \) implies that \( p_{n,r}(X) \) admits a non-trivial factorization in \( \mathbb{Q}[X] \). \( \square \)

We construct a polynomial \( g(X, Y) \) that is irreducible in \( \mathbb{Z}[X, Y] \) and which has the property that for each \( m \in \mathbb{Z} \) there is an \( n_m \in \mathbb{Z} \) such that \( g(X, m) = p_{n_m, r}(X) \). Applying Hilbert’s Irreducibility Theorem [5], as was done in Sect. 1, will then allow us to conclude that there are infinitely many \( m \in \mathbb{Z} \) such that \( p_{n_m, r}(X) \) is irreducible in \( \mathbb{Q}[X] \).

**Proposition 3.9** Let \( r > 0 \) be an odd integer and let \( y_0, c_r \in \mathbb{Z} \), where the latter is chosen such that \( c_r \equiv 1 \pmod{6} \). Let

\[ g(X, Y) := \sum_{k=0}^{3} g_k(Y) X^{rk}, \]

where

\[ g_0(Y) = g_4(Y) = -g_2(Y)/6 = (c_r(30(y_0 + q^2Y) - 1))^r, \]
\[ g_1(Y) = -g_3(Y) = 7(g_0(Y) + 7)/6 + 96. \]

Then \( g(X, Y) \) is irreducible in \( \mathbb{Q}[X, Y] \) and for each \( m \in \mathbb{Z} \), \( g(X, m) = p_{n_m, r}(X) \), where \( n_m \) is the unique integer satisfying \( (c_r(30(y_0 + q^2m) - 1))^r = 6n_m - 7 \).

To establish the proposition, we first need the following

**Lemma 3.10** Let \( t \in \mathbb{Q} \) be such that \( c_r(30(y_0 + q^2t) - 1) = -1 \). Then \( g(X, t) \) is irreducible in \( \mathbb{Q}[X] \).
Proof Note that \(g(X, t) = -f_{-103}(X^r)\). For this proof, let \(f(X) := f_{-103}(X)\) and \(K := K_{-103} = \mathbb{K}_{103}\). If \(g(x, t) = 0\), then \(\prod_{i=0}^{3}(x^r - \rho_i) = f(x^r) = 0\), and so \(x\) is zero of \(X^r - \rho_i \in K[X]\) for some index \(i\). Let \(\rho := \rho_i\) and note that it will suffice to show that \(X^r - \rho\) is irreducible in \(K[X]\). By [6, Chapter VI, §9, Theorem 9.1] it is sufficient to show that \(\rho \not\in (K^\times)^p\) for each prime \(p \mid r\). Using PARI [10] we find that a fundamental system of units of \(K\) is \(\{u_i\}_{i=1}^3\), where

\[
\begin{align*}
u_1 &= (1/125)\rho^3 + (101/125)\rho^2 - (208/125)\rho + 63/125, \\
u_2 &= (1/250)\rho^3 + (53/125)\rho^2 + (156/125)\rho + 83/250, \\
u_3 &= (1/250)\rho^3 + (48/125)\rho^2 - (364/125)\rho - 207/250.
\end{align*}
\]

In terms of these units, \(\rho = u_1^2u_2^3\). If \(z \in K^\times\) is such that \(z^p = \rho\) for some prime \(p\), then \(z \in \mathcal{O}_K^\times\); say \(z = \prod_{i=1}^3 u_i^a_i\). So \(\left(\prod_{i=1}^3 u_i^{a_i}\right)^p = u_1^2u_2^3\). Since there is no prime \(p\) dividing both 2 and 3, we conclude that \(\rho \not\in (K^\times)^p\) for each prime \(p \mid r\). \(\square\)

Proof of Proposition 3.9 Suppose that \(g(X, Y) = k(X, Y)j(X, Y)\) is a non-trivial factorization of \(g(X, Y)\) in \(\mathbb{Q}[X, Y]\) and then by choosing \(t \in \mathbb{Q}\) such that \(c_r(30(30 + q^2t) - 1) = -1\) proceed as in the proof of Lemma 2.9 to show that one of the factors must have degree 0 in \(X\); say \(g(X, Y) = K(Y)j(X, Y)\). Without loss of generality assume that \(k(Y)\) is irreducible in \(\mathbb{Q}[X, Y]\). Hence \(k(Y)\) divides each \(g_i(Y)\) and we conclude that \(k(Y)\) divides \(6g_2(Y) - 7g_1(Y) = 625\). But \(k(Y)\) is a non-trivial factor of \(g(X, Y)\) in \(\mathbb{Q}[X, Y]\) and so must have degree greater than 0 in \(Y\). This contradiction reveals that \(g(X, Y)\) is irreducible in \(\mathbb{Q}[X, Y]\). For each \(m \in \mathbb{Z}\), \((c_r(30(30 + q^2m) - 1))^r \equiv (-c_r)^r \equiv -1 \pmod{6}\). Hence for each \(m \in \mathbb{Z}\) there is an \(n_m \in \mathbb{Z}\) such that \((c_r(30(30 + q^2m) - 1))^r = 6n_m - 7\) and hence such that \(g(X, m) = p_{n_m, r}(X)\). The uniqueness of \(n_m\) is clear. \(\square\)

3.3 The ideal classes

Proposition 3.11 If there is an integer \(y\) not divisible by 5 satisfying \(y^r = 6n - 7 = f_n(-2)\), and if for each prime \(p \mid r\) the following conditions hold:

1. there are primes \(\ell_i\) \((i = 1, 2)\), such that
   1. \(2 \not\mid \ell_1\) \(p = 1\) and \((3 \mid \ell_1) \neq 1\)
   2. \(3 \not\mid \ell_2\) \(p = 1\) and \((2 \mid \ell_2) \neq 1\)
2. \(w/\rho_1\) fails to have a \(p\)th root in \(K_n\).

then \(w\mathcal{O}_K = J^r\) where \([J]\) has order \(r\).

Proof The proof is nearly identical to that used in the proof of Proposition 2.11 except that we assume the unit \(u\) to have the form \(u = \varepsilon^n\rho_0^b\rho_1^c\). Taking norms down to \(k_2\) then allows us to deduce that \(w = \rho_0^b\rho_1^c\). Choosing the unique prime ideals \(\mathcal{L}_i\) \([\ell_i]\mathcal{O}_K\) containing \(\rho_0 + 2\) determines the classes of \(\rho_0, \rho_1,\) and \(w\) \((\bmod \mathcal{L}_i)\) and thereby allows us to deduce that \(z^p \equiv (-1)^b2^b3^{1-c} \pmod{\ell_i}\). Applying the power...
residue hypotheses then forces \( b = 0 \) and \( c = 1 \) and so brings us to the contradiction \( z^p = w/\rho_1 \).

We now prove the following.

**Proposition 3.12** There is a \( y \in \mathbb{Z} \) for which Proposition 3.11 holds and hence a field \( K_n \in \mathfrak{F} \) for which

(i) there is an ideal \( J \in \mathcal{I}_{K_n} \) whose ideal class, \([J]\), has order \( r \).

(ii) \( N_{K/k_2}(J) \) is a principal ideal.

**Proof** Choose \( c_r \) according to Lemma 3.6, let \( y_0 \in \mathbb{Z} \), and let \( y := c_r(30(y_0 + q^2m) - 1) \). Then \( y' \equiv (-c_r)^r \equiv -1 \pmod{6} \). Hence \( y' = 6n - 7 \) for some \( n \in \mathbb{Z} \).

According to Lemma 3.6, for each prime \( p \mid r \) there are primes dividing \( c_r \), and hence dividing \( 6n - 7 \), that satisfy condition (1) of Proposition 3.11. Since \( c_r \equiv 1 \pmod{6} \), Proposition 3.9 and the discussion of Hilbert’s Irreducibility Theorem preceding it reveal that \( p_{n_m,r}(X) \) is irreducible in \( \mathbb{Q}[X] \) for infinitely many \( m \in \mathbb{Z} \). Choose such a pair \((m, n_m)\). Proposition 3.8 reveals that \( w/\rho_1 \) fails to have a \( p \)-th root in \( K_{n_m} \) for each prime \( p \mid r \). We see that for such a pair \((m, n_m)\) all of the hypotheses of Proposition 3.11 are satisfied and we conclude that there is a field \( K := K_{n_m} \in \mathfrak{F} \) for which \( wO_K = J^r \) where \([J]\) has order \( r \). Finally, since \( J^r = wO_K \) and since \( N_{K/k_2}(w) = 1 \), it is clear that \( N_{K/k_2}(J) = O_{k_2} \).

At this point we have found a field \( K \in \mathfrak{F} \) that satisfies conditions (i) and (ii) of Proposition 3.2. All that remains to establish this proposition is to show that \( q \) ramifies in \( k_2 \). This is accomplished through a judicious choice of \( y_0 \) in the following proof.

**Proof of Proposition 3.2** Since \( p(X) \) splits into linear factors \( \pmod{q} \), we deduce that \((-16 \mid q) = 1 \). Choose \( n_0 \in \mathbb{Z} \) such that \( n_0^2 + 16 \equiv 0 \pmod{q} \) and \( n_0^2 + 16 \not\equiv 0 \pmod{q} \). Use the fact that \( p(X) \) splits into linear factors \( \pmod{q} \) to choose \( b_0 \in \mathbb{Z} \) such that \( b_0^r \equiv 6n_0 - 7 \pmod{q} \). Note that \( q \not\equiv 5 \) implies that \( q \nmid b_0 \), since otherwise \( q \) would be a prime common divisor of \( 6n_0 - 7 \) and \( n_0^2 + 16 \mid \text{disc}(f_{n_0}(X)) \). Since \( q \nmid b_0 \) and since \( q \nmid r \), we conclude that we may lift \( b_0 \) to an \( r \)-th root of \( 6n_0 - 7 \) \( \pmod{q} \). Choose \( c_r \) according to Lemma 3.6 and note that since \( q \nmid 30c_r \), we may choose \( y_0 \in \mathbb{Z} \) such that \( b_0 \equiv c_r(30y_0 - 1) \pmod{q} \).

Let \( m \in \mathbb{Z} \) and let \( y := c_r(30(y_0 + q^2m) - 1) \). Then \( y' \equiv b_0' \equiv 6n_0 - 7 \pmod{q} \). Since \( y' \equiv -1 \pmod{6} \), we have \( y' = 6n_m - 7 \), for some \( n_m \in \mathbb{Z} \). Since \( n_m \equiv n_0 \pmod{q} \), we deduce that \( n_m^2 + 108 \equiv 0 \pmod{q} \) and \( n_0^2 + 108 \not\equiv 0 \pmod{q} \). This implies that \( q \) ramifies in \( k_2 = \mathbb{Q}(\sqrt{n_m^2 + 16}) \subset K_{n_m} \), since \( q \) divides the square-free part of \( \text{disc}(X^2 - (n_m^2 + 16)) \) and so divides \( \text{disc}(O_{k_2}/\mathbb{Z}) \).

We conclude that for each \( m \in \mathbb{Z} \), the prime \( q \) ramifies in \( K_{n_m} \). To prove that one of these fields satisfies conditions (i) and (ii) of Proposition 3.2, one may copy the proof of Proposition 3.12 verbatim beginning with the fourth sentence.

### 4 A family of non-Galois cubic number fields

Let \( K_n = \mathbb{Q}(\rho) \), where \( \rho \) is a root of

\[
 f_n(X) := X^3 + nX^2 + nX - 1. \tag{4.1}
\]
Since \( f_n(\rho) = 0 \) if and only if \( f_{-n}(1/\rho) = 0 \), we have that \( K_n = K_{-n} \) and so we restrict our attention to \( n \geq 0 \). When \( n > 0 \), we find that \( f_n(\pm 1) \neq 0 \) and so conclude that \( f_n(X) \) is irreducible in \( \mathbb{Q}[X] \) (since \( \pm 1 \) are the only possible zeros of \( f_n(X) \) in \( \mathbb{Q} \)). Since this clearly doesn’t hold when \( n = 0 \), we restrict our attention to the cubic extensions \( K_n/\mathbb{Q} \) corresponding to \( n > 0 \). When \( n \geq 5 \), \( f_n(X) \) changes sign in the intervals \((1-n, 2-n), (-1-4/n, -1-1/n)\), and \((1/(n+1), 1/n)\). In particular, \( f_n(X) \) has real zeros, two of which are \( < -1 \), while the third is \( > 0 \). When \( |n| < 5 \), \( f_n(X) \) has some complex zeros and so we restrict our attention to the real cubic extensions \( K_n/\mathbb{Q} \) corresponding to \( n \geq 5 \). Note that \( \text{disc}(f_n(X)) = n^3 - 18n^2 - 27 = (n^2 - 9)^2 - 108 \). Since 108 is a difference of two squares in only two ways and since neither 12 nor 28 is of the form \( n^2 - 9 \), we may conclude that \( \text{disc}(f_n(X)) \) is not a square in \( \mathbb{Q} \), and hence that the Galois group of \( f_n(X) \) is \( S_3 \). Thus \( K_n/\mathbb{Q} \) is a non-Galois real cubic extension. We place one last restriction on the parameter \( n \); we restrict \( n \) to have odd parity. This ensures the existence of the explicit unit \( \mu \in \mathcal{O}_K^\times \), distinct from \( \rho \), and introduced in Lemma 4.7 below.

Let
\[
\mathfrak{F} := \{K_n \mid n \text{ is an odd integer } \geq 5\}.
\]

Let \( \mathcal{I}_K \) denote the group of fractional ideals of \( K \in \mathfrak{F} \) and for a fractional ideal \( J \in \mathcal{I}_K \), let \([J]\) denote its ideal class. Let \( h_K \) denote the class number of \( K \). Our primary result is

**Theorem 4.1** Let \( r \not\equiv 0 \pmod{3} \) be a positive integer. There are infinitely many fields \( K \in \mathfrak{F} \) containing an ideal class of order \( r \).

We do not know whether or not the parametrization of \( \mathfrak{F} \) given by \( n \mapsto K_n \) is injective and so in proving Theorem 4.1 we do not attempt to show directly that there are infinitely many \( n \) such that \( K_n \) contains an ideal class of order \( r \). Instead we put most of our effort into first proving

**Proposition 4.2** Let \( r \not\equiv 0 \pmod{3} \) be an integer \( > 1 \). Then there is a field \( K \in \mathfrak{F} \) and an ideal \( J \in \mathcal{I}_K \) whose ideal class, \([J]\), has order \( r \).

Once Proposition 4.2 is established we have the following:

**Proof of Theorem 4.1** Since every class group contains the trivial class, the theorem holds for \( r = 1 \), so assume \( r > 1 \). The proposition tells us that the set \( S \) consisting of all \( K \in \mathfrak{F} \) containing an ideal class of order \( r \) is nonempty. If \( S \) was a finite set, then there would be a natural number \( \alpha \geq 1 \) and a field \( K \in S \) with class number \( h_K \) satisfying \( r^\alpha \mid h_K \) and \( r^{\alpha+1} \nmid h_{K'} \) for each \( K' \in S \). By the proposition there is a field \( L \in \mathfrak{F} \) and an ideal \( J \) of \( L \) whose class has order \( r^{\alpha+1} \). Hence \( L \) also contains a class of order \( r \), but since \( L \notin S \) we’ve reached a contradiction. We conclude that \( S \) is infinite. \( \square \)

To establish Proposition 4.2, we begin by establishing sufficient conditions for the ideal \( (2-\rho)\mathcal{O}_K \in \mathcal{I}_K \) to factor as an \( r \)th power of an ideal \( J \in \mathcal{I}_K \). This is accomplished in Proposition 4.11 and \([J]\), when \( J \) exists, serves as our candidate for
an ideal class of order \( r \). Note that in the previous two sections we accomplished this task with the help of the Galois group, \( G \), of our extensions. For if \( y^r = f_n(m) = \prod_{i=0}^{d}(m-\rho_i) \), where \( d = \deg(f) \), then \( G \) acts transitively on factors \((m-\rho_i)\) and takes prime ideals of \( K \) to prime ideals of \( K \). Since our cubic extension \( K/\mathbb{Q} \) is non-Galois, this technique is no longer available to us. Indeed, if \( \sigma \in \text{Gal}(L/\mathbb{Q}) \setminus \text{Gal}(L/K) \), where \( L \) is the Galois closure of \( K/\mathbb{Q} \), then \( \sigma|_K \) carries a prime ideal of \( K \) to a prime ideal of an isomorphic but distinct cubic extension \( K'/\mathbb{Q} \). At its core, however, this technique requires us to show that a prime ideal \( \mathfrak{P} \) dividing \((m-\rho_0)\mathcal{O}_K\) doesn’t also divide \( \prod_{i=1}^{d}(m-\rho_i)\mathcal{O}_K \), because this ensures that if \( \nu(\mathfrak{P}) \) is the exact power of \( \mathfrak{P} \) dividing \((m-\rho_0)\), then it is also the exact power of this ideal dividing \( y^r = f_n(m) \) and hence that \( r \mid \nu(\mathfrak{P}) \). This sufficiently motivates the following pair of lemmas building up to Proposition 4.11 and in regard to these we add that

\[
6n + 7 = f_n(2) = \prod_{i=0}^{2}(2-\rho_i) .
\] (4.2)

**Lemma 4.3** Let \( \rho_i \) \((i = 0, 1, 2)\) denote the roots of \( f_n(X) \) with \( \rho := \rho_0 \). Then

\[
(2-\rho_1)(2-\rho_2) = \rho^2 + (2+n)\rho + (4+3n) \in \mathcal{O}_{K_n} .
\]

**Proof** Since \( f_n(X) = X^3 + nX^2 + nX - 1 \), we have that \( \sum_{i=0}^{2}\rho_i = -n \) and \( \prod_{i=0}^{2}\rho_i = 1 \).

**Lemma 4.4** If \( p \) is a prime and there is a prime ideal \( \mathfrak{P} \mid p\mathcal{O}_K \) that is a common divisor of \((2-\rho)\mathcal{O}_K\) and \((2-\rho_1)(2-\rho_2)\mathcal{O}_K\), then \( p = 37 \).

**Proof** Since \( \rho \equiv 2 \mod \mathfrak{P} \), Lemma 4.3 implies that \((2-\rho_1)(2-\rho_2) \equiv 12 + 5n \). Also,

\[
0 = \rho^3 + n\rho^2 + n\rho - 1 \equiv 6n + 7 .
\]

These two congruences hold simultaneously only if \( p = 37 \).

We also need the following two results.

**Lemma 4.5** Let \( \mathfrak{P} \) be a prime ideal of \( \mathcal{O}_K \) with \( \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z} \). If \( \rho \equiv 2 \mod \mathfrak{P} \) and \( p \nmid \text{disc}(f_n) \), then \([\mathcal{O}_K/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}] = 1 \).

**Proof** Under the assumptions, every element of \( \mathcal{O}_K \) is congruent to a rational integer \( \mod \mathfrak{P} \).

**Lemma 4.6** If a prime \( p \) is a common divisor of \( 6n + 7 \) and \( \text{disc}(f_n) \), then \( p = 37 \) or \( p = 47 \).

**Proof** The congruences \( n^4 - 18n^2 - 27 \equiv \text{disc}(f_n) \equiv 0 \mod p \) and \( 6n + 7 \equiv 0 \mod p \) hold simultaneously only if \( p = 37 \) or \( p = 47 \).
4.1 A unit index

Lemma 4.7  The algebraic integer
\[ \mu := \left( \frac{n + 3}{2} \right) (1 + \rho) + \rho^2, \]
is a unit in \( \mathcal{O}_K \) with \( \mathcal{N}_K(\mu) = 1 \).

Proof Let \( a, b, c \in \mathbb{Z} \). A straightforward calculation shows that
\[ \mathcal{N}_K(a + b \rho + c \rho^2) = (a^2c + ac^2 - abc)n^2 - (2a^2c + a^2b - 2ac^2 - ab^2 - bc^2 + b^2c)n + (a^3 + b^3 + c^3 - 3abc). \]
Substituting \( a = b = (n + 3)/2 \) and \( c = 1 \) into this expression yields \( \mathcal{N}_K(\mu) = 1 \). Since \( \mu \in \mathcal{O}_K \), the lemma is established.

There doesn’t seem to be a similar expression for a unit of \( \mathcal{O}_K \) when \( n \) is even. If there were such an expression, then the regulator should be small and correspondingly the class number should be large. However, the class numbers when \( n \) is even tend to be much smaller than the class numbers when \( n \) is odd and of comparable size. For example, when \( n = 10^5 \), the class number is 1, while the class number is 3,637,896 when \( n = 10^5 + 1 \).

Lemma 4.8  The unit \( \mu \in \mathcal{O}_K^\times \) is totally positive, while the unit \( \rho \in \mathcal{O}_K^\times \) is neither totally positive nor totally negative.

Proof The unit \( \rho \) is a zero of \( f_n(X) \). As mentioned in the introduction, two of the zeros of \( f_n(X) \) are \( < -1 \), while the third is \( > 0 \). In particular, \( \rho \) is neither totally positive nor totally negative. Since \( \rho_i^3 + n\rho_i^2 + n\rho_i - 1 = 0 \), \( (i = 0, 1, 2) \), we see that \( n = (1 - \rho_i^3)/(\rho_i^2 + \rho_i) \). Substituting this expression for \( n \) into \( \mu_i = (\frac{a + 3}{2}) (1 + \rho_i) + \rho_i^2 \) yields
\[ \mu_i = (\rho_i + 1)^3/(2\rho_i). \quad (4.3) \]
The location of the \( \rho_i \) now confirms that each \( \mu_i \) is positive.

Let \( U := \langle -1, \mu, \rho \rangle \subset \mathcal{O}_K^\times \). We will need to know that \( [\mathcal{O}_K^\times : U] < \infty \). It will suffice to prove the following.

Lemma 4.9  The subset \( S := \{ \mu, \rho \} \subset \mathcal{O}_K^\times \) is multiplicatively independent.

Proof When \( n \geq 7 \), the zeros of \( f_n(X) \) satisfy \( \rho_0 \in (1 - n, 2 - n) \), \( \rho_1 \in (-1 - 3/n, -1 - 1/n) \) and \( \rho_2 \in (1/(n + 1), 1/n) \). The regulator, \( R \), of \( S \) is
\[ R = \left| \log |\mu_0| \log |\rho_1| - \log |\rho_0| \log |\mu_1| \right|. \]

For \( n \geq 7 \), we have that \( 1 + 1/n < |\rho_1| < 1 + 3/n \) and \( 1/n < |\rho_1 + 1| < 3/n \). Using the relation given in Eq. (4.3), we conclude that
\[ 1 > \frac{27}{2n^2(n + 1)} = (3/n)^3/(2(1 + 1/n)) \]
Relative ideal classes of arbitrary order

Choose prime ideals $\mathfrak{p}$

Proposition 4.10

Let $n \geq 5$ be an odd integer and let $\ell_1, \ell_2$ be primes such that $\ell_1 \ell_2 \mid (6n + 7)$. Let $p \neq 3$ be a prime such that

(i) $(2 \mid \ell_1)_p = 1$ and $(3 \mid \ell_1)_p \neq 1$,

(ii) $(2 \mid \ell_2)_p \neq 1$ and $(3 \mid \ell_2)_p \neq 1$.

Then $p \mid (\mathcal{O}_K^\times : U)$.

Proof

Choose prime ideals $\mathcal{L}_i \subset \mathcal{O}_K$, $(i = 1, 2)$, with $\mathcal{L}_i \cap \mathbb{Z} = \ell_i \mathbb{Z}$ and such that $\rho \equiv 2 \pmod{\mathcal{L}_i}$. Then by Eq. (4.3), $\mu \equiv 27/4 \pmod{\mathcal{L}_i}$. If $p \mid (\mathcal{O}_K^\times : U)$, then there is a unit $u \in \mathcal{O}_K^\times \setminus U$ and $a, b \in \mathbb{Z}$ with $0 \leq a, b < p$ and such that $u^p = \pm \rho^a \mu^b$. We remark that Lemma 4.6 guarantees that $\ell_i \nmid \text{disc}(f_n)$ and so Lemma 4.5 then guarantees that $[\mathcal{O}_K / \mathcal{L}_i : \mathbb{Z}/\ell_i \mathbb{Z}] = 1$.

If $p \neq 2$, then by making use of the fact that $[\mathcal{O}_K / \mathcal{L}_i : \mathbb{Z}/\ell_i \mathbb{Z}] = 1$ along with the congruences for $\rho$ and $\mu$, we find that $(2^a - 2b^3 \mid \ell_i)_p = 1$. Upon applying condition (i) we conclude that $p \mid b$ and hence that $b = 0$. Setting $b = 0$, we conclude that $(2^a \mid \ell_i)_p = 1$. Applying condition (ii) we find that $p \mid a$ and so $a = 0$. Hence $u^p = \pm 1$ and we reach the contradiction that $u = \pm 1 \in U$.

Hence $p = 2$ and $u^2 = \pm \rho^a \mu^b$. Since $\pm u^2 \mu^{-b}$ is either totally positive or totally negative and since $\rho$ is neither totally positive nor totally negative, $a = 0$. Furthermore, since both $\mu$ and $u^2$ are totally positive, we are forced to conclude that $u^2 = \mu^b$. If $b = 0$, then $u = \pm 1 \in U$; contradiction. Therefore $b = 1$ and $u^2 = \mu$. Since $\mu \equiv 27/4 \pmod{\mathcal{L}_2}$, we conclude that $(3 \mid \ell_2)_2 = 1$ and so contradict condition (ii).

Having exhausted the possibilities, we are forced to conclude that $p \nmid (\mathcal{O}_K^\times : U)$.  

\(\square\)
As in the previous sections, Bauer's theorem guarantees that, for each $p$, there are infinitely many $\ell_1$, $\ell_2$ satisfying conditions (i) and (ii).

### 4.2 The ideal classes

**Proposition 4.11** If $37 \nmid (6n + 7)$ and $6n + 7 = y^r$ for some $y \in \mathbb{Z}$, then there is an ideal $J \in \mathcal{I}_K$ such that $(2 - \rho)\mathcal{O}_K = J^r$.

**Proof** Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_K$ with $\mathfrak{P} \cap \mathbb{Z} := p\mathbb{Z}$ and with $\mathfrak{P} \mid (2 - \rho)\mathcal{O}_K$. Then $6n + 7 = f_n(2) = \prod_{i=0}^2(2 - \rho_i) \in \mathfrak{P}$. Hence $p \mid 6n + 7$ and since $37 \nmid 6n + 7$, we find that $\mathfrak{P} \mid (2 - \rho_1)(2 - \rho_2)\mathcal{O}_K$. Let $\mathfrak{P}^{\mathfrak{P}}$ denote the exact power of $\mathfrak{P}$ dividing $(2 - \rho)\mathcal{O}_K$. Then it must also be the exact power of $\mathfrak{P}$ dividing $y^r\mathcal{O}_K = (6n + 7)\mathcal{O}_K = \prod_{i=0}^2(2 - \rho_i)\mathcal{O}_K$. Hence $r \mid \nu_{\mathfrak{P}}$. We now set

$$J := \prod_{\mathfrak{P} \mid (2 - \rho)\mathcal{O}_K} \mathfrak{P}^{\nu_{\mathfrak{P}}/r},$$

and note that $J^r = (2 - \rho)\mathcal{O}_K$. $\square$

In Proposition 4.12 we add sufficient conditions to those of Proposition 4.11 to ensure that $[J]$ has order $r$.

**Proposition 4.12** Let $n \geq 5$ be an odd integer. If there is an integer $y$ with $(37 \times 47, y) = 1$ and such that $y^r = 6n + 7$, and if for each prime $p \mid r$ there are primes $\ell_i \mid (6n + 7)$ ($i = 1, 2, 3$) satisfying

(i) $(2 \mid \ell_1)_p = (37 \mid \ell_1)_p = 1$, and $(3 \mid \ell_1)_p \neq 1$,

(ii) $(37 \mid \ell_2)_p = 1$, $(2 \mid \ell_2)_p \neq 1$, and $(3 \mid \ell_2)_p \neq 1$,

(iii) $(37 \mid \ell_3)_p \neq 1$,

then $(2 - \rho) = J^r$ where $[J]$ has order $r$.

**Proof** Since the hypotheses of Proposition 4.11 hold, we have that $(2 - \rho) = J^r$ for some ideal $J \in \mathcal{I}_K$ and so the order of $[J]$ is $\leq r$. If it is strictly $< r$, then $(2 - \rho)$ is a prime power of a principal ideal for some prime $p \mid r$. Supposing this to be the case and writing $(2 - \rho) = (\beta)^p$, for some $\beta \in \mathcal{O}_K$, we have that $2 - \rho = u\beta^p$ for some $u \in \mathcal{O}_K^\times$. Since the hypotheses of Lemma 4.10 hold we have that $p \nmid [\mathcal{O}_K^\times : U]$. Writing $1 = gp + h[\mathcal{O}_K^\times : U]$ for some $g, h \in \mathbb{Z}$, we find that

$$2 - \rho = u\beta^p = u^{sp + h[\mathcal{O}_K^\times : U]}\beta^p = (\pm \rho^a\beta^b)^h(u^g\beta)^p = \pm \rho^a\mu^b(\beta')^p.$$

For notational convenience, replace $\beta'$ with $\beta$ and note that the same relation holds in the other two isomorphic cubic number fields to conclude that $2 - \rho_i = \pm \rho_i^a\mu_i^b\beta_i^p$ ($i = 0, 1, 2$).

Choose prime ideals $\mathcal{L}_i \subset \mathcal{O}_K$, ($i = 1, 2, 3$), with $\mathcal{L}_i \cap \mathbb{Z} = \ell_i\mathbb{Z}$ and such that $\rho \equiv 2 \pmod{\mathcal{L}_i}$. Then $\mu \equiv 27/4 \pmod{\mathcal{L}_i}$. On the one hand, $(2 - \rho_1)(2 - \rho_2) = (\rho_1\rho_2)^a(\mu_1\mu_2)^b(\beta_1\beta_2)^p = \rho^{-a}\mu^{-b}(\beta_1\beta_2)^p \equiv 2^{2b-a}3^{-3b}(\beta_1\beta_2)^p \pmod{\mathcal{L}_i}$. On
the other hand, \((2-\rho_1)(2-\rho_2) = \rho^2 + (2+n)\rho + (4+3n) = 5n + 12 \pmod{37} = 37/6 \pmod{37}_{L_i}\). Hence \(37 \equiv 2^{2b-a+3}3^{1-3b}(\beta_1\beta_2)^p \pmod{L_i}\). Lemma 4.6 guarantees that \(\ell_i \wp \text{disc}(\alpha_n)\) and so Lemma 4.5 then guarantees that \([\mathcal{O}_K/L_i : \mathbb{Z}/\ell_i\mathbb{Z}] = 1\). Thus \((2a-2b-1)^{3b-1}37 \mid \ell_i \pmod{p} = 1\). Applying condition (i), we conclude that \(3b-1 \equiv 0 \pmod{p}\). Using this result along with condition (ii), we find that \(a - 2b - 1 \equiv 0 \pmod{p}\). Since \(p\) divides \(3b - 1\) and \(a - 2b - 1\), we deduce that \((37 \mid \ell_3) \pmod{p} = 1\) and so contradict condition (iii). We conclude that \((2-\rho)\) is not a prime power of a principal ideal for any prime \(p \mid r\) and hence that \([J]\) has order \(r\).

Having established sufficient conditions for a field \(K \in \mathfrak{F}\) to possess an ideal class of arbitrary nontrivial order \(r \neq 0 \pmod{3}\), we now prove Proposition 4.2 by showing that for each such \(r\) there is a field \(K \in \mathfrak{F}\) satisfying these conditions.

For each prime \(p \mid r\), choose a triple of primes \(\{\ell_i,p\}_{i=1}^3\) satisfying conditions (i)–(iii) of Proposition 4.12 making sure never to choose \(2\) or \(3\), 37, or 47. Let \(s \in \mathbb{N}\) with \((s, 37 \times 47) = 1\) and such that \(s \left(\prod_{p\mid r} \prod_{i=1}^3 \ell_{i,p}\right) \equiv 1 \pmod{6}\). Set \(y := s \left(\prod_{p\mid r} \prod_{i=1}^3 \ell_{i,p}\right)\). If \(y^r \equiv 3 \pmod{4}\), then replace \(y\) with \(y^2\) so that \(y^r \equiv 1 \pmod{4}\). Since \(y^r \equiv 7 \pmod{6}\), there is an \(n \in \mathbb{N}\) such that \(y^r = 6n + 7\). Reducing this equation \(\pmod{4}\) shows that \(n\) is odd. Furthermore, since \(y \geq s \left(\prod_{p\mid r} \prod_{i=1}^3 \ell_{i,p}\right)\) and since \(s \in \mathbb{N}\) and \(\ell_i \neq 2, 3\) we deduce that \(y \geq 125\) and hence that \(n \geq 5\). We see that the hypotheses of Proposition 4.12 are satisfied and hence that there is an ideal \(J \in \mathcal{I}_{K_n}\) whose class \([J]\) has order \(r\).

5 Numerical results

In practice, despite the complicated proofs guaranteeing their existence, it is quite easy to find relative ideal classes of a desired order in these fields. This gap between theory and practice occurs even for similar results about imaginary quadratic fields. Here are the results of some easy calculations using PARI.

- For the 1000 sextics with \(100,000 \leq n < 101,000\), there are 44 fields with relative class number divisible by 5 and 282 with relative class number divisible by 7.
- For the 1000 quartics with \(10,000 \leq n < 11,000\), there are 116 fields with relative class number divisible by 3, and 402 fields with relative class number divisible by 5, and 23 with relative class number divisible by 7.
- For the family of non-Galois cubics, for the 1000 odd values of \(n\) with \(2,000,000 < n < 2,002,000\), there are 228 fields with class number divisible by 5 and 166 with class number divisible by 7.

As often seems to be the case in families of fields with explicit small units, the above numbers behave like what is expected from the Cohen–Lenstra heuristics, but with random modules rather than random modules modulo random subgroups corresponding...
to units. For example, the relative ideal class groups for the sextic fields are modules over the ring of sixth roots of unity, and, in the terminology of [1], they seem to satisfy laws for $u$-averages with $u = 0$.

Acknowledgements The authors thank the anonymous referee for several helpful suggestions, especially the algebraic proofs of Lemmas 2.5 and 3.5.

Declarations

Conflict of interest The authors declare that there are no conflicts of interest.

References

1. Cohen, H., Lenstra, H.W.: Heuristics on Class Groups of Number Fields, Number Theory Noordwijkerhout 1983, Proceedings, Springer Lecture Notes in Mathematics, vol. 1068, pp. 33–62
2. Gras, M.-N.: Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$. J. Reine Angew. Math. 277, 89–116 (1975)
3. Gras, M.-N.: Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$. Publ. Math. Besançon, pp. 1–79 (1977/1978)
4. Gras, M.-N.: Familles d’unités dans les extensions cycliques réelles de degré 6 de $\mathbb{Q}$. Publ. Math. Besançon, vol. 2, pp. 1–26 (1984/1985–1985/1986)
5. Hilbert, D.: Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen coefficienten. J. Reine Angew. Math. 110, 104–129 (1892)
6. Lang, S.: Algebra, Graduate Texts in Mathematics, vol. 211, 3rd edn. Springer, New York (2002)
7. Lazarus, A.J.: The class number and cyclotomy of simplest quartic fields. Ph.D. thesis, Berkeley (1989)
8. Nagell, T.: Über die Klassenzahl imaginär-quadratischer Zahlkörper. Abh. Math. Seminar Univ. Hamburg 1, 140–150 (1922)
9. Neukirch, J.: Algebraic Number Theory. Springer, New York (1999)
10. The PARI Group: PARI/GP version 2.11.4. Univ. Bordeaux (2022) http://pari.math.u-bordeaux.fr/

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.