Properties of Class Groups of a Family of Cyclic Cubic Fields

Jaclyn Lang

July 26, 2009

1 Introduction

In this paper, we consider the class groups of totally real cyclic cubic extensions of $\mathbb{Q}$. To fix notation, let

$$f(x) = x^3 + mx^2 - (m+3)x + 1$$

with $m \geq 0$ and $m \not\equiv 3 \pmod 9$, let ρ be a zero of $f(x)$ and $K = \mathbb{Q}(\rho)$. These fields are known as Shanks' simplest cubic fields.

Shanks computed the discriminant of the polynomial, fundamental units of the field, and the regulator [15]. He also used computational methods to investigate the class number of K when the discriminant is small. Louboutin determined the exact number of simplest cubic fields with class number one and found exactly which ones have class number equal to a power of three [10]. In doing so Louboutin finds, for each m, a lower bound for the class number of the simplest cubic field generated by $x^3 + mx^2 - (m+3)x + 1$. Thomas [17] solved an associated family of Thue equations when m is large, obtained by homogenizing $f(x)$ and setting it equal to ± 1.

Washington [19] also studied these fields. His first main result is a generalization of a result of Uchida [18] about the divisibility of class numbers of cubic number fields. His other main result, which is independent from the first result, relates the 2-part of the class group of the simplest cubic fields to the rank of a particular elliptic curve by proving the following theorem.

Theorem 1. *Let E be the elliptic curve defined by $y^2 = f(x)$. There is an exact sequence*

$$1 \to E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \to C_2 \to Ш_2 \to 1,$$

where E° is the connected component of the identity of E, C_2 is the points of order less than or equal to 2 in the ideal class group of K, and $Ш_2$ is the Tate-Shafarevich group of K.

This result implies that $\mathrm{rk}(E(\mathbb{Q})) \leq 1 + \mathrm{rk}_2\,(C_2)$, where $\mathrm{rk}_2\,(C_2)$ is the rank of C_2 as a $\mathbb{Z}/2\mathbb{Z}$-vector space. Hence, he obtains an upper bound on the rank of the elliptic curve and a lower bound on the 2-rank of the class group, depending on the information that is known.

The goal of this paper is to explain Washington's results. In the first section we provide background information needed to understand the theorems in [19]. In particular, we review the necessary information about the theory of discrete valuations and p-adic numbers, class field theory, elliptic curves, and Dedekind zeta functions. Section 3 is about Washington's results. In Section 3.1 we establish some facts about the simplest cubic fields are needed in the rest of the paper. We prove a result about class number divisibility of cubic fields in Section 3.2. This is followed by the proof of Theorem 1 in Section 3.3.2. Finally, we investigate quartic fields that are associated with the simplest cubic fields in a particular way in Section 3.4. The material in this section relies on Theorem 1, and it is related to a theorem of Heilbronn. In particular, Heilbronn established a connection between the number of quartic fields associated with a cubic number field L and the number of elements of order two in the class group of L [6]. We use Theorem 1 to determine these fields explicitly in some special cases.

We conclude with some remarks about why the simplest cubic fields are useful. In particular, we analyze the properties of these fields that are necessary to the results examined in this paper.

2 Preliminary material

2.1 Valuations and completions of extensions of $\mathbb{Q}$

Let K be a field. A discrete valuation on K is a group homomorphism $v : K^\times \to \mathbb{Z}$ such that $v(x+y) \geq \inf\{v(x), v(y)\}$ for all $x, y \in K^\times$. We extend the valuation to 0 by setting $v(0) = \infty$. To each valuation on K, we associate a ring, called the valuation ring of v, given by

$$R_v = \{x \in K : v(x) \geq 0\}.$$

It is easy to show that R_v is an integral domain with quotient field K. In fact, R_v is a local ring with unique maximal ideal, called the valuation ideal,

$$\mathfrak{p}_v = \{x \in K : v(x) > 0\}.$$

Each valuation induces an absolute value on K. Let $0 < \lambda < 1$ and define $|\cdot|_v : K \to \mathbb{R}$ by

$$|x|_v = \lambda^{v(x)}.$$

Note that since valuations are additive, these absolute values are multiplicative. We say that two absolute values are equivalent if they induce the same topology on K. It follows that two absolute values $|\cdot|_1, |\cdot|_2$ are equivalent if and only if there is some $s \in \mathbb{R}^+$ such that $|\cdot|_1 = |\cdot|_2^s$. Therefore, the value of λ chosen above does not change the equivalence class of the absolute value.

For example, let K be a number field and $\mathfrak{p}$ a prime ideal in K. Define $v_\mathfrak{p}(\alpha)$ to be the power of $\mathfrak{p}$ appearing in the prime factorization of $\langle \alpha \rangle$. That is, if

$$\langle \alpha \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

with the $\mathfrak{p}_i$ distinct primes and the $e_i \in \mathbb{Z}$, then $v_{\mathfrak{p}_i}(\alpha) = e_i$. Using the properties of exponents, it is easy to see that $v_\mathfrak{p}$ defines a group homomorphism. The fact that $v(x+y) \geq \inf\{v(x), v(y)\}$ for all $x, y \in K^\times$ also follows from laws of exponents.

Let $K/\mathbb{Q}$ be a degree n extension. The $\mathfrak{p}$-adic absolute value is given by

$$|x|_\mathfrak{p} = \begin{cases} \left(\frac{1}{N(\mathfrak{p})^{v_\mathfrak{p}(x)}}\right)^{1/n} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0 \end{cases}$$

where $N(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}]$ is the norm of the ideal $\mathfrak{p}$. Note that in this case, the chosen value for λ is $N(\mathfrak{p})^{-1/n}$. (As $N(\mathfrak{p}) > 1$, it follows that $0 < N(\mathfrak{p})^{-1/n} < 1$.) Let $K_\mathfrak{p}$ be the completion of K with respect to the absolute value $|\cdot|_\mathfrak{p}$. Then

$$\mathcal{O}_{K_\mathfrak{p}} = \{x \in \mathcal{O}_{K_\mathfrak{p}} : v_\mathfrak{p}(x) \geq 0\},$$

so the ring of integers is the valuation ring of $v_\mathfrak{p}$. Furthermore, the valuation ideal is $\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$. If $\mathfrak{p}$ is the only prime ideal of $\mathcal{O}_K$ lying over p, we will sometimes write $K_\mathfrak{p} = K_p$.

The case when $K = \mathbb{Q}$ is of particular interest. Let p a rational prime. Since $[\mathbb{Q} : \mathbb{Q}] = 1$ and $N(\langle p \rangle) = p$, the p-adic absolute value, $|\cdot|_p : \mathbb{Q} \to \mathbb{Z}$ is given by

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is the field of p-adic numbers, denoted $\mathbb{Q}_p$. Every element of $\mathbb{Q}_p$ can be represented by a Laurent series that converges under $|\cdot|_p$. That is, every element can be written in the form

$$x = a_{-m}p^{-m} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots ,$$

where $m \geq 0$ and $0 \leq a_i \leq p - 1$ for all i. This is called the p-adic expansion of x. The ring of integers of $\mathbb{Q}_p$, denoted $\mathbb{Z}_p$, consists precisely of those series such that $m = 0$. That is, the integers in $\mathbb{Q}_p$ have no negative powers of p in their p-adic expansion.

A critical property of p-adic numbers is their connection with $\mathbb{Z}/p\mathbb{Z}$. The following generalization of a result of Hensel, which can be found in [13], is useful in determining zeros of integral p-adic polynomials from zeros of polynomials over $\mathbb{Z}/p\mathbb{Z}$. Let $\mathcal{O}_K$ be the ring of integers of a field K, which is complete with respect to a nonarchimedean absolute value. Let $\mathfrak{p}$ be the valuation ideal in $\mathcal{O}_K$. A polynomial $f(x) \in \mathcal{O}_K[x]$ is called primitive if $f(x) \not\equiv 0 \pmod{\mathfrak{p}}$.

Theorem 2. *If a primitive polynomial $f(x) \in \mathcal{O}_K[x]$ admits modulo $\mathfrak{p}$ a factorization*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \pmod{\mathfrak{p}}$$

into relatively prime polynomials $\overline{g}, \overline{h} \in \mathcal{O}_K/\mathfrak{p}[x]$, then $f(x)$ admits a factorization

$$f(x) = g(x)h(x)$$

into polynomials $g, h \in \mathcal{O}_K[x]$ such that $\deg(g) = \deg(\overline{g})$ *and*

$$g(x) \equiv \overline{g}(x) \pmod{\mathfrak{p}}$$

and

$$h(x) \equiv \overline{h}(x) \pmod{\mathfrak{p}}.$$

The following corollary of Theorem 2 will be useful in the proof of Proposition 31 in Section 3.3.2.

Corollary 3. *For all primes $p \neq 2$,*

$$\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2 \cong \mathbb{Z}/2\mathbb{Z}.$$

Proof. First we show that $\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2$ is nontrivial. Suppose that $\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2$ is trivial. Then for every $\alpha \in \mathbb{Z}_p^\times$ the polynomial $x^2 - \alpha$ is reducible over $\mathbb{Z}_p^\times$. By reducing all elements in $\mathbb{Z}_p^\times$ modulo p, it follows that $x^2 - a$ is reducible over $(\mathbb{Z}/p\mathbb{Z})^\times$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. However, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$. Hence, for $p > 2$ there are exactly $(p-1)/2$ squares in $(\mathbb{Z}/p\mathbb{Z})^\times$. It must be that $p = 2$. Therefore, if $p > 2$ then $\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2$ is nontrivial.

It suffices to show that if $a, b \in \mathbb{Z}_p^\times - \left(\mathbb{Z}_p^\times\right)^2$ then $ab \in \left(\mathbb{Z}_p^\times\right)^2$. Let $a, b \in \mathbb{Z}_p^\times - \left(\mathbb{Z}_p^\times\right)^2$, so $x^2 - a, x^2 - b$ are irreducible over $\mathbb{Z}_p$. Therefore, $x^2 - \overline{a}, x^2 - \overline{b}$ are irreducible modulo p, otherwise Theorem 2 gives a contradiction. Hence, $\overline{a}, \overline{b} \in (\mathbb{Z}/p\mathbb{Z})^\times - \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2$.

As there are exactly $(p-1)/2$ squares in $(\mathbb{Z}/p\mathbb{Z})^\times$,

$$|(\mathbb{Z}/p\mathbb{Z})^\times / \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2| = \frac{p-1}{(p-1)/2} = 2,$$

so $(\mathbb{Z}/p\mathbb{Z})^\times / \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2 \cong \mathbb{Z}/2\mathbb{Z}$. Thus, $\overline{a}, \overline{b} \in (\mathbb{Z}/p\mathbb{Z})^\times - \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2$ implies $\overline{ab} \in \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2$. Therefore $x^2 - \overline{ab}$ has a root in $\mathbb{Z}/p\mathbb{Z}$. By Theorem 2 there is a unique $\alpha \in \mathbb{Z}_p^\times$ such that $\alpha^2 - ab = 0$ and $\alpha \equiv ab \pmod{p}$. Therefore, $ab = \alpha^2 \in \left(\mathbb{Z}_p^\times\right)^2$, as desired. □

Next we relate the absolute values on $\mathbb{Q}$ to the absolute values on a number field K. If $|\cdot|_{\mathbb{Q}}$ is an absolute value on $\mathbb{Q}$ and $|\cdot|_K$ is an absolute value on K, we say that $|\cdot|_K$ is an extension of $|\cdot|_{\mathbb{Q}}$ if for all $x \in \mathbb{Q}$, $|x|_K = |x|_{\mathbb{Q}}$. The extensions of the p-adic absolute values on $\mathbb{Q}$ are related to how primes of $\mathbb{Z}$ factor in K. In particular, if

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

for distinct prime ideals $\mathfrak{p}_i$, then each of $|\cdot|_{\mathfrak{p}_i}$ is an extension of $|\cdot|_p$ and $|\cdot|_{\mathfrak{p}_i} = |\cdot|_{\mathfrak{p}_j}$ only if $i = j$. Furthermore, these are the only extensions of $|\cdot|_p$ to K. A theorem of Ostrowski, see [9], that states that, up to equivalence, the only absolute values on $\mathbb{Q}$ are $|\cdot|_p$ for p prime and the Euclidean absolute value $|\cdot|$, sometimes written $|\cdot|_\infty$. In light of the information about extensions given above, it follows that the only absolute values on a number field K, up to equivalence, are $|\cdot|_{\mathfrak{p}}$ for prime ideals $\mathfrak{p}$ and extensions of $|\cdot|_\infty$. Any other absolute value on K would restrict to an absolute value on $\mathbb{Q}$ that must be equivalent to some $|\cdot|_p$ or $|\cdot|_\infty$. The following theorem, reworded from [13, page 163], gives more information about the correspondence between absolute values on K and $\mathbb{Q}$.

Theorem 4. *Let L/K be an extension generated by the zero α of the irreducible polynomial $f(x) \in K[x]$. Let $|\cdot|_K$ be an absolute value on K. Then the absolute values $|\cdot|_{L_1}, \dots, |\cdot|_{L_r}$ extending $|\cdot|_K$ to L are in one-to-one correspondence with the irreducible factors $f_1(x), \dots, f_r(x)$ in the decomposition*

$$f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}$$

of $f(x)$ over the completion of K with respect to $|\cdot|_K$.

We use the following well-known theorem to determine how rational primes split in K. A proof can be found in [16].

Theorem 5. *Let K be a number field of degree n with ring of integers $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Given a rational prime p, suppose the minimal polynomial $f(x)$ of α over $\mathbb{Q}$ gives rise to the factorization into irreducibles over $\mathbb{Z}/p\mathbb{Z}$*

$$\bar{f}(x) = \bar{f}_1(x)^{e_1} \cdots \bar{f}_r(x)^{e_r},$$

where the bar denotes the natural map $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$. Then if $f_i(x) \in \mathbb{Z}[x]$ is any polynomial mapping to $\bar{f}_i(x)$, the ideal

$$\mathfrak{p}_i = \langle p, f_i(\alpha) \rangle$$

is prime and the prime factorization of $\langle p \rangle$ in $\mathcal{O}_K$ is

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Having examined how valuations on $\mathbb{Q}$ extend to valuations on number fields, we now turn to finite extensions of $\mathbb{Q}_p$. Let α be an algebraic number, $K = \mathbb{Q}(\alpha)$, and $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ lying over p in $\mathbb{Z}$. One might ask how $K_\mathfrak{p}$ is related to $\mathbb{Q}_p(\alpha)$. We will consider the case when p does not split in K. The following theorem, from [4], is useful in addressing this question.

Theorem 6. *Let F be a complete field with respect to a discrete valuation v and L a finite extension of F. Then there is precisely one extension w on L of the valuation v and $w = \frac{1}{f} v \circ N_{L/F}$, where f is the inertial degree of w over v. The field L is complete with respect to w.*

To use this theorem, we first need to establish the following diagram in the case that p does not split in K.

$$\begin{tikzcd}
& K_\mathfrak{p} \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}_p \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

The containments $K \subset K_{\mathfrak{p}}$ and $\mathbb{Q} \subset \mathbb{Q}_p$ are clear since every field is contained in its completion. Also, $\mathbb{Q} \subseteq K$ by definition of K. Next we show that K contains an isomorphic copy of $\mathbb{Q}_p$. Let $x \in \mathbb{Q}_p$. Then there is a Cauchy sequence $\{x_n\}$ in $\mathbb{Q}$ such that $\lim_{n\to\infty} x_n = x$ with respect to $|\cdot|_p$. Now, $\{x_n\}$ can be viewed as a Cauchy sequence in K. As $|\cdot|_{\mathfrak{p}}$ is an extension of $|\cdot|_p$, it follows that $\lim_{n\to\infty} x_n = x$ with respect to $|\cdot|_{\mathfrak{p}}$ as well. Hence, x may be identified with the limit of $\{x_n\}$ in $K_{\mathfrak{p}}$.

If p does not split in K, there is a unique copy of $\mathbb{Q}_p$ in $K_{\mathfrak{p}}$. This is due to the fact that there is only one prime lying over p in K. Hence we may view $\mathbb{Q}_p(\alpha) \subseteq K_{\mathfrak{p}}$. By restricting the valuation $v_{\mathfrak{p}}$ to $\mathbb{Q}_p(\alpha)$, we obtain a valuation on $\mathbb{Q}_p(\alpha)$ that is an extension of v_p. By Theorem 6, such a valuation is unique, and $\mathbb{Q}_p(\alpha)$ is complete with respect to this valuation. But $K_{\mathfrak{p}}$ is by definition the smallest complete field with respect to $v_{\mathfrak{p}}$ containing K. Hence, it must be that $K_{\mathfrak{p}} = \mathbb{Q}_p(\alpha)$ if p does not split in K.

2.2 Results from class field theory

In general, it is difficult to obtain information about the class group of a number field. Class field theory provides a correspondence between certain extensions of a number field and the subgroups of the class group of that number field. The material for this section can be found in the Introduction of [12].

Throughout this section, let K be a number field and C the ideal class group of K. We say that an extension L/K is unramified if every prime of K is unramified in L. Recall that there are three kinds of primes, namely prime ideals, real valuations, and complex valuations. If $\mathfrak{p}$ is a prime ideal, then it is ramified if for some $r \geq 2, \mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{q}^r$, where $\mathfrak{q}$ is a prime ideal of L. Now let $\mathfrak{p}$ be an infinite prime of K corresponding to a real embedding $\sigma : K \to \mathbb{R}$. Then $\mathfrak{p}$ ramifies in L if σ lifts to a complex embedding of $L \to \mathbb{C}$. Otherwise, $\mathfrak{p}$ splits in L. Complex valuations always split in extension fields.

Definition 1. *Let H be a subgroup of C. An unramified abelian extension L of K is a class field for H if a prime $\mathfrak{p}$ of K splits completely in L if and only if $[\mathfrak{p}] \in H$. The class field of $\{[\mathcal{O}_K]\}$ is called the Hilbert class field of K.*

Note that the Hilbert class field is the maximal abelian unramified extension of K. A priori, it is not clear that the Hilbert class field (or any class field for that matter) is unique. The following theorem addresses this concern.

Theorem 7. *Let H be a subgroup of C. Then there is a unique class field of H. Furthermore, every unramified abelian extension of K is the class field of a subgroup of C. If L is the class field of H, then*

$$\mathrm{Gal}(L/K) \cong C/H.$$

Finally, if $\mathfrak{p}$ is a prime ideal of K, then the inertial degree of $\mathfrak{p}$ in L is equal to the order of $[\mathfrak{p}]H$ in C/H.

The proof of this theorem can be found in [12]. The following corollary will be useful in proving Proposition 31 in Section 3.3.2.

Corollary 8. *Let L be an unramified abelian extension of a number field K. Then every principal prime ideal of K splits completely in L.*

Proof. By Theorem 7, L is the class field of a subgroup H of C. Since $[\mathcal{O}_K]$ is the identity element in C, it follows that $[\mathcal{O}_K] \in H$. If $\mathfrak{p}$ is a principal prime ideal of K, then $[\mathfrak{p}] = [\mathcal{O}_K]$, so $[\mathfrak{p}] \in H$. By Definition 1 it follows that $\mathfrak{p}$ splits completely in L, as desired. □

We would like to extend this correspondence to ramified extensions of K. In order to do this, we need to develop some notation. Define a modulus of K to be a formal product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is a product of prime ideals in $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a (possibly empty) product of infinite primes. We allow the primes appearing in $\mathfrak{m}_0$ to have multiplicity greater than one, but the primes appearing in $\mathfrak{m}_\infty$ appear at most once. Let $I^{\mathfrak{m}}$ be the group of fractional ideals generated by the nonzero prime ideals of $\mathcal{O}_K$ not dividing $\mathfrak{m}_0$. Consider the subgroup of $I^{\mathfrak{m}}$ generated by the principal ideals $\langle a \rangle$, where $a \in K^\times$ satisfies

- for all real primes σ dividing $\mathfrak{m}$, $\sigma(a) > 0$ and
- for all prime ideals $\mathfrak{p} \mid \mathfrak{m}$, the number of times that $\mathfrak{p}$ divides $a - 1$ is greater than or equal to the number of times that $\mathfrak{p}$ divides $\mathfrak{m}_0$.

Call this subgroup $P^{\mathfrak{m}}$ and define $C_{\mathfrak{m}} = I^{\mathfrak{m}}/P^{\mathfrak{m}}$. These groups are called the ray class groups of K.

Note that if $\mathfrak{m} = 1$, so $\mathfrak{m}$ is an empty product of primes, then $I^{\mathfrak{m}}$ is the group of all fractional ideals of K. Also, $P^{\mathfrak{m}}$ is exactly the subgroup of all principal ideals. In this case, $C_{\mathfrak{m}} = C$ is the class group of K. The wide class number of K, also known as the class number, is $|C|$. Another important example of a ray class group requires the following definition.

Definition 2. *Let K be a number field. If all infinite primes are real, then K is a totally real field. If for some $\alpha \in K, \sigma(\alpha) \in \mathbb{R}^+$ for all embeddings $\sigma : K \to \mathbb{Q}$ then α is said to be totally positive.*

Now let $\mathfrak{m} = \mathfrak{m}_\infty$ be the product of all real infinite primes of K. Once again, $I^{\mathfrak{m}}$ is the group of all fractional ideals of K. In this case, $P^{\mathfrak{m}}$ is the subgroup of all principal ideals that can be generated by a totally positive element of K. This ray class group is known as the narrow class group, and $|C_{\mathfrak{m}}|$ is the narrow class number of K. Note that $P^{\mathfrak{m}}$ may not contain all principal ideals.

Therefore, the equivalence classes of $C_{\mathfrak{m}}$ are smaller than those in C and thus $|C_{\mathfrak{m}}| \geq |C|$. The case when equality holds is of interest and will be discussed later.

We are now ready to give a more general definition of a class field as well as a more general correspondence theorem.

Definition 3. *Fix a modulus $\mathfrak{m}$ of K and let H be a subgroup of $C_{\mathfrak{m}}$. An abelian extension L of K is a class field for H if a prime ideal $\mathfrak{p}$ of K splits completely in L if and only if $[\mathfrak{p}] \in H$.*

In addition to giving a more general correspondence between the subgroups of $C_{\mathfrak{m}}$ and the extensions of K, the following theorem shows that the more general definition of class field reduces to Definition 1 if the modulus $\mathfrak{m}$ is taken to be the empty product.

Theorem 9. *Fix a modulus $\mathfrak{m}$ of K. For each subgroup of $C_{\mathfrak{m}}$ there is a unique class field. Furthermore, every abelian extension of K is the class field of a subgroup of some ray class group. If L is the class field of a subgroup H of $C_{\mathfrak{m}}$, then*

$$\mathrm{Gal}(L/K) \cong C_{\mathfrak{m}}/H.$$

Finally, the prime ideals $\mathfrak{p}$ of K not dividing $\mathfrak{m}$ are unramified in L and the inertial degree of $\mathfrak{p}$ is equal to the order of $[\mathfrak{p}]H$ in $C_{\mathfrak{m}}/H$.

Again the proof of this theorem can be found in [12]. The following corollary will be used in the proof of Proposition 31.

Corollary 10. *Let $\mathfrak{m}$ be the product of all infinite primes of K and suppose that $C_{\mathfrak{m}} = C$. If L/K is an abelian extension that is unramified at all finite primes, then this extension is also unramified at all infinite primes.*

Proof. Let F be the class field of the trivial subgroup of $C_{\mathfrak{m}}$. (Theorem 9 guarantees the existence and uniqueness of F.) Then F contains all abelian extensions of K that are unramified at all finite primes. In particular, F contains the Hilbert class field of K, call this H_K. But

$$[F : K] = |C_{\mathfrak{m}}| = |C| = [H_K : K],$$

so we must have $F = H_K$. Therefore, F is an unramified extension since H_K is. It follows that every intermediate field of F/K is also unramified, so L is unramified at the infinite primes, as claimed. □

Now we return to the question of when the narrow and wide class groups are the same. By definition, this occurs if and only if every principal ideal of $\mathcal{O}_K$ can be generated by a totally positive element.

Definition 4. *Let K be a totally real number field of degree n over $\mathbb{Q}$ and $\sigma_1, \ldots, \sigma_n : K \to \mathbb{R}$ be the embeddings of K. The signature of $\alpha \in K^\times$ is an n-tuple of $+$ and $-$, where the i-th coordinate is $+$ if $\sigma_i(\alpha) > 0$ and $-$ if $\sigma_i(\alpha) < 0$.*

Totally positive elements are exactly those whose signatures have a $+$ in every coordinate. Note that when multiplying two elements, their signatures also multiply coordinatewise by the usual rules. Namely, $+ \cdot + = +, + \cdot - = -$, and $- \cdot - = +$. Therefore multiplying two elements with the same signature yields a totally positive element. By examining the signatures of units of $\mathcal{O}_K$, we can decide when the narrow and wide class numbers are equal.

Lemma 11. *If every signature of an element in $\mathcal{O}_K$ can be obtained from unit of $\mathcal{O}_K$, then the narrow and wide class numbers of K are equal.*

Proof. Consider the principal ideal $\langle \alpha \rangle$ for some $\alpha \in K^\times$. By assumption, there is a unit $\varepsilon \in \mathcal{O}_K^\times$ with the same signature as that of α. Therefore, $\varepsilon\alpha$ is totally positive and generates $\langle \alpha \rangle$. Hence, every principal ideal can be generated by a totally positive element and so the narrow and wide class numbers of K are equal, as claimed. □

These results indicate that it is useful to know the primes at which an extension is ramified. The following lemma will prove useful in answering this question about quadratic extensions. An outline of the proof can be found in [21, page 182].

Theorem 12. *Let L be a number field in which 2 is inert and let $\alpha \in L$ be relatively prime to 2. Then, $L\left(\sqrt{\alpha}/L\right)$ is unramified at the prime above 2 if and only if α is congruent to a square modulo 4. This extension is unramified at the other finite primes of L if and only if the (fractional) ideal $\langle \alpha \rangle$ is the square of an ideal of L. If L is totally real, then the extension is unramified at the infinite primes if and only if α is totally positive.*

2.3 Elliptic curves

Throughout this section, let E be an elliptic curve defined over $\mathbb{Q}$ given by

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma),$$

with α, β, γ distinct. It is a well known fact that the rational points on an elliptic curve form a finitely generated abelian group. We assume the reader is familiar with the operation in this group. Throughout the paper the identity element is denoted ∞ and a nonidentity point $P \in E(\mathbb{Q})$ is represented as $P = (x, y)$. In writing $P = (x, y)$ we are assuming that $P \neq \infty$. We write $E[2]$ for the 2-torsion points of E over some fixed algebraic closure $\overline{\mathbb{Q}}$. In particular, $E[2]$ is not necessarily contained in $E(\mathbb{Q})$. It follows from the definition of addition on an elliptic curve that the only 2-torsion points are

$$E[2] = \{(\alpha, 0), (\beta, 0), (\gamma, 0), \infty\}.$$

Let $K/\mathbb{Q}$ be a finite extension and let $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then for a point $P = (x, y) \in E(K)$, we define

$$P^\sigma = (\sigma(x), \sigma(y)).$$

Using the fact that the formulae for addition on an elliptic curve are rational expressions in the coordinates of the points and the fact that σ is a field homomorphism, it follows that

$$(P_1 + P_2)^\sigma = P_1^\sigma + P_2^\sigma.$$

For any field K, we write $2E(K) = \{P \in E(K) : P = 2Q \text{ for some } Q \in E(K)\}$. The following results characterize the points in $2E(K)$. Proposition 13 is a generalization of a result found in [19]. Proposition 15 can be found in [8].

Proposition 13. *Let K be a field of characteristic not equal to 2 or 3. Let $f(x) \in K[x]$ be a cubic polynomial with distinct zeros and let E be the elliptic curve $y^2 = f(x)$. Let $(d, e) \in E(K)$ and let*

$$f(x + d) = ax^3 + bx^2 + cx + e^2,$$

with $a, b, c, e \in K$. Then $(d, e) \in 2E(K)$ if and only if

$$q(x) = x^4 - 2bx^2 - 8aex + b^2 - 4ac$$

has a zero in K.

Proof. Assume that $(d, e) \in 2E(K)$. Then there is some $(x_0, y_0) \in E(K)$ such that $2\,(x_0, y_0) = (d, e)$. By definition of addition on the elliptic curve, there is a line, ℓ, through $(d, -e)$ that is tangent to $y^2 = f(x)$ at (x_0, y_0). The formula for ℓ is $y + e = m(x - d)$ for some slope m. To see that $m \in K$, recall that $m = \frac{y_0+e}{x_0-d}$ and $x_0, y_0, d, e \in K$. Note that if $x_0 = d$, then ℓ is a vertical line and so $(d, e) = 2\,(x_0, y_0) = \infty$, a contradiction. Solving for y and substituting this expression into $y^2 = f(x)$ yields $(m(x - d) - e)^2 = f(x)$. Evaluating this equation at $x + d$ gives

$$(mx - e)^2 = f(x + d) = ax^3 + bx^2 + cx + e^2. \tag{1}$$

Note that the solutions to this equation are $x_0 - d$ and 0 since by construction the solutions to this equation are the points that lie on both ℓ and the elliptic curve. Since ℓ is tangent to the elliptic curve at (x_0, y_0), Equation (1) has a double root at $x_0 - d$. Therefore,

$$ax^3 + bx^2 + cx + e^2 - (mx - e)^2 = ax\,(x - (x_0 - d))^2$$

which reduces to

$$\left(\frac{b-m^2}{a}\right)x+\left(\frac{c+2me}{a}\right)=-2\left(x_0-d\right)x+\left(x_0-d\right)^2.$$

Equating the linear coefficients and solving for x_0 gives $x_0=\frac{1}{2a}\left(m^2-b\right)+d$. Substituting this expression into the formula for the line $y=m(x-d)-e$ gives $y_0=\frac{m}{2a}\left(m^2-b\right)-e$.

Differentiating $y^2=f(x)$ with respect to x, we get

$$2y\frac{dy}{dx}=3x^2+2bx+c.$$

Since ℓ is tangent to the elliptic curve at (x_0,y_0), it follows that $\frac{dy}{dx}|_{(x_0,y_0)}=m$. Hence,

$$2y_0m=3x_0^2+2bx_0+c.$$

Substituting the above expressions for x_0 and y_0 and simplifying we obtain

$$0=m^4-2bm^2-8aem+b^2-4ac=q(m).$$

Therefore, if $(d,e)\in 2E(K)$ then $m\in K$ is a zero of $q(x)$, as desired.

Now suppose that $m\in K$ is a zero of $q(x)$. Let

$$x_0=\frac{1}{2a}\left(m^2-b\right)+d \quad\text{and}\quad y_0=\frac{m}{2a}\left(m^2-b\right)-e.$$

Note that $x_0,y_0\in K$, since $a,b,d,e,m\in K$. We will show that $(x_0,y_0)\in E(K)$ and $2\left(x_0,y_0\right)=(d,e)$. Using the fact that m is a zero of $q(x)$ we obtain

$$\left(m^2-b\right)^2=m^4-2bm^2+b^2=8aem+4ac.$$

This can be used to show that (x_0,y_0) satisfies $y^2=f(x)$, so $(x_0,y_0)\in E(K)$.

Now, let $y=Mx+B$ be the line through (x_0,y_0) that is tangent to $y^2=f(x)$. The slope M is equal to the derivative of the elliptic curve at the point (x_0,y_0) and so $3x_0^2+2bx_0+c=2y_0M$. Substituting in the expressions for x_0 and y_0, then using the fact that $0=m^4-2bm^2-8aem+b^2-4ac$, we get $M=m$. Similarly, by substituting the formulae for x_0 and y_0 into the equation $y=mx+B$, we obtain $B=-md-e$.

Therefore the line $y=Mx+B$ is tangent to (x_0,y_0) and intersects the elliptic curve at $(d,-e)$. It follows that $(x_0,y_0)\in E(K)$ satisfies $2\left(x_0,y_0\right)=(d,e)$, as desired. □

Note that the proof gives rational expressions for x_0 and y_0 in terms of m and elements of $\mathbb{Q}$. Therefore, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the zeros of $q(x)$ induces an action on the points (x_0, y_0) satisfying $2\,(x_0, y_0) = (d, e)$. Let $m_1, m_2, m_3, m_4 \in \overline{\mathbb{Q}}$ be the zeros of $q(x)$ and (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) be the corresponding solutions to $2\,(x_i, y_i) = (d, e)$. Recall that $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the m_i. If $\sigma\,(m_i) = m_j$, then $\sigma\,(x_i, y_i) = (x_j, y_j)$. Furthermore, the above proof shows that $\mathbb{Q}\,(m_i) = \mathbb{Q}\,(x_i, y_i)$ for $1 \leq i \leq 4$.

Before giving another characterization of the points in $2E(K)$, we make some observations about the relationship between the cubic polynomial $f(x)$ and the associated quartic polynomials $q(x)$. Recall that the the cubic resolvent of a quartic polynomial of the form $q(x) = x^4 + ay^2 + by + c$ is

$$h(x) = x^3 + 2ax^2 + \left(a^2 - 4c\right) x - b^2.$$

One can show that if u, v, w are the zeros of $h(x)$, then $\frac{1}{2}\left(\sqrt{u} \pm \left(\sqrt{v} + \sqrt{w}\right)\right)$ and $\frac{1}{2}\left(-\sqrt{u} \pm \left(\sqrt{v} - \sqrt{w}\right)\right)$ are the zeros of $q(x)$. Furthermore, this relationship between the zeros can be used to show that $q(x)$ and $h(x)$ have the same discriminant.

With notation as in Proposition 13, we see that the cubic resolvent of $q(x)$ is

$$\begin{aligned} x^3 + 2(-2b)x^2 + \left((2b)^2 - 4\left(b^2 - 4c\right)\right) x - (-8e)^2 &= x^3 - 4bx^2 + 16cx - 64e^2 \\ &= -64\left(\frac{x^3}{-64} + \frac{bx^2}{16} - \frac{cx}{4} + e^2\right) \\ &= -64 f\left(\frac{-x}{4} + d\right). \end{aligned}$$

Note that if x_1, x_2, x_3 are the zeros of $f(x)$, then $4\,(d - x_1)\,, 4\,(d - x_2)\,, 4\,(d - x_3)$ are the zeros of $-64f\left(\frac{-x}{4} + d\right)$. Therefore,

$$\begin{aligned} \Delta_{q(x)} &= \Delta_{-64f\left(\frac{-x}{4}+d\right)} \\ &= \left[\prod_{1\leq i<j\leq 3} \left(4\,(d - x_i) - 4\,(d - x_j)\right)\right]^2 \\ &= \left[64 \prod_{1\leq i<j\leq 3} (x_i - x_j)\right]^2 \\ &= 64^2 \Delta_{f(x)}, \end{aligned}$$

so the discriminants of $f(x)$ and $q(x)$ differ by a square. This relationship will be used in Section 3.4.

The following theorem provides additional information about the fields generated by these polynomials.

Theorem 14. *Let K be a cubic number field. Let $g = 1$, if $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ and let $g = 1/3$, if $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Let h^* be the number of elements in the ideal class-group of K of order exactly two. Then there exist gh^* quadruplets of conjugate quartic fields K_4 such that $\Delta_{K_4} = \Delta_K$ and $K \subset \overline{K_4}$, where $\overline{K_4}$ is the Galois closure of K_4.*

The proof of this theorem relies on characters of S_4, Artin L-functions, and Dedekind zeta functions [6]. This theorem allows us to find the number of quartic fields over K with the same discriminant such that K is contained in the Galois closure of the quartic field. It does not, however, give a way of finding this collection of conjugate quartic fields. In this paper, we will use elliptic curves to explicitly compute the quartic fields in some special cases.

We now return to the question of characterizing points in $2E(K)$. The following theorem can be found in [8]. The proof given here has been modified to make use of Proposition 13.

Proposition 15. *Let E be an elliptic curve over a field of characteristic not equal to 2 or 3. Suppose E is given by*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = x^3 + rx^2 + sx + t = f(x),$$

with $\alpha, \beta, \gamma \in K$. If $(d, e) \in E(K)$ then $(d, e) \in 2E(K)$ if and only if $d - \alpha$, $d - \beta$, $d - \gamma \in K^2$.

Proof. Fix $(d, e) \in E(K)$. Assume there is some $(x_0, y_0) \in E(K)$ such that $2\,(x_0, y_0) = (d, e)$. Let $y = mx + b$ be the line tangent to E at (x_0, y_0). Note that both (x_0, y_0) and $(d, -e)$ are on $E(K)$ as well as the line $y = mx + b$. Hence for these two points,

$$(x-\alpha)(x-\beta)(x-\gamma) = y^2 = (mx+b)^2.$$

Since $y = mx + b$ is tangent to $E(K)$ at (x_0, y_0), x_0 is a double root of

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = 0,$$

and the third root is d. Hence,

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-d)\left(x-x_0\right)^2. \tag{2}$$

Let $x = \alpha$. Then Equation (2) becomes

$$-(m\alpha+b)^2 = (\alpha-d)\left(\alpha-x_0\right)^2.$$

Providing $\alpha \neq x_0$ it follows that

$$d - \alpha = \left(\frac{m\alpha+b}{\alpha-x_0}\right)^2,$$

which is a square in K, as desired.

Suppose for a contradiction that $\alpha = x_0$. Then $(x_0, 0)$ is on the elliptic curve. Furthermore, $2\,(x_0, 0) = 2(\alpha, 0) = \infty$. But we assumed that $2\,(x_0, y_0) = (d, e) \neq \infty$, a contradiction. Thus, $\alpha \neq x_0$ and $d - \alpha \in K^2$ as claimed.

Letting $x = \beta$ and $x = \gamma$ in Equation (2), one can use a similar argument to see that $d - \beta, d - \gamma \in K^2$ as claimed.

Now assume that $d-\alpha$, $d-\beta$, $d-\gamma \in K^2$, so we can write $d-\alpha = \alpha_1^2$, $d-\beta = \beta_1^2$, $d-\gamma = \gamma_1^2$ for some $\alpha_1, \beta_1, \gamma_1 \in K$. Let $g(x) = f(x+d) \in K[x]$ and let E' be the elliptic curve defined by $y^2 = g(x)$. Note that $g(0) = f(d) = e^2$, so $g(x) = x^3+bx^2+cx+e^2$ where $b = -(\alpha+\beta+\gamma-3d) = \alpha_1^2 + \beta_1^2 + \gamma_1^2$ and $c = (d-\alpha)(d-\beta) + (d-\alpha)(d-\gamma) + (d-\beta)(d-\gamma) = \alpha_1^2\beta_1^2 + \alpha_1^2\gamma_1^2 + \beta_1^2\gamma_1^2$. Furthermore, we have that $e^2 = -(\alpha-d)(\beta-d)(\gamma-d) = (d-\alpha)(d-\beta)(d-\gamma) = (\alpha_1\beta_1\gamma_1)^2$. Without loss of generality, we can choose the signs on $\alpha_1, \beta_1, \gamma_1$ so that $e = -\alpha_1\beta_1\gamma_1$.

We claim that in order to show that $(d, e) \in 2E(K)$, it suffices to show that $(0, e) \in 2E'(K)$. Suppose that $(0, e) = 2\,(x_1, y_1)$ for some $(x_1, y_1) \in E'(K)$. Then $(x_1 + d, y_1) \in E(K)$ since $f\,(x_1 + d) = g\,(x_1) = y_1^2$. Furthermore, $2\,(x_1 + d, y_1) = (d, e)$ since E is simply a translation of E' and addition on an elliptic curve is translation invariant. Thus if $(0, e) \in 2E'(K)$ then $(d, e) \in 2E(K)$, as claimed.

By Proposition 13, $(0, e) \in 2E'(K)$ if and only if

$$q(x) = x^4 - 2bx^2 - 8ex + b^2 - 4c = (b - x^2)^2 - 4(c - 2ex)$$

has a zero in K. Let $m = \alpha_1 - \beta_1 - \gamma_1 \in K$. By using the expressions for b, c and e in terms of $\alpha_1, \beta_1, \gamma_1, d$, it is easy to see that $(b - m^2)^2 = 4(c - 2em)$. Therefore, $m \in K$ is a zero of $q(x)$, as desired. □

We now introduce an important homomorphism between an elliptic curve over a field K and the multiplicative group $K^\times / \left(K^\times\right)^2$. This homomorphism is central to the proof of Theorem 27 in Section 3.3.2. Proposition 16 and Corollary 17 can both be found in [8].

Proposition 16. *Let K be a field of characteristic not equal to 2 or 3 and E be the elliptic curve defined by*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma),$$

with $\alpha, \beta, \gamma \in K$ distinct. Define $\widehat{\varphi}_\alpha : E(K) \to K^\times / \left(K^\times\right)^2$ by

$$\widehat{\varphi}_\alpha(P) = \begin{cases} (x-\alpha)\left(K^\times\right)^2 & \text{if } P = (x, y) \text{ with } x \neq \alpha \\ (\alpha-\beta)(\alpha-\gamma)\left(K^\times\right)^2 & \text{if } P = (\alpha, 0) \\ \left(K^\times\right)^2 & \text{if } P = \infty. \end{cases}$$

Then $\widehat{\varphi}_\alpha$ is a group homomorphism.

Proof. Note that $\widehat{\varphi}_\alpha$ depends only on the x-coordinate of the point, so $\widehat{\varphi}_\alpha((x,y)) = \widehat{\varphi}_\alpha((x,-y))$. Under the addition on an elliptic curve, $(x,-y) = -(x,y)$, so $\widehat{\varphi}_\alpha(P) = \widehat{\varphi}(-P)$ for any $P \in E(K)-\{\infty\}$. Since $\infty = -\infty, \widehat{\varphi}_\alpha(\infty) = \widehat{\varphi}_\alpha(-\infty)$ as well. Further, in $K^\times / \left(K^\times\right)^2$ every element is its own inverse so $\widehat{\varphi}_\alpha(P) = \widehat{\varphi}_\alpha(P)^{-1}$. Hence, it suffices to show that for $P_1, P_2, P_3 \in E(K)$, with $P_1 + P_2 + P_3 = \infty$, $\widehat{\varphi}_\alpha\left(P_1\right)\widehat{\varphi}_\alpha\left(P_2\right)\widehat{\varphi}_\alpha\left(P_3\right) = \left(K^\times\right)^2$. This is clear if more than one of the P_i is equal to ∞, so suppose that exactly one of the $P_i = \infty$. Without loss of generality, assume $P_3 = \infty$. Then $P_1 = -P_2$, so $\widehat{\varphi}_\alpha\left(P_1\right) = \widehat{\varphi}_\alpha\left(-P_2\right) = \widehat{\varphi}_\alpha\left(P_2\right)$. Hence,

$$\widehat{\varphi}_\alpha\left(P_1\right)\widehat{\varphi}_\alpha\left(P_2\right)\widehat{\varphi}_\alpha\left(P_3\right) = \widehat{\varphi}_\alpha\left(P_1\right)\widehat{\varphi}_\alpha\left(P_1\right)\left(K^\times\right)^2 = \left(K^\times\right)^2,$$

as desired. Therefore, assume $P_i = (x_i, y_i)$ for $i = 1,2,3$.

Suppose that $(x_i, y_i) \neq (\alpha, 0)$ for $i = 1,2,3$. By the definition of addition on an elliptic curve, the three points P_i lie on some line $y = mx + b$. Since each x_i satisfies

$$(x-\alpha)(x-\beta)(x-\gamma) = y^2 = (mx+b)^2,$$

it follows that

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = \left(x - x_1\right)\left(x - x_2\right)\left(x - x_3\right).$$

By substituting $x = \alpha$ we have $(m\alpha + b)^2 = \left(x_1 - \alpha\right)\left(x_2 - \alpha\right)\left(x_3 - \alpha\right)$. Thus,

$$\begin{aligned}\widehat{\varphi}_\alpha(P_1)\widehat{\varphi}_\alpha(P_2)\widehat{\varphi}_\alpha(P_3) &= \left(x_1 - \alpha\right)\left(x_2 - \alpha\right)\left(x_3 - \alpha\right)\left(K^\times\right)^2 \\ &= (m\alpha + b)^2\left(K^\times\right)^2 \\ &= \left(K^\times\right)^2.\end{aligned}$$

Now suppose that at least one of the $(x_i, y_i) = (\alpha, 0)$. Without loss of generality, say $(x_i, y_i) = (\alpha, 0)$. Then $(x_j, y_j) \neq (\alpha, 0)$ for $j = 2,3$, since otherwise, the third point would be ∞. Let $y = mx + b$ be the line through P_1, P_2 and P_3. Again,

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = \left(x - x_1\right)\left(x - x_2\right)\left(x - x_3\right). \tag{3}$$

So $(x-\alpha) \mid (mx+b)^2$ in $K[x]$, which is a unique factorization domain. Now, $(mx+b)^2 = m^2\left(x + \frac{b}{m}\right)^2$ and so $x - \alpha = x + \frac{b}{m}$. Since $K[x]$ is an integral domain, it follows from Equation (3) that

$$(x-\beta)(x-\gamma) - m^2(x-\alpha) = \left(x - x_2\right)\left(x - x_3\right).$$

Letting $x = \alpha$ in the above, we have

$$\widehat{\varphi}_\alpha\left(P_1\right) = \widehat{\varphi}_\alpha((\alpha, 0)) = (\alpha-\beta)(\alpha-\gamma)\left(K^\times\right)^2 = \left(\alpha - x_2\right)\left(\alpha - x_3\right)\left(K^\times\right)^2 = \widehat{\varphi}_\alpha\left(P_2\right)\widehat{\varphi}_\alpha\left(P_3\right).$$

Thus,

$$\widehat{\varphi}_\alpha(P_1)\,\widehat{\varphi}_\alpha(P_2)\,\widehat{\varphi}_\alpha(P_3) = \widehat{\varphi}_\alpha(P_2)^2\,\widehat{\varphi}_\alpha(P_3)^2 = \left(K^\times\right)^2,$$

as desired.

Hence, $\widehat{\varphi}_\alpha$ is a homomorphism. □

Note that if $P \in 2E(K)$, we may write $P = 2Q$ for some $Q \in E(K)$. Then $\widehat{\varphi}_\alpha(P) = \widehat{\varphi}_\alpha(2Q) = \widehat{\varphi}_\alpha(Q)^2 = \left(K^\times\right)^2$, so $2E(K) \subseteq \ker\widehat{\varphi}_\alpha$. Hence $\widehat{\varphi}_\alpha$ induces a homomorphism

$$\varphi_\alpha : E(K)/2E(K) \to K^\times/\left(K^\times\right)^2.$$

Note that the homomorphism in Proposition 16 could be defined with β or γ in place of α. The proof is valid in these cases as well, and we define φ_β and φ_γ analogously to φ_α.

Corollary 17. *Let K be a field of characteristic not equal to 2 or 3. With notation as above,*

$$\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma : E(K)/2E(K) \to \left(K^\times/\left(K^\times\right)^2\right) \times \left(K^\times/\left(K^\times\right)^2\right) \times \left(K^\times/\left(K^\times\right)^2\right)$$

is one-to-one.

Proof. Let $P \in E(K)$ such that $\varphi_\alpha(P) = \varphi_\beta(P) = \varphi_\gamma(P) = \left(K^\times\right)^2$. We will show that $P \in 2E(K)$.

First consider the case where $P \notin E[2]$. Then $P = (x, y)$ with $(x-\alpha), (x-\beta), (x-\gamma) \in \left(K^\times\right)^2$. By Proposition 15, there is some $(x', y') \in E(K)$ such that $2\,(x', y') = (x, y)$, so $(x, y) \in 2E(K)$, as desired.

Now assume that $(x, y) = (\alpha, 0)$. Then

$$\left(K^\times\right)^2 = \varphi_\alpha(x, y) = (\alpha-\beta)(\alpha-\gamma)\left(K^\times\right)^2 \tag{4}$$

and

$$\left(K^\times\right)^2 = \varphi_\beta(x, y) = (\alpha-\beta)\left(K^\times\right)^2. \tag{5}$$

Together, Equations (5) and (4) imply that $\alpha-\beta \in \left(K^\times\right)^2$ and $\alpha-\gamma \in \left(K^\times\right)^2$. Since $\alpha-\alpha = 0 \in K^2$, Proposition 15 implies that $(x, y) \in 2E(K)$. Similarly, if $(x, y) = (\beta, 0)$ or $(x, y) = (\gamma, 0)$, then $(x, y) \in 2E(K)$.

Finally, consider $P = \infty$. We have $\varphi_\alpha(\infty) = \varphi_\beta(\infty) = \varphi_\gamma(\infty) = \left(K^\times\right)^2$, so $\infty \in \ker\left(\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma\right)$. Also, $\infty = \infty + \infty \in 2E(K)$, so $\infty \in 2E(K)$.

Hence $\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma$ is one-to-one, as desired. □

Note that Theorem 16 and Corollary 17 hold for any field of characteristic zero. This is important as we will use these homomorphisms for elliptic curves defined over $\mathbb{Q}_p$.

Let $f(x) = (x-\alpha)(x-\beta)(x-\gamma) \in \mathbb{Q}[x]$ be irreducible over $\mathbb{Q}$, and let $K = \mathbb{Q}(\alpha)$. Assume that K is Galois over $\mathbb{Q}$, so α, β, γ are conjugates over $\mathbb{Q}$.

For each rational prime $p \leq \infty$, let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. Recall that if p splits in K, then $f(x)$ splits into three distinct linear factors modulo p. Therefore, Theorem 2 implies that $f(x)$ has three distinct zeros in $\mathbb{Z}_p$. By a slight abuse of notation, we let α, β, γ denote these elements of $\mathbb{Q}_p$. Thus, if p splits in K we can embed $K \hookrightarrow \mathbb{Q}_p^3$ by

$$\alpha \mapsto (\alpha, \beta, \gamma)\,.$$

(We extend this to all points in K by writing them in terms of the basis $\{1, \alpha, \alpha^2\}$ and then using the fact that the embedding is a homomorphism that fixes $\mathbb{Q}$.) Hence, if p splits in K we can define

$$\lambda_p : E\left(\mathbb{Q}_p\right) \to \left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right) \times \left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right) \times \left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right)$$

by

$$P \mapsto \begin{cases} ((x-\alpha)(\mathbb{Q}_p^\times)^2, (x-\beta)(\mathbb{Q}_p^\times)^2, (x-\gamma)(\mathbb{Q}_p^\times)^2) & \text{if } P = (x,y) \notin E[2] \\ ((\alpha-\beta)(\alpha-\gamma)(\mathbb{Q}_p^\times)^2, (\alpha-\beta)(\mathbb{Q}_p^\times)^2, (\alpha-\gamma)(\mathbb{Q}_p^\times)^2) & \text{if } P = (\alpha, 0) \\ ((\beta-\alpha)(\mathbb{Q}_p^\times)^2, (\beta-\alpha)(\beta-\gamma)(\mathbb{Q}_p^\times)^2, (\beta-\gamma)(\mathbb{Q}_p^\times)^2) & \text{if } P = (\beta, 0) \\ ((\gamma-\alpha)(\mathbb{Q}_p^\times)^2, (\gamma-\beta)(\mathbb{Q}_p^\times)^2, (\gamma-\alpha)(\gamma-\beta)(\mathbb{Q}_p^\times)^2) & \text{if } P = (\gamma, 0) \\ ((\mathbb{Q}_p^\times)^2, (\mathbb{Q}_p^\times)^2, (\mathbb{Q}_p^\times)^2) & \text{if } P = \infty. \end{cases}$$

Note that with $\mathbb{Q}_p$ being the field in Corollary 17,

$$\lambda_p = \varphi_\alpha \times \varphi_\beta \times \varphi_\gamma.$$

Therefore, this corollary implies that λ_p is a monomorphism. In the rest of the paper we will write $\left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right)^3$ for $\left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right) \times \left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right) \times \left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right)$ and we will drop the $\left(\mathbb{Q}_p^\times\right)^2$ when writing cosets. This will not create any ambiguity.

We would like to define λ_p for all rational primes, but this would require that $f(x)$ have three distinct zeros in $\mathbb{Q}_p$. As we shall now see, this is not the case. Suppose that p is inert in K. Then $f(x)$ is irreducible modulo p. If $f(x)$ had a zero in $\mathbb{Z}_p$, say a, then by reducing a modulo p, $\bar{a}$ would be a zero of $f(x)$ modulo p, a contradiction. Hence, if p is inert in K then $f(x)$ does not have a zero in $\mathbb{Z}_p$. Note that any zero of $f(x)$ is an algebraic integer, so if $f(x)$ is inert then $f(x)$ does not have a zero in $\mathbb{Q}_p$.

Now suppose that p is ramified in K, so there is a single prime $\mathfrak{p}$ lying over p in K. Therefore there is only one extension of $|\cdot|_p$ to K_p, where K_p is the completion of K with respect to $|\cdot|_{\mathfrak{p}}$. By Theorem 4 it follows that $f(x)$ has only one irreducible factor in $\mathbb{Q}_p[x]$. That is, $f(x) = g(x)^m$ for some $g(x) \in \mathbb{Q}_p[x], m \in \mathbb{Z}^+$. As the degree of $f(x)$ is 3, either $g(x)$ is a linear polynomial and $m = 3$ or $g(x)$ is a cubic polynomial and $m = 1$. Suppose for a contradiction that $m = 3$. Then $f(x) = 0$ has a triple root in $\mathbb{Q}_p$. Note that if $K \subseteq \mathbb{Q}_p$ then the zeros of $f(x)$ in $\mathbb{Q}_p$ are α, β, γ, which are distinct, contradicting that $f(x) = g(x)^3$. Since $K \cap \mathbb{Q}_p$ is a subfield of K and $[K : \mathbb{Q}] = 3$, it follows that $K \cap \mathbb{Q}_p = \mathbb{Q}$. Then K_p has at least six zeros (counting multiplicities) of $f(x)$, three from each of K and $\mathbb{Q}_p$. This is impossible since $f(x)$ is of degree 3 and K_p is a field. Hence, it must be that $m = 1$ and $f(x)$ is irreducible over $\mathbb{Q}_p$. Therefore, if p does not split then $f(x)$ does not have a zero in $\mathbb{Q}_p$.

If p does not split in K, then p ramifies or is inert and there is a unique prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p. Let K_p be the completion of K with respect to $|\cdot|_{\mathfrak{p}}$. Define

$$\lambda_p : E(\mathbb{Q}_p) \to K_p^\times / \left(K_p^\times\right)^2$$

by

$$P \mapsto \begin{cases} (x-\alpha)\left(K_p^\times\right)^2 & \text{if } P = (x,y) \\ \left(K_p^\times\right)^2 & \text{if } P = \infty. \end{cases}$$

By Proposition 16 there is a homomorphism $\widehat{\varphi}_\alpha : E(K_p) \to K_p^\times / \left(K_p^\times\right)^2$ that restricts to λ_p on $E(\mathbb{Q}_p)$ provided that $\alpha \notin \mathbb{Q}_p$. We showed above that if p does not split in K then $f(x)$ has no zeros in $\mathbb{Q}_p$. In particular, $\alpha \notin \mathbb{Q}_p$ so λ_p is a group homomorphism.

We would like to consider the intersection of $\operatorname{Im} \lambda_p$ for all primes p, but each λ_p maps to a different codomain. Recall that K embeds into $\mathbb{Q}_p^3$ and K_p. These induce embeddings of $K^\times / (K^\times)^2$ into $\left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right)^3$ and $K_p^\times / \left(K_p^\times\right)^2$. Let $i_p : K^\times / (K^\times)^2 \hookrightarrow \left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right)^3$ be the embedding if p splits and $i_p : K^\times / (K^\times)^2 \hookrightarrow K_p^\times / \left(K_p^\times\right)^2$ be the embedding if p does not split. By taking the preimage of $\operatorname{Im} \lambda_p \cap i_p\left(K^\times / (K^\times)^2\right)$ under i_p we obtain a subgroup of $K^\times / (K^\times)^2$.

Definition 5. *The* <u>*2-Selmer group*</u> *of K, denoted S_2, is*

$$S_2 = \bigcap_p i_p^{-1}\left(\operatorname{Im} \lambda_p \cap i_p\left(K^\times / (K^\times)^2\right)\right),$$

where the intersection is taken over all primes, finite and infinite, of $\mathbb{Q}$.

Note that since each $i_p^{-1}\left(\operatorname{Im} \lambda_p \cap i_p\left(K^\times / (K^\times)^2\right)\right)$ is a subgroup of $K^\times / (K^\times)^2$, it follows that S_2 is a subgroup of $K^\times / (K^\times)^2$. Furthermore for all p, $\lambda_p|_{E(\mathbb{Q})}$ maps into $i_p\left(K^\times / (K^\times)^2\right)$

since $x-\alpha, x-\beta, x-\gamma \in K^{\times}$. Define $\overline{\varphi} : E(\mathbb{Q}) \to S_2$ by $\overline{\varphi}(x,y) = (x-\alpha)\left(K^{\times}\right)^2$ and $\overline{\varphi}(\infty) = \left(K^{\times}\right)^2$, so $\overline{\varphi}$ is essentially the restriction $\lambda_p|_{E(\mathbb{Q})}$ for all p. It follows from Proposition 15 that $\ker \overline{\varphi} = 2E(\mathbb{Q})$. So $\overline{\varphi}$ induces a monomorphism $\varphi : E(\mathbb{Q})/2E(\mathbb{Q}) \to S_2$ such that the following diagram commutes.

$$\begin{tikzcd}
E(\mathbb{Q}) \arrow[r, "\overline{\varphi}"] \arrow[d] & S_2 \\
E(\mathbb{Q})/2E(\mathbb{Q}) \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Recall that the domain of λ_p is $E\left(\mathbb{Q}_p\right)$, so φ need not be surjective. This leads to the following definition.

Definition 6. *The 2-part of the Tate-Shafarevich group of K, denoted Ш_2, is defined such that the sequence*

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to^{\varphi} S_2 \to \text{Ш}_2 \to 0$$

is exact. We will identify Ш_2 with $S_2/\operatorname{Im}\varphi$.

Note that if all of the elements in S_2 come from points on $E(\mathbb{Q})$, then Ш_2 is trivial. Heuristically, Ш_2 measures how much of S_2 comes from points not on $E(\mathbb{Q})$.

2.4 Characters and zeta functions

In this section we give a brief review of characters of group representations and Dedekind zeta functions. We prove Proposition 19, which is a special case of a result of Heilbronn [6].

Definition 7. *Let V be a finite dimensional vector space over $\mathbb{C}$. A representation of a finite group G is a homomorphism $f : G \to GL(V)$. The character of the representation f is the function $\chi : G \to \mathbb{C}$ given by $\chi(g) = \operatorname{Trace} f(g)$. The character of the trivial representation is called the principal character.*

Using the properties of the trace of a matrix, it is not difficult to check that a character of a group is constant on conjugacy classes of the group. A character table of a group G lists all conjugacy classes C of G, the number of elements in each class, denoted $n(C)$, and the value of each character on each conjugacy class.

A character χ of a subgroup H of G induces a character on G as follows. Partition G into right cosets of H, say $G = \bigcup_{i=1}^{n} H\alpha_i$. Extend χ to all of G by letting

$$\chi(g) = \begin{cases} \chi(g) & \text{if } g \in H \\ 0 & \text{if } g \notin H. \end{cases}$$

The induced characters χ^* of G is defined to be

$$\chi^*(g) = \sum_{i=1}^{n} \chi\left(\alpha_i g \alpha_i^{-1}\right).$$

Definition 8. *Let G be a finite group and $f : G \to GL(V)$ be a representation. An $\underline{f\text{-invariant}}$ $\underline{\text{subspace}}$ W of V is a subspace of V such that $f(g)(W) \subseteq W$ for all $g \in G$. We say that f is an $\underline{\text{irreducible representation}}$ if V has no proper nontrivial f-invariant subspaces. A character of G is said to be $\underline{\text{irreducible}}$ if it is the character of an irreducible representation.*

Often character tables for a group list only the irreducible characters of the group.

Definition 9. *Let K be a number field. The $\underline{\text{Dedekind zeta function}}$ of K, defined for $s \in \mathbb{C}$ such that $\Re(s) > 1$, is*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

where the sum is taken over all nonzero ideals of $\mathcal{O}_K$ and $N(\mathfrak{a})$ is the norm of the ideal $\mathfrak{a}$.

The Dedekind zeta function converges for all $s \in \mathbb{C}$ such that $\Re(s) > 1$. Let r_K be the number of real embeddings of K and $2t_K$ the number of complex embeddings of K. The Dedekind zeta function can be extended to a meromorphic function on $\mathbb{C}$ via the functional equation

$$\Lambda_K(s) = |\Delta_K|^{1/2-s}\Lambda_K(1-s),$$

where

$$\Lambda_K(s) = \pi^{-r_K s/2}(2\pi)^{-t_K s}\Gamma\left(\frac{s}{2}\right)^{r_K}\Gamma(s)^{t_K}\zeta_K(s). \tag{6}$$

We note that the gamma function, Γ, is independent of K. (More information about Γ can be found in [13].)

Characters and Dedekind zeta functions are related via Artin $\mathcal{L}$-series. These are functions of s that depend on a Galois extension L/K and a character of the Galois group. In the proof of Proposition 19, we need the properties of Artin $\mathcal{L}$-functions given in the following theorem that can be found, with proof, in [14].

Theorem 18. *Let L/K be a Galois extension.*

1. *For the principal character $\chi = 1$ we obtain the Dedekind zeta function*

$$\mathcal{L}(s, \chi, L/K) = \zeta_K(s).$$

Table 1: Irreducible Characters of A_4

C	$n(C)$	χ_1	χ_2	χ_3	χ_4
(1)	1	1	1	1	3
(12)(34)	3	1	1	1	-1
(123)	4	1	$e^{2i\pi/3}$	$e^{4i\pi/3}$	0
(132)	4	1	$e^{4i\pi/3}$	$e^{2i\pi/3}$	0

2. *If* χ_1, χ_2 *are two characters of* $\mathrm{Gal}(L/K)$*, then*

$$\mathcal{L}\left(s, \chi_1 + \chi_2, L/K\right) = \mathcal{L}\left(s, \chi_1, L/K\right)\mathcal{L}\left(s, \chi_2, L/K\right).$$

3. *If* M *is an intermediate field,* $K \subseteq M \subseteq L$*,* φ *a character of* $\mathrm{Gal}(L/M)$*, and* φ^* *the induced character of* $\mathrm{Gal}(L/K)$*, then*

$$\mathcal{L}(s, \varphi^*, L/K) = \mathcal{L}(s, \varphi, L/M).$$

The following proposition will be needed in Section 3.4 in the proof of Proposition 37. This proposition is a special case of part of the proof of Theorem 14, and the proof given here is based on Heilbronn's proof [6].

Proposition 19. *Let* F *be a Galois extension of* $\mathbb{Q}$ *with* $\mathrm{Gal}(F/\mathbb{Q}) \cong A_4$*. Let* K *be the unique cubic subfield of* F*,* M_j *be the quartic subfields of* F *for* $j = 1, 2, 3, 4$*, and* L_i *be the sextic subfields of* F *for* $i = 1, 2, 3$*. If* $r_{L_i} = 2 + r_{M_j}$ *and* $t_{L_i} = t_{M_j}$*, then*

$$|\Delta_{L_i}| = |\Delta_K||\Delta_{M_j}|$$

for any $i \in \{1, 2, 3\}$ *and* $j \in \{1, 2, 3, 4\}$*.*

Proof. For each conjugacy class C of $A_4 = \mathrm{Gal}(F/K)$, let $n(C)$ denote the number of elements of A_4 in the conjugacy class. The table of irreducible characters for $A_4 = \mathrm{Gal}(F/\mathbb{Q})$ is shown in Table 1.

Fix $i \in \{1, 2, 3\}$ and $j \in \{1, 2, 3, 4\}$. Let φ, ψ, γ be the principal characters for $\mathrm{Gal}(F/K)$, $\mathrm{Gal}\left(F/M_j\right)$, $\mathrm{Gal}\left(F/L_i\right)$, respectively. Let W, A, V be the subgroups of A_4 corresponding to $\mathrm{Gal}(F/K)$, $\mathrm{Gal}\left(F/M_j\right)$, $\mathrm{Gal}\left(F/L_i\right)$, respectively, under the isomorphism $\mathrm{Gal}(F/\mathbb{Q}) \cong A_4$. Writing

$$\begin{aligned} A_4 &= W \cup W(123) \cup W(132) \\ &= A \cup A(12)(34) \cup A(13)(24) \cup A(14)(23) \\ &= V \cup V(123) \cup V(124) \cup V(132) \cup V(142) \cup V(13)(24) \end{aligned}$$

Table 2: Induced Characters of A_4

C	φ^*	ψ^*	γ^*
(1)	3	4	6
(12)(34)	3	0	2
(123)	0	1	0
(132)	0	1	0

we find the induced characters of φ, ψ, and γ of A_4, shown in Table 2.

Note that these induced characters can be written in terms of the irreducible characters as the sums $\varphi^* = \chi_1 + \chi_2 + \chi_3$, $\psi^* = \chi_1 + \chi_4$, and $\gamma^* = \chi_1 + \chi_2 + \chi_3 + \chi_4$. This together with Theorem 18 gives that for all $s \in \mathbb{C}$ such that $\Re(s) > 1$,

$$\begin{aligned}
\zeta(s) &= \mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right) \\
\zeta_K(s) &= \mathcal{L}(s, \varphi, F/K) = \mathcal{L}\left(s, \varphi^*, F/\mathbb{Q}\right) = \mathcal{L}\left(s, \chi_1 + \chi_2 + \chi_3\right) \\
&= \mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_2, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_3, F/\mathbb{Q}\right) \\
\zeta_{M_j}(s) &= \mathcal{L}\left(s, \psi, F/M_j\right) = \mathcal{L}\left(s, \psi^*, F/\mathbb{Q}\right) = \mathcal{L}\left(s, \chi_1 + \chi_4, F/\mathbb{Q}\right) \\
&= \mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_4, F/\mathbb{Q}\right) \\
\zeta_{L_i}(s) &= \mathcal{L}\left(s, \gamma, F/L_i\right) = \mathcal{L}\left(s, \gamma^*, F/\mathbb{Q}\right) = \mathcal{L}\left(s, \chi_1 + \chi_2 + \chi_3 + \chi_4, F/\mathbb{Q}\right) \\
&= \mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_2, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_3, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_4, F/\mathbb{Q}\right).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\zeta(s)\zeta_{L_i}(s) &= \left[\mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right)\right] \left[\mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_2, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_3, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_4, F/\mathbb{Q}\right)\right] \\
&= \left[\mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_2, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_3, F/\mathbb{Q}\right)\right] \left[\mathcal{L}\left(s, \chi_1, F/\mathbb{Q}\right) \mathcal{L}\left(s, \chi_4, F/\mathbb{Q}\right)\right] \\
&= \zeta_K(s)\zeta_{M_j}(s).
\end{aligned}$$

Note that $\mathbb{Q}$ has one real embedding and no complex embeddings. Also, since K corresponds to the only normal subgroup of A_4, K is Galois. Since K is a cyclic cubic extension, it must be that $K \subseteq \mathbb{R}$. Manipulating Equation (6) gives

$$\begin{aligned}
\zeta(s) &= \pi^{s/2}\Gamma\left(\frac{s}{2}\right)^{-1}\Lambda(s) \\
\zeta_K(s) &= \pi^{3s/2}\Gamma\left(\frac{s}{2}\right)^{-3}\Lambda_K(s)
\end{aligned}$$

$$\zeta_{M_j}(s) = \pi^{r_{M_j} s/2}(2\pi)^{t_{M_j} s}\Gamma\left(\frac{s}{2}\right)^{-r_{M_j}}\Gamma(s)^{-t_{M_j}}\Lambda_{M_j}(s)$$
$$\zeta_{L_i}(s) = \pi^{r_{L_i} s/2}(2\pi)^{t_{L_i} s}\Gamma\left(\frac{s}{2}\right)^{-r_{L_i}}\Gamma(s)^{-t_{L_i}}\Lambda_{L_i}(s).$$

Substituting these expressions for the zeta functions into $\zeta(s)\zeta_{L_i}(s) = \zeta_K(s)\zeta_{M_j}(s)$ and using $1 + r_{L_i} = 3 + r_{M_j}$ and $t_{L_i} = t_{M_j}$ yields

$$\Lambda(s)\Lambda_{L_i}(s) = \Lambda_K(s)\Lambda_{M_j}(s), \tag{7}$$

for all $s \in \mathbb{C}$ such that $\Re(s) > 1$. The functional equations for Dedekind zeta functions imply that

$$|\Delta_{L_i}|^{1/2-s}\Lambda(1-s)\Lambda_{L_i}(1-s) = |\Delta_K|^{1/2-s}|\Delta_{M_j}|^{1/2-s}\Lambda_K(1-s)\Lambda_{M_j}(1-s).$$

Letting $s = -1/2$ in the above equation we have

$$|\Delta_{L_i}|\Lambda(3/2)\Lambda_{L_i}(3/2) = |\Delta_K||\Delta_{M_j}|\Lambda_K(3/2)\Lambda_{M_j}(3/2).$$

As Equation (7) holds for $s = 3/2 > 1$, it follows that $|\Delta_{L_i}| = |\Delta_K||\Delta_{M_j}|$, as claimed. □

3 The simplest cubic fields

In this section we discuss the results in [19]. We begin by defining a family of cubic polynomials that were studied by Shanks [15]. In the first subsection, we establish some basic properties of these polynomials and their associated fields. Next, we prove two results about the divisibility of the class numbers of the cubic fields generated by these polynomials. Finally, we obtain information about the 2-part of the class groups via methods of elliptic curves. The results in the second and third subsections are entirely independent, but both require the basic properties presented in the first section.

3.1 Properties of Shanks' simplest cubic fields

Define

$$f(x) = x^3 + mx^2 - (m+3)x + 1,$$

where $m \geq 0$ is an integer such that $m \not\equiv 3 \pmod 9$. Note that $f(x)$ is irreducible over $\mathbb{Q}$ since $f(1) \neq 0$ and $f(-1) \neq 0$.

By evaluating f at $-m-2$ and $-m-1$ and using the intermediate value theorem, we see that $f(x)$ has a real zero, call it ρ, between $-m-2$ and $-m-1$. Let $K = \mathbb{Q}(\rho)$. Since $f(x)$ is irreducible over $\mathbb{Q}$, $[K : \mathbb{Q}] = 3$. Define

$$\rho' = 1/(1-\rho) \text{ and } \rho'' = 1 - 1/\rho.$$

It is easy to check that

$$f\left(\rho'\right) = \frac{-f(\rho)}{(1-\rho)^3} = 0 \text{ and } f\left(\rho''\right) = \frac{-f(\rho)}{\rho^3} = 0,$$

so ρ' and ρ'' are the two other zeros of $f(x)$. Since ρ', ρ'' are rational expressions in ρ it follows that $\rho', \rho'' \in K = \mathbb{Q}(\rho)$. So K is a Galois extension of $\mathbb{Q}$. To fix notation, we let $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3\}$, where σ_1 is the identity and $\sigma_2(\rho) = \rho'$. Note that since $\rho \in \mathbb{R}$ and K is Galois, K is a totally real field.

Next we show that the discriminant of $f(x)$ is $D^2 = \left(m^2+3m+9\right)^2$. Solving $f(\rho) = 0$ for m yields

$$m = \frac{\rho^3 - 3\rho + 1}{\rho - \rho^2}.$$

Using the expressions for ρ', ρ'' in terms of ρ it is easy to show that

$$D = (\rho - \rho')(\rho - \rho'')(\rho' - \rho'') = \frac{\left(\rho^2 - \rho + 1\right)^3}{\left(\rho - \rho^2\right)^2}.$$

Substituting the equation for m into $m^2 + 3m + 9$ shows that $D = m^2 + 3m + 9$, as desired.

We claim that $m \not\equiv 3 \pmod 9$ implies that $D \not\equiv 0 \pmod{27}$. Suppose for a contradiction that $D \equiv 0 \pmod{27}$. Then $0 \equiv m^2 + 3m + 9 \equiv m^2 \pmod 3$. It follows that $m \equiv 0 \pmod 3$ and so $m \equiv 0, 3, 6 \pmod 9$. If $m \equiv 0 \pmod 9$, then $9 \mid m$, and so $27 \mid m^2$ and $27 \mid 3m$. But then $D = m^2 + 3m + 9 \equiv 9 \not\equiv 0 \pmod{27}$, a contradiction. If $m \equiv 6 \pmod 9$, then $9 \mid m - 6$, and so $27 \mid (m-6)^2$. Now,

$$0 \equiv (m-6)^2 = m^2 - 12m + 36 \equiv m^2 + 15m + 9 = m^2 + 3m + 9 + 12m \equiv 12m \pmod{27},$$

so $27 \mid 12m$. Therefore $9 \mid m$, a contradiction since $m \equiv 6 \pmod 9$. Therefore, $m \equiv 3 \pmod 9$. But by assumption $m \not\equiv 3 \pmod 9$, so it must be that $D \not\equiv 0 \pmod{27}$, as claimed.

Next we investigate the units in $\mathcal{O}_K$. Any zero of $f(x)$ must divide 1, so ρ, ρ', ρ'' are units in $\mathcal{O}_K$. Note that $\rho < -m - 1 \leq -1$, so $0 < 1/(1-\rho) < 1/2 < 1$ and $1 < 1 - 1/\rho < 2$. Therefore

$$-m - 2 < \rho < -m - 1 < 0 < \rho' < 1 < \rho'' < 2. \tag{8}$$

Using this information, we obtain Table 3 which shows that all possible signatures can be obtained from the units of $\mathcal{O}_K$. By Lemma 11 it follows that the narrow and wide class numbers of K are equal.

Let $\mathcal{O}_K^\times$ be the group of units in $\mathcal{O}_K$. By Dirichlet's Unit Theorem, $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$, since K is a totally real cubic extension of $\mathbb{Q}$. Furthermore, Shanks proved that ρ and ρ' are independent [15]. Therefore, $\left[\mathcal{O}_K^\times : \langle -1, \rho, \rho' \rangle\right]$ is finite. The following lemma is used often throughout the paper.

Table 3: Signatures of units

unit u	$(\sigma_1(u), \sigma_2(u), \sigma_3(u))$	signature of u
ρ	(ρ, ρ', ρ'')	$(-, +, +)$
ρ'	(ρ', ρ'', ρ)	$(+, +, -)$
1	$(1, 1, 1)$	$(+, +, +)$
-1	$(-1, -1, -1)$	$(-, -, -)$
ρ''	(ρ'', ρ, ρ')	$(+, -, +)$
$-\rho$	$(-\rho, -\rho', -\rho'')$	$(+, -, -)$
$-\rho'$	$(-\rho', -\rho'', -\rho)$	$(-, -, +)$
$-\rho''$	$(-\rho'', -\rho, -\rho')$	$(-, +, -)$

Lemma 20. *If $\mathcal{O}_K^\times = \langle -1, \rho, \rho' \rangle$ then every totally positive element of $\mathcal{O}_K^\times$ is a square in $\mathcal{O}_K$.*

Proof. Let $x \in \mathcal{O}_K^\times$ be totally positive. We can write $x = (-1)^a \rho^b (\rho')^c$ for some $a, b, c \in \mathbb{Z}$. Since x is totally positive applying $\sigma_1, \sigma_2, \sigma_3$, we have

$$(-1)^a \rho^b (\rho')^c > 0 \tag{9}$$

$$(-1)^a (\rho')^b (\rho'')^c > 0 \tag{10}$$

$$(-1)^a (\rho'')^b \rho^c > 0. \tag{11}$$

Since $0 < \rho' < \rho''$, (10) implies that $a \in 2\mathbb{Z}$. Then using the fact that $\rho < 0$ along with (9) and (11), it follows that $b, c \in 2\mathbb{Z}$. Therefore, x is a square in $\mathcal{O}_K$, as desired. □

Proposition 21. *Let $m \not\equiv 3 \pmod 9$ be an integer. Write $D = m^2 + 3m + 9 = bc^3$ with $b, c \in \mathbb{Z}$ and b cube-free. Then the discriminant of K is*

$$\Delta_K = \begin{cases} \left(\prod_{p|b} p\right)^2 & \textit{if} 3 \nmid b \\ \left(3\prod_{p|b} p\right)^2 & \textit{if} 3 \mid b, \end{cases}$$

where the product is taken over all primes p that divide b.

Proof. Recall that the primes that ramify in K are exactly those dividing Δ_K. We will show that a prime ramifies if and only if it divides b.

Define

$$g(x) = x^3 + D(x+1)^2.$$

A direct verification shows that $\alpha = -1 + \rho - \rho^2$ is a zero of $g(x)$. We know that $\alpha \notin \mathbb{Q}$ since otherwise ρ would satisfy the quadratic equation $-x^2 + x - 1 - \alpha = 0$ and so $f(x)$ would be reducible over $\mathbb{Q}$, a contradiction. The discriminant of $g(x)$ is $\Delta_g = D^2(4D - 27)$. To see this, note that $g(x - D/3) = x^3 + px + q$, where $p = -D^3/3 + 2D$ and $q = 2D^3/27 - 2D^2/3 + D$. Then the discriminant of $g(x)$ is $-4p^3 - 27q^2 = D^2(4D - 27)$ [7, page 271]. Write $D = bc^3$ with $b, c \in \mathbb{Z}$ and b cube-free.

Define

$$h(x) = c^{-3}g(cx) = x^3 + b(cx + 1)^2.$$

Note that the zeros of $h(x)$ differ from the zeros of $g(x)$ by a multiple of c. Therefore,

$$\Delta_h = \Delta_g/c^6 = b^2(4D - 27).$$

Since $\alpha \in K$ is a zero of $g(x)$, $\alpha/c \in K$ is a root of $h(x)$. Since $[K : \mathbb{Q}] = 3$, either and $\alpha/c \notin \mathbb{Q}$, $\mathbb{Q}(\alpha/c) = K$. So $h(x)$ also generates the extension $K/\mathbb{Q}$.

Let p be a prime that ramifies in K. Recall that the discriminant of a field always divides the discriminant of a polynomial that generates the field. Then $p \mid \Delta_K \mid \Delta_f = D^2$, so $p \mid D$. Similarly, $p \mid \Delta_K \mid \Delta_h$, so $p \mid b(4D - 27)$. Hence $p \mid \gcd(D, b(4D - 27)) = \gcd(D, 27b) = \gcd(bc^3, 27b)$. Note that $\gcd(c, 3) = 1$, since $D = bc^3 \not\equiv 0 \pmod{27}$. Therefore $p \mid \gcd(bc^3, 27b^2) = b$. Hence, if p is ramified then $p \mid b$.

Now let p be a prime dividing b and $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal lying above p. Then $v_p(b)$ is either 1 or 2 since b is cube-free and $p \mid b$. Let β be a root of $h(x)$, so $-\beta^3 = b(c\beta + 1)^2$. Then,

$$3v_{\mathfrak{p}}(\beta) = v_{\mathfrak{p}}\left(\beta^3\right) = v_{\mathfrak{p}}\left(-\beta^3\right) = v_{\mathfrak{p}}\left(b(c\beta + 1)^2\right) = v_{\mathfrak{p}}(b) + 2v_{\mathfrak{p}}(c\beta + 1). \tag{12}$$

Recall that $\mathfrak{p} \mid p \mid b$, so $v_{\mathfrak{p}}(b) > 0$. Furthermore, since β is a zero of $h(x) = c^{-3}g(cx)$, $c\beta$ is a zero of $g(x)$ and thus is an algebraic integer. We showed that $h(x)$ generates K, so $\beta \in \mathcal{O}_K$. Thus, $c\beta + 1 \in \mathcal{O}_K$ and so $v_{\mathfrak{p}}(c\beta + 1) \geq 0$. Therefore, Equation (12) implies that $v_{\mathfrak{p}}(\beta) > 0$. Then $\beta \equiv 0 \pmod{\mathfrak{p}}$, so $c\beta + 1 \equiv 1 \pmod{\mathfrak{p}}$. Since $1 \notin \mathfrak{p}$, it follows that $c\beta + 1 \notin \mathfrak{p}$, so $v_{\mathfrak{p}}(c\beta + 1) \leq 0$. Hence, $v_{\mathfrak{p}}(c\beta + 1) = 0$. Thus, Equation (12) becomes $3v_{\mathfrak{p}}(\beta) = v_{\mathfrak{p}}(b)$.

If p is inert or splits completely, then $v_{\mathfrak{p}}(b) = v_p(b)$, and so $v_{\mathfrak{p}}(b)$ is either $1/3$ or $2/3$ which is a contradiction. Therefore p is ramified, as desired.

Hence, p is ramified in K if and only if $p \mid b$ which implies that the primes occurring in Δ_K are exactly the primes that divide b. It remains to find the powers to which these primes appear in Δ_K. To answer this question we investigate if the ramification of primes is wild or tame. Note that if p is ramified, it is totally ramified so the ramification index of p is $e_p = 3$. Therefore, p is tamely ramified if and only if $p \neq 3$. If p is tamely ramified, then $p^{e_p - 1} = p^2$ is the exact power of p dividing Δ_K [2, page 21]. If 3 is ramified, then 3^3 divides $\Delta_K = D^2$, which is a square in $\mathbb{Z}$. Therefore $3^4 \mid \Delta_K$. Suppose for a contradiction that $3^5 \mid \Delta_K$. Since Δ_K is a square, this would force $3^6 \mid \Delta_K$. But then $3^3 \mid D$, so $D \equiv 0 \pmod{27}$, a contradiction. Therefore if 3 is ramified, 3^4 is the exact power of 3 dividing Δ_K. It follows that

$$\Delta_K = \begin{cases} (\prod_{p|b} p)^2 & \text{if } 3 \nmid b \\ (3\prod_{p|b} p)^2 & \text{if } 3 \mid b, \end{cases}$$

as desired. □

Corollary 22. *If $D = m^2 + 3m + 9$ is square-free, then $\{1, \rho, \rho^2\}$ is an integral basis for K and $\{-1, \rho, \rho'\}$ generates the full group of units $\mathcal{O}_K$.*

Proof. The fact that $\{1, \rho, \rho^2\}$ forms an integral basis for K if $m^2 + 3m + 9$ is square-free is a well-known result in algebraic number theory. The statement about the group of units $\mathcal{O}_K^\times$ is can be found in [15]. □

Next, we establish a lemma about the prime 2.

Lemma 23. *If D is square-free, then 2 is inert in K.*

Proof. As D is square-free, Corollary 22 implies that $\mathcal{O}_K = \mathbb{Z}[\rho]$. Reducing $f(x)$ modulo 2 we have

$$\overline{f}(x) \equiv x^3 + \overline{m}x^2 - \overline{(m+3)}x + 1 \equiv \begin{cases} x^3 + x^2 + 1 \pmod{2} & \text{if } m \text{ is odd} \\ x^3 + x + 1 \pmod{2} & \text{if } m \text{ is even.} \end{cases}$$

In either case, $\overline{f}(x)$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$, so 2 is inert in K by Theorem 5. □

3.2 Divisibility of class numbers of simplest cubic fields

Recall that $K = \mathbb{Q}(\rho)$, where ρ is a zero of the polynomial $f(x)$. The goal of this section is to obtain results about the divisibility of the class number of K. Proposition 24 uses rational solutions to $y^n = f(x)$ to obtain information about possible elements of order n in the class group of K. Theorem 26 gives congruence conditions that allow us to determine if the ideals studied in Proposition 24 are of order n. Hence, we obtain information about the divisibility of the class number of K by studying the order of ideal classes.

Proposition 24. *Let $n \geq 2$ be an integer. Let $x, y \in \mathbb{Q}$ and suppose*

$$y^n = x^3 + mx^2 - (m+3)x + 1.$$

Let $D = m^2 + 3m + 9$ be the square root of the discriminant of $f(x) = x^3 + mx^2 - (m + 3)x + 1$. Write $D = bc^3$ with $b, c \in \mathbb{Z}$ and b cube-free. If D is not cube-free, we also assume that the the numerator of $x^2 - x + 1$, the numerator of y, and c are mutually relatively prime (not necessarily pairwise). If $n \not\equiv 0 \pmod 3$ or if $x \in \mathbb{Z}$, then the principal ideal $\langle x - \rho \rangle$ is the n-th power of an ideal of K. If $x \notin \mathbb{Z}$ and $n \equiv 0 \pmod 3$, then the principal ideal $\langle x - \rho \rangle$ is the $(n/3)$-rd power of an ideal.

Proof. Let $\mathfrak{p}$ be a prime ideal of K. First we show that the proposition holds for the denominator of $x - \rho$. Write $x = \alpha/\beta$ for some nonzero $\alpha, \beta \in \mathbb{Z}$ such that α and β are relatively prime. Assume that $\mathfrak{p}^a$ is the largest power of $\mathfrak{p}$ that divides $\langle \beta \rangle$. It follows that the largest power of $\mathfrak{p}$ that divides $\langle \beta^3 \rangle$ is $\mathfrak{p}^{3a}$. We claim that $\mathfrak{p}^{3a}$ is the exact power of $\mathfrak{p}$ that divides the denominator of $\langle y^n \rangle$. Since the denominator of y^n comes only from x, the exact power of $\mathfrak{p}$ dividing the denominator of $\langle y^n \rangle$ is at most $\mathfrak{p}^{3a}$. If $\mathfrak{p}$ divides the numerator of y^n, then $\mathfrak{p}$ divides one of $\langle \alpha - \beta\rho \rangle, \langle \alpha - \beta\rho' \rangle, \langle \alpha - \beta\rho'' \rangle$. In any case, this implies that $\mathfrak{p} \mid \langle \alpha \rangle$ since $\mathfrak{p} \mid \langle \beta \rangle$. But then the unique rational prime p lying under $\mathfrak{p}$ divides both α and β, a contradiction since $\gcd(\alpha, \beta) = 1$. Therefore, $\mathfrak{p}^{3a}$ is the exact power of $\mathfrak{p}$ dividing the denominator of $\langle y^n \rangle$.

Now, write the denominator of $\langle y^n \rangle$ as $\mathfrak{p}^{3a}\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ for distinct prime ideals $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Since $\langle y^n \rangle$ is the n-th power of an ideal, we must have $\mathfrak{p}^{e_i} = (\mathfrak{p}^{m_i})^n$ for some $m_i \in \mathbb{Z}$. It follows that $e_i = m_i n$, so $n \mid e_i$ for each e_i. In particular, $n \mid 3a$.

If $n \not\equiv 0 \pmod 3$ then $n \mid a$, so $\langle \beta \rangle = \mathfrak{p}^{3a}\mathfrak{a} = \mathfrak{p}^{nm}\mathfrak{a}$ for some ideal $\mathfrak{a}$ relatively prime to $\mathfrak{p}$. This holds for every prime divisor of $\langle \beta \rangle$, so $\langle \beta \rangle$ is the n-th power of an ideal of K. If $n \equiv 0 \pmod 3$, then $\frac{n}{3} \mid a$. Replacing n with $n/3$ in the previous argument gives that in this case, $\langle \beta \rangle$ is the $n/3$-rd power of an ideal in $\mathcal{O}_K$.

Now we deal with the numerator of $x - \rho = \alpha/\beta$. Assume that $\mathfrak{p}^a$ is the exact power of $\mathfrak{p}$ dividing the numerator of $\langle \alpha \rangle$. Let $p \in \mathbb{Z}$ be the unique rational prime lying under $\mathfrak{p}$.

If p is ramified in K then $\mathfrak{p}$ is totally ramified since $[K : \mathbb{Q}] = 3$. Thus $\sigma(\mathfrak{p}) = \mathfrak{p}$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathfrak{p}^a$ be the exact power of $\mathfrak{p}$ dividing $\langle x - \rho \rangle$ and write $\langle x - \rho \rangle = \mathfrak{p}^a\mathfrak{q}$ with $\mathfrak{p} \nmid \mathfrak{q}$. Then for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,

$$\langle x - \sigma(\rho) \rangle = \sigma(\langle x - \rho \rangle) = \sigma(\mathfrak{p}^a\mathfrak{q}) = \sigma(\mathfrak{p})^a\sigma(\mathfrak{q}) = \mathfrak{p}^a\sigma(\mathfrak{q}).$$

If $\mathfrak{p} \mid \sigma(\mathfrak{q})$, then for some ideal $\mathfrak{a}$, $\sigma(\mathfrak{q}) = \mathfrak{p}\mathfrak{a} = \sigma(\mathfrak{p})\mathfrak{a}$. Applying σ^{-1} gives $\mathfrak{q} = \mathfrak{p}\sigma^{-1}(\mathfrak{a})$ which implies that $\mathfrak{p} \mid \mathfrak{q}$, a contradiction. Therefore $\mathfrak{p}^a$ is the exact power of $\mathfrak{p}$ dividing $\langle x - \sigma(\rho) \rangle$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Note that $\langle x - \sigma(\rho) \rangle$ is either $\langle x - \rho \rangle$, $\langle x - \rho' \rangle$, or $\langle x - \rho'' \rangle$.

Now, $y^n = (x - \rho)(x - \rho')(x - \rho'')$, so $\mathfrak{p}^{3a}$ is the exact power of $\mathfrak{p}$ dividing $\langle y^n \rangle$. As when we were dealing with the denominator, we must have $n \mid 3a$. If $n \not\equiv 0 \pmod 3$, then $n \mid a$ and so $\mathfrak{p}$ is the n-th power of an ideal. If $n \not\equiv 0 \pmod 3$, then $\frac{n}{3} \mid a$ and so $\mathfrak{p}$ is the $n/3$-rd power of an ideal.

Now suppose that p is unramified in K. We will show later that $\mathfrak{p} \nmid \langle x - \rho' \rangle \langle x - \rho'' \rangle$, so by the unique factorization of ideals in $\mathcal{O}_K$ it follows that $\mathfrak{p}^a$ is the exact power of $\mathfrak{p}$ that divides

$\langle y^n\rangle = \langle x-\rho\rangle\langle x-\rho'\rangle\langle x-\rho''\rangle$. Therefore $n \mid a$ and so $\mathfrak{p}$ is the n-th power of an ideal. Note that if $n \equiv 0 \pmod 3$ then $\mathfrak{p}$ is also an $n/3$-rd power of an ideal.

Hence, any prime $\mathfrak{p}$ dividing the numerator of $\langle x-\rho\rangle$ is an n-th power of an ideal if $n \not\equiv 0 \pmod 3$ and is an $n/3$-rd power of an ideal if $n \equiv 0 \pmod 3$, as desired.

Hence, it suffices to show that if p is unramified in K then $\mathfrak{p} \nmid \langle x-\rho'\rangle\langle x-\rho''\rangle$. Suppose for contradiction that $\mathfrak{p}$ is unramified and either $\mathfrak{p} \mid \langle x-\rho'\rangle$ or $\mathfrak{p} \mid \langle x-\rho''\rangle$. Without loss of generality assume $\mathfrak{p} \mid \langle x-\rho'\rangle$. It follows that $\mathfrak{p} \mid \langle x-\rho'-(x-\rho)\rangle = \langle \rho-\rho'\rangle$. Recall that D^2 is the discriminant of $f(x)$, so $D = (\rho-\rho')(\rho-\rho'')(\rho'-\rho'')$. Therefore, $\mathfrak{p} \mid \langle D\rangle$.

For the next part of the proof we work in local rings. We know that $x-\rho \equiv 0 \pmod{\mathfrak{p}}$. By this we mean that $\mathfrak{p}$ divides the numerator of $x-\rho$. Similarly, $\rho-\rho' \equiv 0 \pmod{\mathfrak{p}}$. Let $\mathcal{O}_{K\mathfrak{p}}$ denote the localization of $\mathcal{O}_K$ at $\mathfrak{p}$ and $\mathfrak{p}_\mathfrak{p}$ the localization of $\mathfrak{p}$ at $\mathfrak{p}$. That is,

$$\mathcal{O}_{K\mathfrak{p}} = \left\{\frac{r}{s} \mid r \in \mathcal{O}_K, s \in \mathcal{O}_K \setminus \mathfrak{p}\right\}$$

and

$$\mathfrak{p}_\mathfrak{p} = \left\{\frac{r}{s} \mid r \in \mathfrak{p}, s \in \mathcal{O}_K \setminus \mathfrak{p}\right\}.$$

We know that $x-\rho \in \mathfrak{p}$ and $1 \in \mathcal{O}_K$, so $\frac{x-\rho}{1} \in \mathfrak{p}_\mathfrak{p}$. Hence $x-\rho = 0$ in $(\mathcal{O}_{K\mathfrak{p}})/\mathfrak{p}_\mathfrak{p}$, so $x=\rho$ in $(\mathcal{O}_{K\mathfrak{p}})/\mathfrak{p}_\mathfrak{p}$. Similarly, $\rho-\rho' \in \mathfrak{p}$, so $\frac{\rho-\rho'}{1} \in \mathfrak{p}_\mathfrak{p}$. Thus, $\rho=\rho'$ in $(\mathcal{O}_{K\mathfrak{p}})/\mathfrak{p}_\mathfrak{p}$. Recall that in $\mathcal{O}_K$, $\rho' = \frac{1}{1-\rho}$. So long as $1-\rho \notin \mathfrak{p}$, we can use $x=\rho=\rho'$ in $(\mathcal{O}_{K\mathfrak{p}})/\mathfrak{p}_\mathfrak{p}$ to get $x = \frac{1}{1-x}$. Note that if $1-\rho \in \mathfrak{p}$ then $1 = \rho'(1-\rho) \in \mathfrak{p}$ since $\mathfrak{p}$ is an ideal. But $\mathfrak{p}$ is a prime ideal, so $1 \notin \mathfrak{p}$, a contradiction. Therefore, $x = \frac{1}{1-x}$ in $(\mathcal{O}_{K\mathfrak{p}})/\mathfrak{p}_\mathfrak{p}$. Multiplying through by $1-x$ gives $x^2-x+1 = 0 \pmod{\mathfrak{p}}$. Hence, $\mathfrak{p}$ divides the numerator of x^2-x+1.

Recall that we are assuming that p is unramified. We showed above that this is true if and only if $p \nmid b$, where $D = bc^3$ with $b, c \in \mathbb{Z}$ and b cube-free. Since $\mathfrak{p} \mid \langle \rho-\rho'\rangle$, it follows that $\mathfrak{p} \mid \langle D\rangle$. Since $\mathfrak{p}$ is prime, either $\mathfrak{p} \mid \langle b\rangle$ or $\mathfrak{p} \mid \langle c\rangle$. If $\mathfrak{p} \mid \langle b\rangle$, then $\langle b\rangle = \mathfrak{p}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_K$. Intersecting with $\mathbb{Z}$ gives $b\mathbb{Z} = (\mathfrak{p}\cap\mathbb{Z})(\mathfrak{a}\cap\mathbb{Z}) = (p\mathbb{Z})(a\mathbb{Z})$ for some $a \in \mathbb{Z}$. But this implies that $p \mid b$, which is a contradiction. Therefore, $\mathfrak{p} \mid \langle c\rangle$.

Furthermore, we claim that $\mathfrak{p} \mid \langle x-\rho\rangle$ implies that $\mathfrak{p} \mid \langle y\rangle$. To see this, recall that by $\mathfrak{p} \mid \langle x-\rho\rangle$ we mean that $\mathfrak{p}$ divides the numerator of $x-\rho$ and similarly for $\mathfrak{p} \mid \langle y\rangle$. We know that $y^n = (x-\rho)(x-\rho')(x-\rho'')$. Since $\rho, \rho', \rho'' \in \mathcal{O}_K$, the denominator of y^n comes from x. Since $x \in \mathbb{Q}$, write $x = m/z$ for $m, z \in \mathbb{Z}, z \neq 0$. Then the denominator of y^n is z^3. If $\mathfrak{p}$ divides the numerator of $x-\rho$, it does not divide the denominator, so it follows that $\mathfrak{p}$ divides the numerator of y^n. Since $\mathfrak{p}$ is prime, it must divide the numerator of y, as claimed.

We have shown that $\mathfrak{p}$ is a common divisor of c, the numerator of x^2-x+1 and the numerator of y. But this contradicts the assumption that these three quantities were mutually relatively prime. It follows that if $\mathfrak{p}$ divides the numerator of $x-\rho$ then $\mathfrak{p}$ must either be ramified or $\mathfrak{p} \nmid (x-\rho')(x-\rho'')$, as desired. $\square$

The following lemma will be useful in the proof of the next proposition.

Lemma 25. *Let p be a prime that splits completely in K. Let $\ell \in \mathbb{Z}$ be a prime and $m \in \mathbb{Z}, a \in \mathcal{O}_K$ satisfy*

$$m^x \equiv a^\ell \pmod{\mathfrak{p}}.$$

If $\ell \nmid x$ then m is an ℓ-power residue modulo p.

Proof. If $\ell \nmid x$ then $\gcd(x, \ell) = 1$. Therefore there are $r, s \in \mathbb{Z}$ such that $r\ell + sx = 1$. Hence,

$$m = m^1 = m^{r\ell+sx} = m^{r\ell}\left(m^x\right)^s \equiv m^{r\ell}\left(a^\ell\right)^s \equiv \left(m^r a^s\right)^\ell \pmod{\mathfrak{p}}.$$

Therefore m is an ℓ-th power residue modulo $\mathfrak{p}$. Since p splits in K, it follows that $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. Therefore, m is an ℓ-th power residue modulo p, as desired. □

The following result was first proved by Uchida in [18]. It provides congruence conditions for when the ideal $\langle -1-\rho \rangle$ is the n-th power of an ideal and is not the k-th power of an ideal for any $k < n$. In particular, this result gives conditions that guarantee that the class number of K is divisible by n.

Theorem 26. *Suppose $(-1, y)$ satisfies the hypotheses of Proposition 24 (so $y^n = 2m + 3$) and $m \not\equiv 0 \pmod 3$. Assume that for each prime factor ℓ of n there exist corresponding prime factors p and q of y such that 2 is an ℓ-th power nonresidue modulo both p and q and such that 3 is an ℓ-th power residue modulo p and an ℓ-th power nonresidue modulo q. Then the ideal $\langle -1-\rho \rangle$ is the n-th power of an ideal I whose ideal class has order n.*

Proof. The beginning of the proof holds for any prime dividing y and thus holds for the primes p and q fixed in the theorem. We will specifically state if we are referring to the fixed primes p and q of the theorem; otherwise p will be any prime dividing y.

First we establish that $\langle -1-\rho \rangle$ is the n-th power of an ideal I of $\mathcal{O}_K$. Let p be a prime such that $p \mid y$, so $p \mid y^n = (-1-\rho)(-1-\rho')(-1-\rho'')$. We claim that we can choose a prime $\mathfrak{p}$ lying over p such that $\mathfrak{p} \mid \langle -1-\rho \rangle$. To see this, note that since $\mathfrak{p}$ is prime and $\mathfrak{p} \mid \langle p \rangle \mid \langle (-1-\rho)(-1-\rho')(-1-\rho'') \rangle$, it must be that $\mathfrak{p} \mid \sigma(\langle -1-\rho \rangle)$ for some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Suppose that $\mathfrak{p} \mid \langle -1-\rho' \rangle$. Then there is some ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that $\langle -1-\rho \rangle = \mathfrak{p}\mathfrak{a}$. Then

$$\sigma_3(\mathfrak{p})\sigma_3(\mathfrak{a}) = \sigma_3(\mathfrak{p}\mathfrak{a}) = \sigma_3(\langle -1-\rho' \rangle) = \langle -1-\rho \rangle.$$

Thus, $\sigma_3(\mathfrak{p}) \mid \langle -1-\rho \rangle$ and $\sigma_3(\mathfrak{p})$ is a prime ideal lying over p since the elements of the Galois group permute the primes lying over a given prime. Similarly, if $\mathfrak{p} \mid \langle -1-\rho'' \rangle$ then $\sigma_2(\mathfrak{p})$ is a prime lying over p such that $\sigma_2(\mathfrak{p}) \mid \langle -1-\rho \rangle$. Hence, it is possible to choose $\mathfrak{p}$ lying over p such that $\mathfrak{p} \mid \langle -1-\rho \rangle$.

Using the fact that $\rho' = \frac{1}{1-\rho}$ and $\rho'' = 1 - 1/\rho$, it follows that

$$\rho' \equiv 1/2 \pmod{\mathfrak{p}} \quad \text{and} \quad \rho'' \equiv 2 \pmod{\mathfrak{p}}. \tag{13}$$

We claim that p splits in K. To see this, note that if p does not split in K then there is a unique prime $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p. Thus, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q}), \sigma(\mathfrak{p}) = \mathfrak{p}$. We know that $\mathfrak{p} \mid \sigma\langle -1-\rho\rangle$ for some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. As described above, the conjugates of $\mathfrak{p}$ must divide the conjugates of $\sigma\langle -1-\rho\rangle$. Since $\mathfrak{p}$ is only conjugate to itself it follows that $\mathfrak{p} \mid \sigma\langle -1-\rho\rangle$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Hence, $\rho \equiv \rho' \equiv \rho'' \equiv 0 \pmod{\mathfrak{p}}$. But this implies that $-1 \equiv \rho \equiv \rho'' \equiv 2 \pmod{\mathfrak{p}}$, so $3 \in \mathfrak{p}$. Hence $p = 3$ since each prime ideal of $\mathcal{O}_K$ lies over a unique prime in $\mathbb{Z}$. However, $3 \mid y$ implies that $2m \equiv 2m + 3 = y^n \equiv 0 \pmod 3$ and so $m \equiv 0 \pmod 3$, a contradiction. Therefore, it must be that p splits completely in K.

Note that $f(x) \equiv x^3 + x^2 + 2x + 1 \pmod 3$ or $f(x) \equiv x^3 + 2x^2 + x + 1 \pmod 3$. Using the fact that $m \not\equiv 0 \pmod 3$ and Theorem 5, it follows that 3 never splits in K. Hence, 3 is not a prime dividing y.

Note that if p^a is the exact power of p dividing y, then p^{an} is the exact power of p dividing $y^n = (-1-\rho)(-1-\rho')(-1-\rho'')$. Since p splits, there is exactly one $\mathfrak{p}$ lying over p such that $\mathfrak{p} \mid \langle -1-\rho\rangle$. In fact, $\mathfrak{p}^{an}$ is the exact power of $\mathfrak{p}$ dividing $\langle -1-\rho\rangle$. Let $p_1, \ldots, p_r$ be the primes dividing y and let $p_i^{a_i}$ be the exact power of p_i dividing y. For each i, there is a unique prime $\mathfrak{p}_i$ lying over p_i such that $\mathfrak{p}_i \mid \langle -1-\rho\rangle$. Then

$$\langle -1-\rho\rangle = \mathfrak{p}_1^{a_1 n} \cdots \mathfrak{p}_r^{a_r n} = \left(\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}\right)^n.$$

Let $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$. Then $\langle -1-\rho\rangle = I^n$, as desired. It remains to show that every smaller power of I is not principal.

If $D = M^2 + 3m + 9$ is square-free, then Corollary 22 implies that the group $E = \langle -1, \rho, \rho'\rangle$ is the full group of units $\mathcal{O}_K^\times$. In general, however, this is not the case.

The goal of the next part of the proof is to show that n is relatively prime to $[\mathcal{O}_K^\times : E]$. This is helpful in establishing that I^ℓ is not principal for any divisor ℓ of n. We do this by considering each prime that divides n separately. Throughout the remainder of the proof, p and q are the fixed primes referred to in the statement of the theorem.

For ease of notation, let $m = \left[\mathcal{O}_K^\times : E\right]$. Let ℓ be a prime dividing n and suppose $\ell \mid m$. We will see that there is a unit ε such that $\varepsilon^\ell = \pm\rho^a\left(\rho'\right)^b$, where $a, b \in \mathbb{Z}$ and ℓ does not divide both a and b. We have $\ell \mid m = |\mathcal{O}_K^\times/E|$. Since ℓ is prime, there is some $\varepsilon_1 E \in \mathcal{O}_K^\times/E$ such that $\varepsilon_1 E$ has order ℓ. Thus, $\varepsilon_1^\ell \in E = \langle -1, \rho, \rho'\rangle$. Hence, we can write

$$\varepsilon_1^\ell = \pm\rho^c\left(\rho'\right)^d,$$

for some $c, d \in \mathbb{Z}$. Since $\varepsilon_1, \rho, \rho' \in \mathcal{O}_K^\times$, for any $v, w \in \mathbb{Z}, \varepsilon_1\rho^v\left(\rho'\right)^w \in \mathcal{O}_K^\times$. Thus,

$$\left(\varepsilon_1\rho^v\left(\rho'\right)^w\right)^\ell = \varepsilon_1^\ell\rho^{v\ell}\left(\rho'\right)^{w\ell} = \pm\rho^{c+v\ell}\left(\rho'\right)^{d+w\ell}.$$

By the division algorithm we can write $c = q_1\ell + a$ and $d = q_2\ell + b$ with $0 \leq a, b < \ell$. Let $\varepsilon = \varepsilon_1\rho^{-q_1}\left(\rho'\right)^{-q^2}$. Then

$$\begin{aligned}
\varepsilon^\ell &= \varepsilon_1^\ell\rho^{-q_1\ell}\left(\rho'\right)^{-q_2\ell} \\
&= \pm\rho^c\left(\rho'\right)^d\rho^{-q_1\ell}\left(\rho'\right)^{-q_2\ell} \\
&= \pm\rho^{q_1\ell+a-q_1\ell}\left(\rho'\right)^{q_2+b-q_2\ell} \\
&= \pm\rho^a\left(\rho'\right)^b.
\end{aligned}$$

Hence, there is some $\varepsilon \in \mathcal{O}_K^\times$ such that $\varepsilon^\ell = \pm\rho^a\left(\rho'\right)^b$ with $0 \leq a, b < \ell$. Note that if $a = b = 0$ then $\varepsilon^\ell = \pm 1 \in E$, so either $\varepsilon^\ell = 1$ or $(-\varepsilon)^\ell = 1$ so long as ℓ is odd. If $\ell = 2$ and $\varepsilon^2 = -1$ then $x^2 + 1$ is reducible over K and so $i = \sqrt{-1} \in K$. But $K \subseteq \mathbb{R}$ so this is a contradiction. Thus, if $\ell = 2$ then $\varepsilon^2 = 1$. Without loss of generality, assume $\varepsilon^\ell = 1$. The same argument can be made with $-\varepsilon$ in place of ε if necessary. Since ℓ is prime, ε has order 1 or ℓ. If $|\varepsilon| = 1$, then $\varepsilon = 1$ so $1 = \varepsilon_1\rho^{-q_1}\left(\rho'\right)^{-q_2}$. Hence, $\varepsilon_1 = \rho^{q_1}\left(\rho'\right)^{q_2} \in \langle -1, \rho, \rho' \rangle = E$. But this contradicts the assumption that $\varepsilon_1 E$ has order ℓ in $\mathcal{O}_K^\times/E$. Hence, $|\varepsilon| = \ell$. Recall that $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$, so there are no elements of order ℓ. Hence, we have reached a contradiction, so it must be that at least one of a, b is nonzero, as claimed. Therefore, there is some $\varepsilon \in \mathcal{O}_K^\times$ such that $\varepsilon^\ell = \pm\rho^a\left(\rho'\right)^b$ where $a, b \in \mathbb{Z}$ and not both a and b are divisible by ℓ.

First suppose that ℓ is odd. Then, by possibly replacing ε with $-\varepsilon$, we may assume that $\varepsilon^\ell = \rho^a\left(\rho'\right)^b$ with $a, b \in \mathbb{Z}$ and a, b not both divisible by ℓ. Hence,

$$\varepsilon^\ell = \rho^a\left(\rho'\right)^b \equiv (-1)^a(1/2)^b \equiv (-1)^a 2^{-b} \pmod{\mathfrak{p}}.$$

Since we are assuming that 2 is not an ℓ-th power modulo p, it follows that $b \equiv 0 \pmod{\ell}$ by Lemma 25. Now, let $\varepsilon' = \sigma_2(\varepsilon)$. Then

$$\left(\varepsilon'\right)^\ell = \left(\rho'\right)^a\left(\rho''\right)^b \equiv (1/2)^a 2^b \equiv 2^{b-a} \pmod{\mathfrak{p}}.$$

Again by Lemma 25, it follows that $b - a \equiv 0 \pmod{\ell}$ and so $a \equiv b \equiv 0 \pmod{\ell}$. But this contradicts the assumption that at least one of a and b is not divisible by ℓ. Therefore, any odd prime ℓ dividing n cannot divide $[\mathcal{O}_K^\times : E]$.

Now suppose that $\ell = 2$, $\ell \mid n$ and $\ell \mid m$. Then $\varepsilon^2 = \pm\rho^a\left(\rho'\right)^b$. Note that for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\varepsilon^2) = (\sigma(\varepsilon))^2 > 0$ since $K \subset \mathbb{R}$. We know that $\sigma(\varepsilon^2) \neq 0$ since $\varepsilon \in \mathcal{O}_K^\times$. Hence, ε^2 is totally positive, so we must have $\pm\rho^a\left(\rho'\right)^b$ totally positive as well. In particular we need

$$\pm\rho^a\left(\rho'\right)^b = \sigma_1\left(\pm\rho^a\left(\rho'\right)^b\right) > 0 \tag{14}$$

$$\pm\left(\rho'\right)^a\left(\rho''\right)^b = \sigma_2\left(\pm\rho^a\left(\rho'\right)^b\right) > 0 \tag{15}$$

$$\pm\left(\rho''\right)^a\rho^b = \sigma_3\left(\pm\rho^a\left(\rho'\right)^b\right) > 0. \tag{16}$$

We know from the inequalities in (8) that $0 < \rho' < \rho''$, so (15) implies that it is necessary to have the $+$ sign. Since $\rho < 0$, (14) implies that $a \in 2\mathbb{Z}$ and (16) implies that $b \in 2\mathbb{Z}$. But then $a \equiv b \equiv 0 \pmod 2$, which is a contradiction to the assumption that $\ell = 2$ does not divide both a and b. Hence, if $2 \mid n$ then $2 \nmid m$. We have shown that n and m must be relatively prime.

Now suppose that $\langle -1-\rho \rangle = \langle \alpha \rangle^{\ell}$ for some $\alpha \in \mathcal{O}_K$ and some prime ℓ dividing n, so $\ell \nmid m$. As ℓ and m are relatively prime, there exist $r, s \in \mathbb{Z}$ such that $r\ell + sm = 1$. Since $-1-\rho$ and α^{ℓ} generate the same ideal, we can write $-1-\rho = \varepsilon_0 \alpha^{\ell}$ for some $\varepsilon_0 \in \mathcal{O}_K^{\times}$. Note that $\varepsilon_0^m \in E$. Let $\alpha_1 = \varepsilon_0^r \alpha$. Then

$$-1-\rho = \varepsilon_0 \alpha = \varepsilon_0 \varepsilon_0^{-r\ell} \left(\varepsilon^r \alpha\right)^{\ell} = \varepsilon_0^{sm} \alpha_1^{\ell},$$

with $\varepsilon_0^{sm} \in E$. Let $\varepsilon = \varepsilon_0^{sm}$ and write $\varepsilon = \pm \rho^a (\rho')^b$ for some $a, b \in \mathbb{Z}$. Hence

$$-1-\rho = \pm \rho^a (\rho')^b \alpha_1^{\ell}.$$

Applying σ_2 to the above equation we obtain

$$-1-\rho' = \pm \left(\rho'\right)^a \left(\rho''\right)^b \left(\sigma_2\left(\alpha_1\right)\right)^{\ell}. \tag{17}$$

Letting $\sigma_2\left(\alpha_1\right) = \alpha_1' \in \mathcal{O}_K$, we have $-1-\rho' = \pm \left(\rho'\right)^a \left(\rho''\right)^b \left(\alpha_1'\right)^{\ell}$. Using the congruences in (13) we have

$$-\frac{3}{2} \equiv \pm 2^{b-a} \left(\alpha_1'\right)^{\ell} \pmod{\mathfrak{p}} \quad \text{and} \quad -\frac{3}{2} \equiv \pm 2^{b-a} \left(\alpha_1'\right)^{\ell} \pmod{\mathfrak{q}}.$$

We are trying to reach a contradiction so that we can conclude that $\langle -1-\rho \rangle \neq \langle \alpha \rangle^{\ell}$ for any prime ℓ dividing n. The contradiction will come from the assumptions about when 2 and 3 are ℓ-th power residues modulo p and q. First consider the case when ℓ is an odd prime. Then by replacing α_1' with $-\alpha_1'$ if necessary, we have $\frac{3}{2} \equiv 2^{b-a}\left(\alpha_1'\right)^{\ell} \pmod{\mathfrak{p}}$. This will help us show that $b-a+1 \equiv 0 \pmod{\ell}$. Note that if $3 \equiv 0 \pmod p$ then $p = 3$, a contradiction since $3 \nmid y$. Hence, $\alpha_1' \neq 0$, so it has an inverse in $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$. Recall that 3 is an ℓ-th power residue modulo p, so $3 \equiv m^{\ell} \pmod p$ for some $m \in \mathbb{Z}/p\mathbb{Z}$. Thus, $\left(\frac{m}{\alpha_1'}\right)^{\ell} = 2^{b-a+1} \pmod{\mathfrak{p}}$. It follows from Lemma 25 that $b-a+1 \equiv 0 \pmod{\ell}$. Therefore, we can write $b-a+1 = \ell x$ for some $x \in \mathbb{Z}$. Then

$$3 \equiv 2^{b-a+1}\left(\alpha_1'\right)^{\ell} \equiv 2^{\ell x}\left(\alpha_1'\right)^{\ell} \equiv \left(2^x \alpha_1'\right)^{\ell} \pmod{\mathfrak{q}}.$$

So 3 is an ℓ-th power residue modulo $\mathfrak{q}$. But this is a contradiction because 3 was assumed not to be an ℓ-th power residue modulo $\mathfrak{q}$. Therefore $\langle -1-\rho \rangle$ is not the ℓ-th power of a principal ideal for any odd prime ℓ dividing n.

Now consider the case when $\ell = 2$. Since $-1-\rho' < 0$ and $0 < \rho' < \rho''$, (17) becomes

$$-1-\rho' = -\left(\rho'\right)^a \left(\rho''\right)^b \left(\alpha_1'\right)^2. \tag{18}$$

By applying σ_2 we obtain

$$0 > -1 - \rho'' = -\left(\rho''\right)^a \rho^b \left(\alpha_1''\right)^2,$$

where $\alpha_1'' = \sigma_2\left(\alpha_1'\right)$. This implies that b is even since $-\left(\rho''\right)^a \left(\alpha_1''\right)^2 < 0$. By applying $\sigma_3 = \sigma_2^{-1}$ we have

$$0 < -1 - \rho = -\rho^a \left(\rho'\right)^b \alpha_1^2.$$

We showed in (8) that $\rho < -1$, so this equation implies that a must be odd. Hence, $b - a$ is odd and $b - a + 1 \in 2\mathbb{Z}$. Thus, (18) yields

$$-\frac{3}{2} = -2^{b-a}\left(\alpha_1'\right)^2 \pmod{\mathfrak{q}}$$

and so $3 \equiv 2^{b-a+1}\left(\alpha_1'\right)^2 \pmod{\mathfrak{q}}$. By Lemma 25 this implies that 3 is a quadratic residue modulo q, which contradicts our assumption. Hence, $\langle -1 - \rho \rangle \neq \langle \alpha \rangle^\ell$ for any prime ℓ dividing n, so it must be that n is the smallest positive integer such that I^n is principal. Hence, $[I]$ has order n, as claimed. □

3.3 2-part of the class group of the simplest cubic fields

As above, let $K = \mathbb{Q}(\rho)$. Let E be the elliptic curve defined over $\mathbb{Q}$ by

$$y^2 = f(x) = x^3 + mx^2 - (m+3)x + 1,$$

where m satisfies the same assumptions as in Section 3.1. Furthermore, throughout this section we assume that $D = m^2 + 3m + 9$ is square-free.

In general, the free rank of an elliptic curve is difficult to compute as is the 2-part of the class group of K. A relationship between these would allow us to use elliptic curves to obtain information about the class group and vice versa. We establish such a relationship in Theorem 27. In Section 3.4 we use Theorem 27 to prove additional results and investigate some examples.

3.3.1 Properties of this elliptic curve

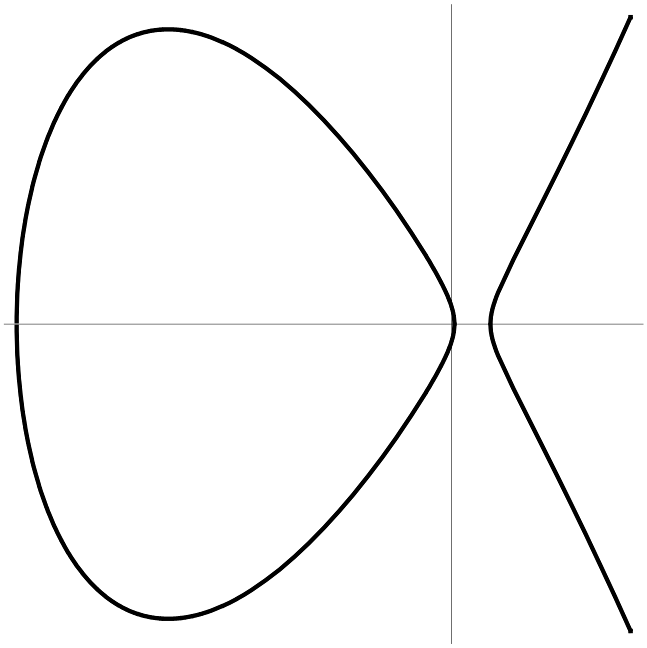
Let

$$E^\circ = \{P \in E \mid P = \infty \text{ or } P = (x, y) \text{ with } x \geq \rho''\}.$$

Note that E° forms a subgroup of E. Also, the sum of two points on $E - E^\circ$ is in E°. In particular, this means that $2E(\mathbb{Q}) \subseteq E^\circ(\mathbb{Q})$. We will write $\mathrm{rk}(E(\mathbb{Q}))$ for the free rank of $E(\mathbb{Q})$.

Let C be the ideal class group of K, where K is the cubic field defined above. Let $C_2 = \{x \in C \mid x^2 = 1\}$. That is, C_2 consists of all ideal classes such that squaring gives the ideal class of principal ideals. Let $\mathrm{rk}_2\left(C_2\right)$ be the dimension of C_2 as a $\mathbb{Z}/2\mathbb{Z}$-vector space.

Figure 1: Graph of $y^2 = x^3 + 11x^2 - 14x + 1$



3.3.2 Relating the elliptic curve to the class group

The goal of this section is to establish a relationship between the elliptic curve defined by $y^2 = f(x)$ and the 2-part of the class group K. We do this via an exact sequence. The primary goal of this section is to prove the following theorem.

Theorem 27. *There is an exact sequence*

$$1 \to E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \to C_2 \to Ш_2 \to 1.$$

The proof of this theorem relies on the maps λ_p as well as S_2 and $Ш_2$, defined at the end of Section 2.3. Note that since K is a totally real field, the infinite prime splits in K. Unless otherwise specified, the phrase "all primes p" includes the infinite primes. We will drop the inclusion maps of $K^\times / \left(K^\times\right)^2$ into the codomains of each λ_p when considering elements in S_2. In particular, we say that $\alpha \left(K^\times\right)^2 \in S_2$ if $\alpha \left(K^\times\right)^2 \in \operatorname{Im} \lambda_p$ for all primes p. Before proving Theorem 27, we develop several lemmas and propositions.

First we show how to obtain an element in C_2 from an element of S_2.

Proposition 28. *If $\alpha \left(K^\times\right)^2 \in S_2$, then $\langle \alpha \rangle = I^2$ for some (fractional) ideal I of K.*

Proof. We prove this by showing that $\langle\alpha\rangle$ has even valuation at all prime ideals of $\mathcal{O}_K$.

First suppose that p does not split in K. Since $\alpha\left(K^\times\right)^2 \in \operatorname{Im}\lambda_p$ there is some $x \in \mathbb{Q}_p$ such that $\lambda_p(x) = \alpha\left(K_p^\times\right)^2$. Then $\alpha\left(K_p^\times\right)^2 = (x-\rho)\left(K_p^\times\right)^2$ and so $x-\rho$ and α differ by a square in $K_p^\times$. Hence, we can look at $\langle x-\rho\rangle$ to understand the parity of the $\mathfrak{p}$-valuation of $\langle\alpha\rangle$. As there is only one prime ideal, say $\mathfrak{p}$, in K_p it follows that $\langle x-\rho\rangle = \mathfrak{p}^v$ for some $v \in \mathbb{Z}$.

Since p does not split in K, f is irreducible over $\mathbb{Q}_p$ as shown in Section 2.3. Hence $[\mathbb{Q}_p(\rho) : \mathbb{Q}_p] = 3$ and $\operatorname{Gal}\left(\mathbb{Q}_p(\rho)/\mathbb{Q}_p\right) \cong \operatorname{Gal}(K/\mathbb{Q})$. In fact, each element in $\operatorname{Gal}\left(\mathbb{Q}_p(\rho)/\mathbb{Q}_p\right)$ is an extension of an automorphism in $\operatorname{Gal}(K/\mathbb{Q})$. Recall from Section 12 that $\mathbb{Q}_p(\rho) = K_{\mathfrak{p}}$, so $\operatorname{Gal}\left(\mathbb{Q}_p(\rho)/\mathbb{Q}\right) = \operatorname{Gal}\left(K_{\mathfrak{p}}/\mathbb{Q}_p\right)$. Then for $\sigma \in \operatorname{Gal}\left(K_{\mathfrak{p}}/\mathbb{Q}_p\right)$,

$$\langle x-\sigma(\rho)\rangle = \sigma\left(\langle x-\rho\rangle\right) = \sigma\left(\mathfrak{p}^v\right) = \sigma\left(\mathfrak{p}\right)^v.$$

This implies that $v = v_{\mathfrak{p}}\left(\langle x-\rho\rangle\right) = v_{\mathfrak{p}}\left(\langle x-\rho'\rangle\right) = v_{\mathfrak{p}}\left(\langle x-\rho''\rangle\right)$.

Recall that $(x,y) \in E\left(\mathbb{Q}_p\right)$. Thus,

$$2v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}\left(y^2\right) = v_{\mathfrak{p}}\left((x-\rho)\left(x-\rho'\right)\left(x-\rho''\right)\right) = v_{\mathfrak{p}}(x-\rho) + v_{\mathfrak{p}}\left(x-\rho'\right) + v_{\mathfrak{p}}\left(x-\rho''\right) = 3v.$$

So $2 \mid v = v_{\mathfrak{p}}(x-\rho)$. If p is inert, then $v_{\mathfrak{p}} = v_p$, so $v_p(x-\rho)$ is also even. If p is ramified, then it is totally ramified and $v_{\mathfrak{p}} = 3v_p$. Hence, $v_p(x-\rho)$ is even. Therefore, any prime that does not split in K that divides $\langle x-\rho\rangle$ must divide $\langle x-\rho\rangle$ an even number of times. But since $\alpha\left(K_p^\times\right)^2 = (x-\rho)\left(K_p^\times\right)^2$, α differs from $x-\rho$ by a square, so the same holds for α.

Now suppose that p splits in K. Let $\alpha' = \sigma_2(\alpha)$ and $\alpha'' = \sigma_3(\alpha)$. Since $\alpha\left(K^\times\right)^2 \in S_2$, there is some $(x,y) \in E\left(\mathbb{Q}_p\right)$ such that

$$\left(\alpha, \alpha', \alpha''\right) = \lambda_p(x,y) = \left((x-\rho)\beta_1^2, \left(x-\rho'\right)\beta_2^2, \left(x-\rho''\right)\beta_3^2\right),$$

where $\beta_i \in \mathbb{Q}_p^\times$ for $i = 1,2,3$.

If $v_p(x-\rho) > 0$ and either $v_p\left(x-\rho'\right) > 0$ or $v_p\left(x-\rho''\right) > 0$, then either $v_p\left(\rho-\rho'\right) > 0$ or $v_p\left(\rho-\rho''\right) > 0$. Then $p \mid \left(\rho-\rho'\right)\left(\rho-\rho''\right)\left(\rho'-\rho''\right)$, so $p \mid D$. Recall that D is assumed to be square-free and thus cube-free. It follows from Proposition 21 that p ramifies in K, a contradiction.

Now suppose $v_p(x-\rho) > 0$ and $v_p\left(x-\rho'\right), v_p\left(x-\rho''\right) \leq 0$. Write $x = \frac{a}{b}$ for $a, b \in \mathbb{Z}_p, b \neq 0$ and a, b relatively prime. (Note that, the only prime in $\mathbb{Z}_p$ is p, so a, b relatively prime simply requires that both are not divisible by p.) Then b is the denominator of $x-\rho, x-\rho', x-\rho''$ since $\rho, \rho', \rho'' \in \mathbb{Z}_p$. Suppose for a contradiction that $p \mid b$. Since $v_p(x-\rho) > 0$, it follows that p divides the numerator of $x-\rho$, namely $a - b\rho$. Since $p \mid b$ this implies that $p \mid a$, a contradiction since a, b were assumed to be relatively prime. Thus, $p \nmid b$ and $v_p(x-\rho), v_p\left(x-\rho'\right), v_p\left(x-\rho''\right) \geq 0$. Hence, $v_p\left(x-\rho'\right) = 0 = v_p\left(x-\rho''\right)$. Thus,

$$\begin{aligned}
2v_p(y) = v_p\left(y^2\right) &= v_p\left((x-\rho)\left(x-\rho'\right)\left(x-\rho''\right)\right) \\
&= v_p(x-\rho) + v_p\left(x-\rho'\right) + v_p\left(x-\rho''\right) \\
&= v_p(x-\rho),
\end{aligned}$$

Table 4: Square residue classes in $\mathcal{O}_K/4\mathcal{O}_K$

$m \in \mathbb{Z}/4\mathbb{Z}$	Square residue classes $\pmod 4$							
0	$0,$	$1,$	$\rho+2,$	$\rho^2,$	$3\rho^2+3\rho,$	$\rho^2+2\rho+1,$	$\rho^2+3\rho+1,$	$2\rho^2+3\rho+3$
1	$0,$	$1,$	$3\rho+3,$	$\rho^2,$	$2\rho^2+\rho,$	$\rho^2+2\rho+1,$	$\rho^2+3\rho+1,$	$3\rho^2+3\rho+2$
2	$0,$	$1,$	$\rho+1,$	$\rho^2,$	$2\rho^2+3\rho,$	$\rho^2+\rho+2,$	$\rho^2+2\rho+1,$	$3\rho^2+\rho+3$
3	$0,$	$1,$	$3\rho+2,$	$\rho^2,$	$\rho^2+\rho,$	$\rho^2+2\rho+1,$	$2\rho^2+\rho+1,$	$3\rho^2+\rho+3$

so $v_p(x-\rho)$ is even.

If $v_p(x-\rho) < 0$ then, with notation as above, $p \mid b$. Then $v_p(x-\rho) = v_p(x-\rho') = v_p(x-\rho'') = v_p(1/b)$. Hence,

$$\begin{aligned} 2v_p(y) = v_p\left(y^2\right) &= v_p\left((x-\rho)\left(x-\rho'\right)\left(x-\rho''\right)\right) \\ &= v_p(x-\rho) + v_p\left(x-\rho'\right) + v_p\left(x-\rho''\right) \\ &= 3v_p(1/b), \end{aligned}$$

so $2 \mid v_p(1/b) = v_p(x-\rho)$.

Finally, if $v_p(x-\rho) = 0$ then $2 \mid v_p(x-\rho)$. Therefore, $\langle x-\rho\rangle$ has even valuation at all primes. Since $\langle\alpha\rangle$ and $\langle x-\rho\rangle$ differ by a square, it follows that $\langle\alpha\rangle$ has even valuation at all primes. Hence $\langle\alpha\rangle = I^2$ for some (fractional) ideal I of $\mathcal{O}_K$, as desired. □

The next two lemmas are needed in the proof of Proposition 31. In particular, Lemma 29 is needed to allow us to apply Theorem 12 to a particular extension. The argument in Lemma 30 is used several times in Section 3.3.2 and Section 3.4.

Lemma 29. *Let $x \in \mathcal{O}_K$ with $\langle x\rangle$ relatively prime to $\langle 2\rangle$. Then there exists $\varepsilon \in \mathcal{O}_K^\times$ such that εx is congruent to a square modulo 4.*

Proof. We begin with some observations about $\mathcal{O}_K/4\mathcal{O}_K$. Recall that we are assuming that $D = m^2+3m+9$ is square-free and hence by Corollary 22 $\mathcal{O}_K = \mathbb{Z}[\rho]$. Since an arbitrary element in $\mathcal{O}_K$ can be written in the form $a+b\rho+c\rho^2$ with $a,b,c \in \mathbb{Z}$, there are $4^3 = 64$ elements in $\mathcal{O}_K/4\mathcal{O}_K$. By squaring an arbitrary element in $\mathcal{O}_K$ and reducing the coefficients modulo 4, we obtain the square residue classes of $\mathcal{O}_K/4\mathcal{O}_K$. The results, given in Table 4, depend on the value of m modulo 4 and were computed using Mathematica [23].

Let G be the multiplicative group $(\mathcal{O}_K/4\mathcal{O}_K)^\times$. Then since 2 is inert in K

$$G = \left\{a+b\rho+c\rho^2 : a,b,c \in \mathbb{Z}/4\mathbb{Z} \text{ where at least one of } a,b,c \text{ is not even}\right\},$$

so $|G| = 56$. Let H be the set of all nonzero squares in G and L be the set of equivalence classes in $\mathcal{O}_K/4\mathcal{O}_K$ represented by $\{\pm 1, \pm\rho, \pm(1-\rho), \pm\left(\rho-\rho^2\right)\}$. It is tedious though not difficult to show that

$$G = LH = \{\ell h : \ell \in L \text{ and } h \in H\}.$$

Now, if $x \in \mathcal{O}_K$ and $\langle x\rangle$ is relatively prime to $\langle 2\rangle$, then $x + 4\mathcal{O}_K \in \left(\mathcal{O}_K/4\mathcal{O}_K\right)^\times$. Hence, we may write $x \equiv \ell h \pmod{4\mathcal{O}_K}$ for some $\ell \in L, h \in H$. Let $\varepsilon \in \mathcal{O}_K^\times$ such that $\varepsilon \equiv \ell \pmod{4\mathcal{O}_K}$. Then $\varepsilon^{-1}x \equiv h \pmod{4\mathcal{O}_K}$ with $h \in \left(\mathcal{O}_K/4\mathcal{O}_K\right)^2$. Hence there is a unit in $\mathcal{O}_K$, namely ε^{-1}, such that $\varepsilon^{-1}x$ is a square modulo 4, as claimed. □

Lemma 30. *If $\alpha \in K^\times$ is totally positive and relatively prime to 2 such that $\langle\alpha\rangle = I^2$ for some ideal I, then $K\left(\sqrt{\alpha}\right)/K$ is an unramified extension.*

Proof. By Lemma 29 there is some $\varepsilon \in \mathcal{O}_K^\times$ such that $\varepsilon\alpha$ is congruent to a square modulo 4. Since 2 is inert in K, Theorem 12 implies that $K\left(\sqrt{\varepsilon\alpha}\right)/K$ is unramified at 2. Also, $\langle\varepsilon\alpha\rangle = \langle\alpha\rangle = I^2$ is the square of an ideal, so $K\left(\sqrt{\varepsilon\alpha}\right)/K$ is unramified at all finite primes, again by Theorem 12. Now Corollary 10 implies that $K\left(\sqrt{\varepsilon\alpha}\right)/K$ is unramified at all infinite primes and is thus an unramified extension of K. Since K is totally real, it follows from Theorem 12 that $\varepsilon\alpha$ is totally positive. Since α was assumed to be totally positive, it must be that ε is also totally positive and hence a square in $\mathcal{O}_K^\times$. Therefore, $K\left(\sqrt{\varepsilon\alpha}\right) = K\left(\sqrt{\alpha}\right)$ and $K\left(\sqrt{\alpha}\right)/K$ is an unramified extension, as claimed. □

The following claim is a critical step in relating the elliptic curve E to the 2-part of the class group of K. Recall that S_2 is defined by the maps λ_p whose domain is $E\left(\mathbb{Q}_p\right)$. Thus S_2 contains information about E that we wish to connect to C_2. The homomorphism g, defined in Proposition 31, will allow us to relate C_2 to $E(\mathbb{Q})$ through a short exact sequence.

Proposition 31. *The map $g : S_2 \to C_2$ given by*

$$\alpha\left(K^\times\right)^2 \mapsto [I],$$

where I is an ideal such that $I^2 = \langle\alpha\rangle$, is a well-defined epimorphism.

Proof. Note that by Proposition 28, g maps into its codomain C_2. Now suppose that $\alpha\left(K^\times\right)^2 = \beta\left(K^\times\right)^2 \in S_2$. Then we may write $\alpha = \beta\gamma^2$ for some $\gamma \in K^\times$. By Proposition 28, there are ideals I, J such that $\langle\alpha\rangle = I^2$ and $\langle\beta\rangle = J^2$. Hence, $I^2 = \langle\alpha\rangle = \langle\beta\gamma^2\rangle = J^2\langle\gamma\rangle^2$. By unique factorization of ideals, $I = J\langle\gamma\rangle$. Therefore $[I] = [J]$ and so $g\left(\alpha\left(K^\times\right)^2\right) = g\left(\beta\left(K^\times\right)^2\right)$. Hence, g is a well defined function.

To see that g is a homomorphism, let $\alpha\left(K^\times\right)^2, \beta\left(K^\times\right)^2 \in S_2$. Then there are ideals I, J such that $I^2 = \langle\alpha\rangle$ and $J^2 = \langle\beta\rangle$, so $\langle\alpha\beta\rangle = I^2J^2 = (IJ)^2$. Then $g\left(\alpha\beta\left(K^\times\right)^2\right) = [IJ] = [I][J] = g\left(\alpha\left(K^\times\right)^2\right)g\left(\beta\left(K^\times\right)^2\right)$, as desired.

It remains to show that g maps onto C_2. Let $[I] \in C_2$. Without loss of generality, we may assume that $I \subseteq \mathcal{O}_K$. If $\langle 2 \rangle \mid I$ then write $I = \langle 2 \rangle^e \mathfrak{a}$ for some ideal $\mathfrak{a}$ prime to $\langle 2 \rangle$. Since I and $\mathfrak{a}$ differ by a principal ideal, $[I] = [\mathfrak{a}]$. Hence, without loss of generality assume that $\langle 2 \rangle \nmid I$. By definition of C_2, $I^2 = \langle \alpha \rangle$ for some $\alpha \in \mathcal{O}_K$. Note that by multiplying α by a unit with the same signature as α we obtain a totally positive generator of I^2. Hence, we will assume that α is totally positive. We will show that $\alpha \left(K^\times\right)^2 \in \operatorname{Im} \lambda_p$, for all primes p, and hence $\alpha \left(K^\times\right)^2 \in S_2$.

First consider $p = \infty$. Since $K \subseteq \mathbb{R}$, the infinite prime does not ramify so p splits. Hence $K_\infty = \mathbb{R}$, so $\left(K_\infty^\times\right)^2 = \mathbb{R}^+$. Let $x > \rho''$ and $(x, y) \in E(\mathbb{R})$. Then x is totally positive and so

$$\lambda_\infty(x) = \left((x-\rho)\mathbb{R}^+, (x-\rho')\,\mathbb{R}^+, (x-\rho'')\,\mathbb{R}^+\right) = \left(\mathbb{R}^+, \mathbb{R}^+, \mathbb{R}^+\right) = \left(\alpha\mathbb{R}^+, \alpha'\mathbb{R}^+, \alpha''\mathbb{R}^+\right).$$

Thus, $\alpha \left(K^\times\right)^2 \in \operatorname{Im} \lambda_\infty$.

Since I was chosen to be relatively prime to 2 and $\langle \alpha \rangle = I^2$, it follows that α is relatively prime to 2. By Lemma 30, $K\left(\sqrt{\alpha}\right)/K$ is an unramified extension.

Next we show that $\alpha \left(K^\times\right)^2 \in \operatorname{Im} \lambda_p$ if p is inert in $K/\mathbb{Q}$. If p is inert in K, then $\langle p \rangle$ is a principal prime ideal. As $K\left(\sqrt{\alpha}\right)/K$ is unramified, Corollary 8 implies that p splits in $K\left(\sqrt{\alpha}\right)$. Therefore, $x^2 - \alpha$ splits into two linear factors modulo p. By Theorem 2, $x^2 - \alpha$ has a root in K_p. Thus, $\alpha \in \left(K_p^\times\right)^2$. Hence, $\alpha\left(K_p^\times\right)^2 = \left(K_p^\times\right)^2 \in \operatorname{Im} \lambda_p$ since $\left(K_p^\times\right)^2$ is the identity element in $K_p^\times / \left(K_p^\times\right)^2$.

Now suppose that p is ramified in K. Then $\langle p \rangle = \mathfrak{p}^3$, where $\mathfrak{p}$ is the unique prime of $\mathcal{O}_K$ lying over p. Since $\mathfrak{p}^3$ is principal, it follows that $[\mathfrak{p}]$ has order 1 or 3 in C. If $|[\mathfrak{p}]| = 1$ then $\mathfrak{p}$ is principal and prime, and it follows that $\alpha\left(K_p^\times\right)^2 \in \operatorname{Im} \lambda_p$ as in the case where p is inert. If $|[\mathfrak{p}]| = 3$, let $H \leq C$ be the subgroup of C with class field $K\left(\sqrt{\alpha}\right)$. Then

$$\mathbb{Z}/2\mathbb{Z} \cong \operatorname{Gal}(K\left(\sqrt{\alpha}\right)/K) \cong C/H,$$

by Theorem 7. Therefore, $|[\mathfrak{p}]H|$ is either 1 or 2. Since $|[\mathfrak{p}]H| \mid |[\mathfrak{p}]| = 3$, it must be that $|[\mathfrak{p}]H| = 1$ so $[\mathfrak{p}] \in H$. Thus, $\mathfrak{p}$ splits in $K\left(\sqrt{\alpha}\right)$. It now follows that $\alpha \left(K^\times\right)^2 \in \operatorname{Im} \lambda_p$ using the same argument as above.

Finally, assume that p splits in K. Recall from Corollary 17 that λ_p induces an injection $\overline{\lambda_p} : E\left(\mathbb{Q}_p\right)/2E\left(\mathbb{Q}_p\right) \hookrightarrow \left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right)^3$, and $\operatorname{Im} \overline{\lambda_p} = \operatorname{Im} \lambda_p$. We claim that the image of this homomorphism can be viewed as being in $\left(\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2\right)^3$, which is naturally contained in $\left(\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2\right)^3$. Let $x \in \mathbb{Q}_p^\times$ and write $x = a/b$ for $a, b \in \mathbb{Z}_p$ relatively prime. It suffices to show that $(x-\rho)\left(\mathbb{Q}_p^\times\right)^2 \cap \mathbb{Z}_p^\times \neq \emptyset$, $(x-\rho')\left(\mathbb{Q}_p^\times\right)^2 \cap \mathbb{Z}_p^\times \neq \emptyset$, and $(x-\rho'')\left(\mathbb{Q}_p^\times\right)^2 \cap \mathbb{Z}_p^\times \neq \emptyset$. We will show $(x-\rho)\left(\mathbb{Q}_p^\times\right)^2 \cap \mathbb{Z}_p^\times \neq \emptyset$. The other cases are similar.

First suppose $b \in \mathbb{Z}_p^\times$. Then $a/b \in \mathbb{Z}_p$, so $x - \rho \in \mathbb{Z}_p$. If $v_p(x-\rho) = 0$, then $x - \rho \in \mathbb{Z}_p^\times$ and thus $(x-\rho)\left(\mathbb{Q}_p^\times\right)^2$ can be represented as $(x-\rho)\left(\mathbb{Z}_p^\times\right)^2 \in \mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2$. If $v_p(x-\rho) > 0$, it must be that $v_p\left(x-\rho'\right) = 0 = v_p\left(x-\rho''\right)$. Otherwise $p \mid D = \left(\rho-\rho'\right)\left(\rho-\rho''\right)\left(\rho'-\rho''\right)$ which implies that p ramifies, a contradiction. Hence,

$$\begin{aligned} 2v_p(y) &= v_p\left(y^2\right) = v_p\left((x-\rho)\left(x-\rho'\right)\left(x-\rho''\right)\right) \\ &= v_p(x-\rho) + v_p\left(x-\rho'\right) + v_p\left(x-\rho''\right) \\ &= v_p(x-\rho). \end{aligned}$$

Thus, $v_p(x-\rho)$ is even and we may write $x-\rho = p^{2k}c$ with $c \in \mathbb{Z}_p^\times$. Then $x - \rho \equiv c \pmod{\left(\mathbb{Q}_p^\times\right)^2}$, so $(x-\rho)\left(\mathbb{Q}_p^\times\right)^2$ can be represented as $c\mathbb{Z}_p^\times \in \mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2$.

Now suppose $b \notin \mathbb{Z}_p^\times$. Then $p \mid b$ and so $a \in \mathbb{Z}_p^\times$ since a and b were assumed to be relatively prime and p is the only prime in $\mathbb{Z}_p$. It follows that

$$v_p(x-\rho) = v_p\left(x-\rho'\right) = v_p\left(x-\rho''\right) = v_p(1/b) = -v_p(b).$$

Hence,

$$\begin{aligned} 2v_p(y) &= v_p\left(y^2\right) = v_p\left((x-\rho)\left(x-\rho'\right)\left(x-\rho''\right)\right) \\ &= v_p(x-\rho) + v_p\left(x-\rho'\right) + v_p\left(x-\rho''\right) \\ &= -3v_p(b). \end{aligned}$$

Hence $v_p(b)$ is even and we may write $b = p^{2k}c$ with $c \in \mathbb{Z}_p^\times$. Then $p^{2k}(x-\rho) = \frac{a-b\rho}{c} \in \mathbb{Z}_p^\times$ and $p^{2k}(x-\rho) \equiv x - \rho \pmod{\left(\mathbb{Q}_p^\times\right)^2}$. Thus $(x-\rho)\left(\mathbb{Q}_p^\times\right)^2$ can be represented as $\left(\frac{a-b\rho}{c}\right)\left(\mathbb{Z}_p^\times\right)^2 \in \mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2$. Thus, λ_p induces an embedding

$$\overline{\lambda_p} : E\left(\mathbb{Q}_p\right)/2E\left(\mathbb{Q}_p\right) \hookrightarrow \left(\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2\right)^3.$$

By Lemma 23, 2 does not split in K. Hence, Corollary 3 implies that for all p that split in K, $\mathbb{Z}_p / \left(\mathbb{Z}_p^\times\right)^2 \cong \mathbb{Z}/2\mathbb{Z}$. Note that if $(a,b,c) \in \operatorname{Im}\overline{\lambda_p}$ with $a,b,c \in \mathbb{Z}_p^\times$, then there is some $(x,y) \in E\left(\mathbb{Q}_p\right)$ such that $a \equiv x - \rho \pmod{\left(\mathbb{Q}_p^\times\right)^2}$, $b \equiv x - \rho' \pmod{\left(\mathbb{Q}_p^\times\right)^2}$, $c \equiv x - \rho'' \pmod{\left(\mathbb{Q}_p^\times\right)^2}$, and so $abc \equiv (x-\rho)\left(x-\rho'\right)\left(x-\rho''\right) = y^2 \in \left(\mathbb{Q}_p^\times\right)^2$. So $abc \in \left(\mathbb{Z}_p\right)^2$ It is easy to check that there are exactly four elements in $\left(\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2\right)^3 \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^3$ satisfying this property, namely $(1,1,0),(1,0,1),(0,1,1),(0,0,0)$. One can check that the image of $E[2]$, where E is defined over $\mathbb{Q}_p$, under $\overline{\lambda_p}$ is precisely these points, so we have

$$\operatorname{Im}\lambda_p = \operatorname{Im}\overline{\lambda_p} \cong \{(1,1,0),(1,0,1),(0,1,1),(0,0,0)\}.$$

Hence in order to show that $\alpha\left(K^{\times}\right)^{2} \in \operatorname{Im}\lambda_p$ if p splits in K, we will show that $\alpha\alpha'\alpha'' \in \left(\mathbb{Z}_p^{\times}\right)^{2}$.

Since p splits in K and $\mathcal{O}_K = \mathbb{Z}[\rho]$, by Theorem 5 we have that $f(x)$ factors into distinct linear factors over $\mathbb{Z}/p\mathbb{Z}$, and the three distinct primes in $\mathcal{O}_K$ lying over p are

$$\mathfrak{p}_i = \langle p, g_i(\rho)\rangle,$$

as in the theorem. Since every $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ permutes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ we may assume without loss of generality that $\sigma_2\left(\mathfrak{p}_1\right) = \mathfrak{p}_2$.

In $\mathcal{O}_K$, let

$$\langle\alpha\rangle = \mathfrak{a}\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}, \tag{19}$$

where $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$ relatively prime to $p\mathcal{O}_K$ and each $e_i \geq 0$. Note that since $\langle\alpha\rangle = I^2$, e_1 is even.

By (19), $v_{\mathfrak{p}_1}(\alpha) = e_1$. Applying σ_2 to (19) yields

$$\langle\alpha'\rangle = \sigma_2(\mathfrak{a})\mathfrak{p}_2^{e_1}\mathfrak{p}_3^{e_2}\mathfrak{p}_1^{e_3}, \tag{20}$$

and so $v_{\mathfrak{p}_1}(\alpha') = e_3$. Applying σ_2 to (20) yields $v_{\mathfrak{p}_1}(\alpha'') = e_2$. Hence, $v_{\mathfrak{p}_1}(\alpha\alpha'\alpha'') = e_1 + e_2 + e_3$.

Similarly, $v_{\mathfrak{p}_2}(\alpha\alpha'\alpha'') = e_1 + e_2 + e_3 = v_{\mathfrak{p}_3}(\alpha\alpha'\alpha'')$. It follows that the exact power of $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ dividing $\langle\alpha\alpha'\alpha''\rangle$ is $e_1 + e_2 + e_3$. So

$$\alpha\alpha'\alpha'' = p^{e_1+e_2+e_3}u, \tag{21}$$

for some $u \in \mathcal{O}_K$ such that $p\mathcal{O}_K$ is relatively prime to $u\mathcal{O}_K$. But $\alpha\alpha'\alpha'' = N_K(\alpha) \in \mathbb{Z}$ and $p \in \mathbb{Z}$, so $u \in \mathbb{Z}$. Hence, $\alpha\alpha'\alpha'' = p^{e_1+e_2+e_3}u$ for some $u \in \mathbb{Z}$ not divisible by p.

Now, (19) implies that there is some $a \in \mathfrak{a}$ and $a_{ik}, b_{ik} \in \mathcal{O}_K$ such that

$$\alpha = a\prod_{i=1}^{3}\prod_{k=1}^{e_i}\left(a_{ik}p + b_{ik}g_i(\rho)\right). \tag{22}$$

For $1 \leq i \leq 3$, let $g_i(x) = x - w_i$. By Theorem 2, for each i, there is a zero of $f(x)$ in $\mathbb{Z}_p$ that is congruent to w_i modulo $p\mathbb{Z}_p$. We embed K into $\mathbb{Z}_p$ by writing each element of K as a linear combination of 1, ρ, ρ^2 and mapping ρ to the zero of $f(x)$ in $\mathbb{Z}_p$ that is congruent to w_1 modulo $p\mathbb{Z}_p$. Then in $\mathbb{Z}_p$, $g_1(\rho) \equiv 0 \pmod{p\mathbb{Z}_p}$. So for each k, we have $a_{1k}p + b_{1k}g_1(\rho) \in p\mathbb{Z}_p$. By Equation (22), α is a multiple of

$$\prod_{k=1}^{e_1}\left(a_{1k}p + b_{1k}g_1(\rho)\right) \in \left(p\mathbb{Z}_p\right)^{e_1},$$

so $v_{p\mathbb{Z}_p}(\alpha) \geq e_1$.

Following a similar procedure, it follows that $v_{p\mathbb{Z}_p}(\alpha') \geq e_3$ and $v_{p\mathbb{Z}_p}(\alpha'') \geq e_2$. Hence,

$$v_{p\mathbb{Z}_p}(\alpha\alpha'\alpha'') = v_{p\mathbb{Z}_p}(\alpha) + v_{p\mathbb{Z}_p}(\alpha') + v_{p\mathbb{Z}_p}(\alpha'') \geq e_1 + e_2 + e_3.$$

However, since $\alpha\alpha'\alpha'' = up^{e_1+e_2+e_3}$ in $\mathbb{Z}$ with $p \nmid u$, we have $v_{p\mathbb{Z}_p}(\alpha\alpha'\alpha'') = e_1+e_2+e_3$. Therefore $v_{p\mathbb{Z}_p}(\alpha) = e_1$, which is even.

Thus, $\alpha \in \operatorname{Im}\lambda_p$ for all primes p, so $\alpha\left(K^\times\right)^2 \in S_2$. Hence, g is surjective, as desired. □

Having proved that g is surjective, we easily obtain the following short exact sequence.

Proposition 32. *The sequence*

$$1 \to \left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\} \to S_2 \to C_2 \to 1$$

is exact. Here, $\left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\} \to S_2$ *is inclusion and* $g : S_2 \to C_2$ *is the map defined in Proposition 31.*

Proof. Note that since $(0,1) \in E(\mathbb{Q})$, it follows that $(0,1) \in E\left(\mathbb{Q}_p\right)$ for all p. Thus,

$$\lambda_p\left((0,1)\right) = \begin{cases} 0-\rho = -\rho & \text{if } p \text{ does not split in } K \\ (0-\rho, 0-\rho', 0-\rho'') = (-\rho,-\rho',-\rho'') & \text{if } p \text{ splits in } K. \end{cases}$$

When p does not split, $-\rho$ is the image of $-\rho$ under the embedding $K \hookrightarrow K_p$. When p splits, $(-\rho,-\rho',-\rho'')$ is the image of $-\rho$ under the embedding $K \hookrightarrow \mathbb{Q}_p^3$. Thus, $-\rho\left(K^\times\right)^2 \in \operatorname{Im}\lambda_p$ for all p. Hence, $-\rho\left(K^\times\right)^2 \in S_2$. Therefore, the inclusion map is well defined and is clearly injective. Hence, the sequence is exact at $\left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\}$.

To show exactness at S_2 we need to check that $\left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\} = \ker g$. Suppose $\alpha\left(K^\times\right)^2 \in \ker g$. Then $g\left(\alpha\left(K^\times\right)^2\right) = [\mathcal{O}_K]$ which implies that $\langle\alpha\rangle = \langle\beta\rangle^2$ for some $\beta \in \mathcal{O}_K$. Then $\alpha = \varepsilon\beta^2$ for some $\varepsilon \in \mathcal{O}_K^\times$. Recall that $\alpha\left(K^\times\right)^2 \in \operatorname{Im}\lambda_\infty$ and $K_\infty = \mathbb{R}$. Thus for some $(x,y) \in E(\mathbb{R})$,

$$(\alpha,\alpha',\alpha'') = \left((x-\rho)\beta_1^2, (x-\rho')\,\beta_2^2, (x-\rho'')\,\beta_3^2\right)$$

where the $\beta_i \in \mathbb{R}^\times$. Now, we know that $\rho < \rho' < \rho''$, so

$$x-\rho > x-\rho' > x-\rho''.$$

Also, $(x-\rho)\,(x-\rho')\,(x-\rho'') = y^2 \geq 0$. Thus, the only possible signatures for $x-\rho$ are $(+,+,+)$ and $(+,-,-)$. These are also the only possible signatures for α and thus the only possible signatures for ε as well. If the signature of ε is $(+,+,+)$, then ε is totally positive. If the signature of ε is $(+,-,-)$, then $-\rho\varepsilon$ is totally positive since the signature of $-\rho$ is $(+,-,-)$ as noted in Table 3. Since every totally positive unit is a square, it follows that either ε or $-\rho\varepsilon$ is a square. Therefore, either α or $-\rho\alpha$ is a square. If α is a square, then $\alpha\left(K^\times\right)^2 = \left(K^\times\right)^2$. If $-\rho\alpha$ is a square, then $\alpha\left(K^\times\right)^2 = (\alpha)(-\rho\alpha)\left(K^\times\right)^2 = -\rho\left(K^\times\right)^2$. Therefore, $\ker g \subseteq \left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\}$.

Note that since $1, -\rho$ are units, both $\langle 1\rangle$ and $\langle -\rho\rangle$ are equal to $\mathcal{O}_K = \mathcal{O}_K^2$. Therefore,

$$g\left(-\rho\left(K^\times\right)^2\right) = [\mathcal{O}_K] = g\left(\left(K^\times\right)^2\right),$$

so $\left(K^\times\right)^2, -\rho\left(K^\times\right)^2 \in \ker g$. Hence, $\ker g = \left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\}$ and the sequence is exact at S_2.

By Proposition 31, g is surjective an so the sequence is exact at C_2. This completes the proof. □

We are now ready to prove Theorem 27.

Proof of Theorem 27. We have the following exact sequences

$$1 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S_2 \to \text{Ш}_2 \to 1$$

and

$$1 \to \left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\} \to S_2 \to C_2 \to 1.$$

Let $i : E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/2E(\mathbb{Q})$ be inclusion. Define $\alpha : E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \to C_2$ by $\alpha = g \circ \varphi \circ i$ and $\beta : C_2 \to \text{Ш}_2$ such that the following diagram commutes.

$$\begin{tikzcd}
& & 1 \arrow[d] & & \\
& & \left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\} \arrow[d] & & \\
1 \arrow[r] & E(\mathbb{Q})/2E(\mathbb{Q}) \arrow[r, "\varphi"] & S_2 \arrow[r, "\pi"] \arrow[d, "g"'] & \text{Ш}_2 \arrow[r] \arrow[d, "id"'] & 1 \\
1 \arrow[r] & E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \arrow[r, "\alpha"] \arrow[u, "i"'] & C_2 \arrow[r, "\beta"] \arrow[d] & \text{Ш}_2 \arrow[r] & 1 \\
& & 1 & &
\end{tikzcd}$$

To see that β is uniquely defined, note that $\left\{(K^\times)^2, -\rho(K^\times)^2\right\} \subseteq \operatorname{Im}\varphi$ since $\varphi((0,1)+2E(\mathbb{Q})) = -\rho(K^\times)^2$ and $\varphi(2E(\mathbb{Q})) = (K^\times)^2$. By the exactness of the vertical sequence,

$$\ker g = \left\{\left(K^\times\right)^2, -\rho\left(K^\times\right)^2\right\} \subseteq \operatorname{Im}\varphi = \ker\pi.$$

It follows that there is a unique homomorphism $\beta : C_2 \to Ш_2$ such that $\beta \circ g = id \circ \pi$.

First we show exactness at $Ш_2$. Note that β is onto if and only if π is onto, which it is, since the upper sequence is known to be exact.

Next we show exactness at $E^\circ(\mathbb{Q})/2E(\mathbb{Q})$. Let $(x,y) \in \ker\alpha$, so $(x,y) \in E^\circ(\mathbb{Q})$. Then

$$[\mathcal{O}_K] = \alpha((x,y)+2E(\mathbb{Q})) = g \circ \varphi \circ i((x,y)+2E(\mathbb{Q})),$$

so $\varphi \circ i((x,y)+2E(\mathbb{Q})) \in \ker g = \left\{(K^\times)^2, -\rho(K^\times)^2\right\}$. Suppose for contradiction that $\varphi \circ i((x,y)+2E(\mathbb{Q})) = -\rho(K^\times)^2$. Then

$$\varphi((x,y)+2E(\mathbb{Q})) = -\rho\left(K^\times\right)^2 = \varphi((0,1)+2E(\mathbb{Q})),$$

so $(x,y)+2E(\mathbb{Q}) = (0,1)+2E(\mathbb{Q})$ since φ is injective. Thus, $(x,y)-(0,1) \in 2E(\mathbb{Q}) \subseteq E^\circ(\mathbb{Q})$. But $(x,y) \in E^\circ(\mathbb{Q})$ and $E^\circ(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$, so $(0,1) \in E^\circ(\mathbb{Q})$. This implies that $0 > \rho''$, a contradiction. Hence, it must be that $\varphi \circ i((x,y)+2E(\mathbb{Q})) = (K^\times)^2$. Thus, $(x,y)+2E(\mathbb{Q}) \in \ker\varphi\circ i$. Since φ, i are each injective, $\varphi\circ i$ is also injective, so $(x,y)+2E(\mathbb{Q}) = 2E(\mathbb{Q})$. Thus, α is injective and the sequence is exact at $E^\circ(\mathbb{Q})/2E(\mathbb{Q})$.

It remains to show exactness at C_2. To see that $\operatorname{Im}\alpha \subseteq \ker\beta$, let $(x,y)+2E(\mathbb{Q}) \in E^\circ(\mathbb{Q})/2E(\mathbb{Q})$. Then

$$\beta\circ\alpha((x,y)+2E(\mathbb{Q})) = \beta\circ g\circ\varphi\circ i((x,y)+2E(\mathbb{Q})) = id\circ\pi\circ\varphi\circ i((x,y)+2E(\mathbb{Q})).$$

Note that $\varphi\circ i((x,y)+2E(\mathbb{Q})) \in \operatorname{Im}\varphi = \ker\pi$, so $id\circ\pi\circ\varphi\circ i((x,y)+2E(\mathbb{Q})) = \operatorname{Im}\varphi$ in $S_2/\operatorname{Im}\varphi = Ш_2$. Thus, $\operatorname{Im}\alpha \subseteq \ker\beta$.

Finally, let $[I] \in \ker\beta$, so $\beta[I] = \operatorname{Im}\varphi$ in $Ш_2 = S_2/\operatorname{Im}\varphi$. Since g is surjective, there is some $z(K^\times)^2 \in S_2$ such that $g\left(z(K^\times)^2\right) = [I]$. Then $\beta\circ g\left(z(K^\times)^2\right) = \operatorname{Im}\varphi$. Thus,

$$z\left(K^\times\right)^2 \in \ker\beta\circ g = \ker id\circ\pi = \ker\pi = \operatorname{Im}\varphi.$$

Therefore there is some $(x,y)+2E(\mathbb{Q}) \in E(\mathbb{Q})/2E(\mathbb{Q})$ such that $\varphi((x,y)+2E(\mathbb{Q})) = z(K^\times)^2$. If $(x,y)+2E(\mathbb{Q}) \in E^\circ(\mathbb{Q})/2E(\mathbb{Q})$, then

$$\begin{aligned}\alpha((x,y)+2E(\mathbb{Q})) &= g\circ\varphi\circ i((x,y)+2E(\mathbb{Q}))\\ &= g(\varphi((x,y)+2E(\mathbb{Q})))\\ &= g(z\left(K^\times\right)^2)\\ &= [I],\end{aligned}$$

and so $[I] \in \operatorname{Im} \alpha$, as desired. If $(x, y) + 2E(\mathbb{Q}) \notin E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})$, then $(x, y) + (0, 1) + 2E(\mathbb{Q}) \in E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})$, since the sum of any two points in $E(\mathbb{Q}) - E^{\circ}(\mathbb{Q})$ is in $E^{\circ}(\mathbb{Q})$. Thus,

$$\begin{aligned}
\alpha((x, y) + (0, 1) + 2E(\mathbb{Q})) &= g \circ \varphi \circ i((x, y) + (0, 1) + 2E(\mathbb{Q})) \\
&= g \circ \varphi((x, y) + (0, 1) + 2E(\mathbb{Q})) \\
&= g \circ \varphi((x, y) + 2E(\mathbb{Q}))g \circ \varphi((0, 1) + 2E(\mathbb{Q})) \\
&= g\left(z\left(K^{\times}\right)^{2}\right) g\left(-\rho\left(K^{\times}\right)^{2}\right) \\
&= [I]\left[\mathcal{O}_{K}\right] \\
&= [I].
\end{aligned}$$

Therefore in any case $[I] \in \operatorname{Im} \alpha$. Thus, $\ker \beta \subseteq \operatorname{Im} \alpha$ so $\ker \beta = \operatorname{Im} \alpha$. Hence, the sequence is exact, as claimed. □

Theorem 27 gives an important inequality relating the rank of $E(\mathbb{Q})$ to the 2-rank of the class group of K, as seen in the following corollary. This relationship will be particularly useful when examining specific examples in Section 3.5.

Corollary 33. *With $E, C_2, Ш_2$ as above,*

$$\operatorname{rk}(E(\mathbb{Q})) \leq 1 + \operatorname{rk}_2(C_2),$$

with equality holding if and only if $Ш_2 = 0$.

Proof. By a well-known theorem, see for example [16], $E(\mathbb{Q})$ is isomorphic to one of

$$\begin{gathered}
\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}^{r} \text{for } 1 \leq \ell \leq 10 \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\ell\mathbb{Z} \oplus \mathbb{Z}^{r} \text{for } 1 \leq \ell \leq 4,
\end{gathered}$$

for some $r \in \mathbb{Z}^{+}$. In our case, we know that none of the elements in E of order 2 is rational, so $E(\mathbb{Q}) \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}^{r}$, with ℓ odd. Note that if ℓ is odd, then $2(\mathbb{Z}/\ell\mathbb{Z}) = \mathbb{Z}/\ell\mathbb{Z}$. Hence,

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \left(\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}^{r}\right) / \left(2\left(\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}^{r}\right)\right) \cong (\mathbb{Z}/2\mathbb{Z})^{r}.$$

Therefore, $\operatorname{rk}(E(\mathbb{Q})) = r = \operatorname{rk}_2(E(\mathbb{Q})/2E(\mathbb{Q}))$.

Note that $E(\mathbb{Q}/2E(\mathbb{Q}))$ is a $\mathbb{Z}/2\mathbb{Z}$-vector space. Furthermore, $E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})$ is a subspace of $E(\mathbb{Q})/2E(\mathbb{Q})$. Let B be a basis for $E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})$ over $\mathbb{Z}/2\mathbb{Z}$. We claim that $B' = B \cup \{(0, 1)\}$ is a basis for $E(\mathbb{Q})/2E(\mathbb{Q})$. It is clear that B' is linearly independent since $(0, 1) \in E(\mathbb{Q}) - E^{\circ}(\mathbb{Q})$, so it suffices to show that B' spans $E(\mathbb{Q})/2E(\mathbb{Q})$. Let $(x, y) \in E(\mathbb{Q})$. If $(x, y) \in E^{\circ}(\mathbb{Q})$ then $(x, y) \in \operatorname{span}(B) \subseteq \operatorname{span}(B')$, as desired. If $(x, y) \in E(\mathbb{Q}) - E^{\circ}(\mathbb{Q})$ then $(x, y) + (0, 1) = (v, w)$

for some $(v, w) \in E^{\circ}(\mathbb{Q})$. Therefore $(x, y) + 2E(\mathbb{Q}) = (v, w) - (0, 1) + 2E(\mathbb{Q}) \in \operatorname{span}(B')$, as desired. Hence, $\operatorname{rk}_2(E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})) = |B| = |B'| - 1 = \operatorname{rk}(E(\mathbb{Q})/2E(\mathbb{Q})) - 1$.

By Theorem 27, there is a monomorphism $\alpha : E^{\circ}(\mathbb{Q}) \to C_2$. Therefore, $\operatorname{rk}_2(E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})) \leq \operatorname{rk}_2(C_2)$. Using the fact that $\operatorname{rk}_2(E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})) = \operatorname{rk}(E(\mathbb{Q})/2E(\mathbb{Q})) - 1$ we have

$$\operatorname{rk}(E(\mathbb{Q})/2E(\mathbb{Q})) = \operatorname{rk}_2(E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})) + 1 \leq \operatorname{rk}_2(C_2) + 1,$$

as desired.

Note that if $Ш_2 = 0$ then α is an isomorphism and so

$$C_2 \cong E^{\circ}(\mathbb{Q})/2E(\mathbb{Q}).$$

Therefore, $\operatorname{rk}_2(C_2) = \operatorname{rk}_2(E^{\circ}(\mathbb{Q})/2E(\mathbb{Q}))$ and $\operatorname{rk}(E(\mathbb{Q})/2E(\mathbb{Q})) = 1 + \operatorname{rk}_2(C_2)$. If $Ш_2 \neq 0$ then

$$C_2/\operatorname{Im}(\alpha) \cong Ш_2 \neq 0,$$

so $\operatorname{Im} f \subsetneq C_2$. Thus, $\operatorname{rk}_2(E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})) < \operatorname{rk}_2(C_2)$. In this case, $\operatorname{rk}(E(\mathbb{Q})/2E(\mathbb{Q})) < 1 + \operatorname{rk}_2(C_2)$, as claimed. □

3.4 Quartic fields associated with the simplest cubic fields

The goal of this section is to establish connections between points on $E(\mathbb{Q})$ and certain extension fields of K under the assumption that $Ш_2$ is trivial. In particular, we will use information about the elliptic curve to determine the sets of conjugate quartic fields referred to in Theorem 14.

First we set up some notation. Note that all extensions of $\mathbb{Q}$ and K defined in this section are contained in $\mathbb{C}$. Since $Ш_2 = 0$, it follows from Theorem 27 that $E^{\circ}(\mathbb{Q})/2E(\mathbb{Q}) \cong C_2$ via the map α, where

$$\alpha((x, y) + 2E(\mathbb{Q})) = [I],$$

with I a (fractional) ideal such that $I^2 = \langle x - \rho \rangle$.

Let $(d, e) \in E(\mathbb{Q})$ and $q(x)$ be the quartic polynomial obtained from (d, e) as in Proposition 13. Let F be the splitting field of $q(x)$ and m_1, m_2, m_3, m_4 be the zeros of $q(x)$. For $i = 1, 2, 3, 4$ let (x_i, y_i) be the point on E satisfying $2(x_i, y_i) = (d, e)$ obtained from m_i as in the proof of Proposition 13. That is, if $f(x + d) = ax^3 + bx^2 + cx + d$, then

$$x_i = \frac{1}{2a}\left(m_i^2 - b\right) + d$$

and

$$y_i = \frac{m_i}{2a}\left(m_i^2 - b\right) - e.$$

It follows from Proposition 13 that these are the only solutions to $2\,(x_i, y_i) = (d, e)$. Recall that $E[2] = \{(\rho, 0), (\rho', 0), (\rho'', 0), \infty\}$. Hence for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,

$$2\,((x_1, y_1) + (\sigma(\rho), 0)) = 2\,(x_1, y_1) + 2(\sigma(\rho), 0) = (d, e) + \infty = (d, e),$$

so $(x_1, y_1) + (\sigma(\rho), 0) = (x_j, y_j)$ for some j. Without loss of generality, assume the m_i are ordered such that

$$\begin{aligned}(x_2, y_2) &= (x_1, y_1) + (\rho, 0)\\ (x_3, y_3) &= (x_1, y_1) + (\rho', 0)\\ (x_4, y_4) &= (x_1, y_1) + (\rho'', 0)\end{aligned}$$

It is easy to see that $\mathbb{Q}\,(m_i) = \mathbb{Q}\,(x_i, y_i)$. Define the set of conjugate fields determined by $q(x)$ to be

$$S_q = \{\mathbb{Q}(m_i) : i = 1, 2, 3, 4\}\,.$$

Proposition 34. *Let $(d, e), (d_1, e_1) \in E(\mathbb{Q}) - 2E(\mathbb{Q})$ such that $(d, e) \equiv (d_1, e_1) \pmod{2E(\mathbb{Q})}$. Let $q_1(x)$ be the quartic polynomial determined by (d_1, e_1) as in Proposition 13. Then $S_q = S_{q_1}$.*

Proof. Let n_1, n_2, n_3, n_4 be the zeros of $q_1(x)$. For $i = 1, 2, 3, 4$ let (u_i, v_i) be the point on E satisfying $2\,(u_i, v_i) = (d_1, e_1)$ obtained from n_i as in the proof of Proposition 13.

Since $(d_1, e_1) \equiv (d, e) \pmod{2E(\mathbb{Q})}$, we may write $(d_1, e_1) = (d, e) + 2(x, y)$ for some $(x, y) \in E(\mathbb{Q})$. Fix $i \in \{1, 2, 3, 4\}$. Note that

$$(d_1, e_1) = 2\,((x_i, y_i) + (x, y))\,,$$

so it must be that $(x_i, y_i) + (x, y) = (u_j, v_j)$ for some $j \in \{1, 2, 3, 4\}$.

We claim that $\mathbb{Q}\,(u_j, v_j) = \mathbb{Q}\,(x_i, y_i)$. Note that since $(x_i, y_i)\,, (x, y) \in E\,(\mathbb{Q}\,(x_i, y_i))$, it follows that $(u_j, v_j) = (x_i, y_i) + (x, y) \in E\,(\mathbb{Q}\,(x_i, y_i))$, so $u_j, v_j \in \mathbb{Q}\,(x_i, y_i)$. Similarly, $(u_j, v_j)\,, (x, y) \in E\,(\mathbb{Q}\,(u_j, v_j))$, so $(x_i, y_i) = (u_j, v_j) - (x, y) \in E\,(\mathbb{Q}\,(u_j, v_j))$. Hence, $x_i, y_i \in \mathbb{Q}\,(u_j, v_j)$. Therefore, $\mathbb{Q}\,(u_j, v_j) = \mathbb{Q}\,(x_i, y_i)$, as claimed.

We have

$$\mathbb{Q}\,(m_i) = \mathbb{Q}\,(x_i, y_i) = \mathbb{Q}\,(u_j, v_j) = \mathbb{Q}\,(n_j) \in S_{q_1}.$$

Since this holds for each i, $S_q \subseteq S_{q_1}$. The proof that $S_{q_1} \subseteq S_q$ is similar. Hence, $q(x)$ and $q_1(x)$ determine the same sets of conjugate quartic fields. □

Next we investigate the structure of $F = \mathbb{Q}\,(m_1, m_2, m_3, m_4)$.

Proposition 35. *Let* $(d,e) \in E(\mathbb{Q})$. $F = K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right)$. *Furthermore,*

$$\mathrm{Gal}(F/\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & \textit{if } F = K \\ A_4 & \textit{if } F \neq K. \end{cases}$$

Proof. Recall that $F = \mathbb{Q}(x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4)$. First we show that $K \subseteq F$. It suffices to show that $\rho \in F$. Since $x_i, y_, \in F$ for $i = 1, 2, 3, 4$,

$$(\rho, 0) = (x_2, y_2) - (x_1, y_1) \in E(F).$$

Hence $\rho \in F$ and $K \subseteq F$, as claimed.

Recall from Corollary 17 that there is an injection $E(F)/2E(F) \hookrightarrow \left(F^\times/\left(F^\times\right)^2\right)^3$ given by

$$(x, y) + 2E(F) \mapsto (x - \rho, x - \rho', x - \rho'').$$

Therefore $(d, e) \in 2E(F)$ if and only if $d - \rho, d - \rho', d - \rho'' \in \left(F^\times\right)^2$. Hence,

$$F = K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}, \sqrt{d-\rho''}\right).$$

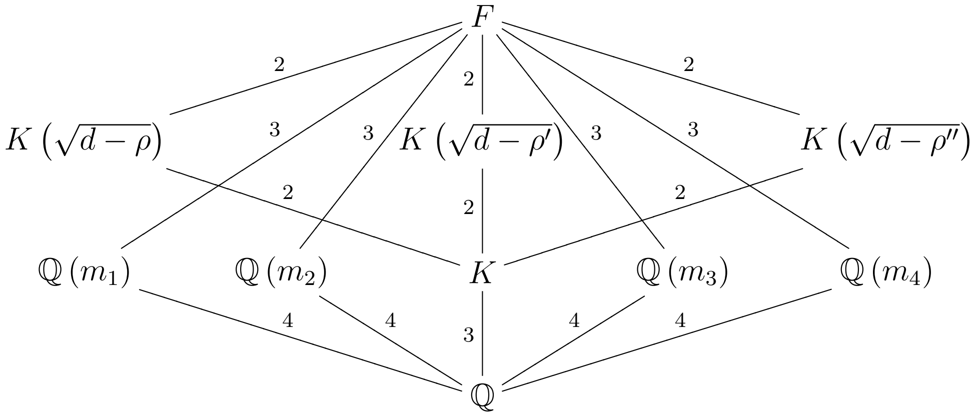
Note that $e^2 = (d-\rho)(d-\rho')(d-\rho'')$ so

$$\sqrt{d-\rho''} = \frac{\pm e}{\sqrt{d-\rho}\sqrt{d-\rho'}} \in K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right).$$

Hence $F = K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right)$, as claimed.

Note that if $F = K$ then $\mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Therefore, assume that $F \neq K$. Let Δ_f, Δ_q, and Δ_K be the discriminants of $f(x)$, $q(x)$, and K, respectively. We know $\Delta_f \neq 0$ since $f(x)$ has three distinct zeros. Also, $\Delta_f = n^2\Delta_K = (nD)^2$ for some $n \in \mathbb{Z}^+$. We showed in Section 2.3 that Δ_f and Δ_q differ by a nonzero square in $\mathbb{Q}$. Since $\Delta_f \in \left(\mathbb{Q}^\times\right)^2$, it follows that $\Delta_q \in \left(\mathbb{Q}^\times\right)^2$ as well. By [7, Corollary V.4.6], $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of A_4. Since the cubic field $K \subsetneq F$, $3 \mid |\mathrm{Gal}(F/\mathbb{Q})|$ and so $|\mathrm{Gal}(F/\mathbb{Q})| = 6$ or 12. As A_4 does not have a subgroup of order 6 and $F/\mathbb{Q}$ is Galois, it must be that $|\mathrm{Gal}(F/\mathbb{Q})| = 12$. Therefore $\mathrm{Gal}(F/\mathbb{Q}) \cong A_4$, as claimed. □

If $F \neq K$, we have the following diagram.



The fields $\mathbb{Q}(m_i)$ are quadratic extensions of $\mathbb{Q}$ whose Galois closure, namely F, contains K. If $|\Delta_{\mathbb{Q}(m_i)}| = |\Delta_K|$, then the $\mathbb{Q}(m_i)$ are some of the fields that are counted in Theorem 14. The following lemma is needed to prove Proposition 37, which shows that this condition on the discriminants is satisfied.

Lemma 36. *If $(d, e) \in E(\mathbb{Q})$, then $d = a/b$ where $\gcd(a, b) = 1$ and b is a square in $\mathbb{Z}$.*

Proof. Write $d = a/b$ and $e = r/s$ with $a, b, r, s \in \mathbb{Z}$ and $\gcd(a, b) = 1 = \gcd(r, s)$. Using the fact that $f(d) = e^2$ we have

$$b^3r^2 = s^2\left(a^3 + ma^2b - (m+3)ab^2 + b^3\right).$$

Let p be a prime such that $v_p(b) > 0$. Then $p \nmid a^3 + ma^2b - (m+3)ab^2 + b^3$ since $\gcd(a, b) = 1$. By unique prime factorization, $p^{3v_p(b)} \mid s^2$. Since $p \mid s$ and $\gcd(r, s) = 1$, it follows that $2v_p(s) = v_p\left(s^2\right) = 3v_p(b)$. Hence, $v_p(b) \in 2\mathbb{Z}$ for all primes p. Therefore b is a square in $\mathbb{Z}$, as claimed. □

Proposition 37. *If $(d, e) \in E^\circ(\mathbb{Q}) - 2E(\mathbb{Q})$, then $|\Delta_{\mathbb{Q}(m_i)}| = |\Delta_K|$ and $K\left(\sqrt{d-\rho}\right)/K$ is unramified. If $(d, e) \in E(\mathbb{Q}) - E^\circ(\mathbb{Q})$, then $|\Delta_{\mathbb{Q}(m_i)}| = 64|\Delta_K|$ and $K\left(\sqrt{d-\rho}\right)/K$ is ramified at 2 and two infinite primes and unramified elsewhere.*

Proof. First we prove the statements about ramification. Recall that there is some ideal I such that $I^2 = \langle d - \rho\rangle$. Since $\langle 2\rangle$ is prime in K, we can write

$$\langle d-\rho\rangle = \langle 2\rangle^{2e}\mathfrak{a}^2$$

for some ideal $\mathfrak{a}$ relatively prime to 2. We know $\mathfrak{a}^2$ must be principal, say $\mathfrak{a}^2 = \langle\alpha\rangle$. By choosing the appropriate α, we may write $d - \rho = 2^{2e}\alpha$, so

$$K\left(\sqrt{d-\rho}\right) = K\left(\sqrt{2^{2e}\alpha}\right) = K\left(2^e\sqrt{\alpha}\right) = K\left(\sqrt{\alpha}\right).$$

Therefore, it suffices to show $K\left(\sqrt{\alpha}\right)/K$ has the desired ramification.

Note that α and $d-\rho$ have the same signature. If $(d,e)\in E^{\circ}(\mathbb{Q})-2E(\mathbb{Q})$ then $d-\rho$ is totally positive and hence α is totally positive. By construction α is relatively prime to 2, so Lemma 30 implies that $K\left(\sqrt{\alpha}\right)/K$ is an unramified extension, as claimed.

Now suppose that $(d,e)\in E(\mathbb{Q})-E^{\circ}(\mathbb{Q})$. Then $d-\rho>0, d-\rho'<0, d-\rho''<0$. Hence, $\sqrt{d-\rho'}, \sqrt{d-\rho''}\in\mathbb{C}-\mathbb{R}$ so $K\left(\sqrt{d-\rho}\right)/K$ is ramified at the two infinite primes corresponding to $\sigma_2,\sigma_3\in\operatorname{Gal}(K/\mathbb{Q})$. Furthermore by Theorem 12, $K\left(\sqrt{\alpha}\right)/K$ is unramified at all finite primes except possibly 2. Suppose for contradiction that $K\left(\sqrt{d-\rho}\right)=K\left(\sqrt{\alpha}\right)$ is unramified at 2. Then $K\left(\sqrt{\alpha}\right)/K$ is unramified at all finite primes. Corollary 10 implies that $K\left(\sqrt{\alpha}\right)/K$ is also unramified at all infinite primes, a contradiction. Therefore 2 must be ramified in $K\left(\sqrt{d-\rho}\right)/K$, as desired.

To see that $|\Delta_{\mathbb{Q}(m_i)}|=|\Delta_K|$ when $(d,e)\in E^{\circ}(\mathbb{Q})-2E(\mathbb{Q})$, note that $\operatorname{Gal}(F/\mathbb{Q})\cong A_4$ by Proposition 35, since $(d,e)\notin 2E(\mathbb{Q})$ and so $F\neq K$. Also, since $(d,e)\in E^{\circ}(\mathbb{Q})$, $d-\rho, d-\rho'>0$, so $F=K\left(\sqrt{d-\rho},\sqrt{d-\rho'}\right)\subseteq\mathbb{R}$. Hence any subfield of F has no complex embeddings. With notation as in Proposition 19, $M_j=\mathbb{Q}\left(m_j\right)$ for $j=1,2,3,4$ and $L_i=K\left(\sqrt{d-\sigma_i(\rho)}\right)$ for $i=1,2,3$. We have $r_{L_i}=6=2+r_{m_j}$ and $t_{L_i}=0=t_{M_j}$. Hence, by Proposition 19, $|\Delta_{L_1}|=|\Delta_K\Delta_{M_j}|$.

Recall that $\Delta_{L_1}=N_{K/\mathbb{Q}}\left(\delta_{L_1/K}\right)\Delta_K^{[L_1:K]}$, where $\delta_{L_1/K}$ is the relative discriminant of L_1 over K. As $L_1=K\left(\sqrt{d-\rho}\right)$ is an unramified extension of K, $\delta_{L_1/K}$ is a unit in $\mathcal{O}_K$ since any primes that divide $\langle\delta_{L_1/K}\rangle$ must ramify in L_1. Hence, $\Delta_{L_1}=\Delta_K^2$ and $\Delta_K^2=|\Delta_{L_1}|=|\Delta_K\Delta_{M_j}|$. Therefore, $|\Delta_{\mathbb{Q}(m_j)}|=|\Delta_{M_j}|=|\Delta_K|$ for $j=1,2,3,4$, as claimed.

Next we show that $|\Delta_{\mathbb{Q}(m_i)}|=64|\Delta_K|$ if $(d,e)\in E(\mathbb{Q})-E^{\circ}(\mathbb{Q})$. By Lemma 36 we may write $d=a/g^2$ for $a,g\in\mathbb{Z}$ relatively prime. Let $\beta=g^2(d-\rho)=a-g^2\rho$. Since 2 is inert in K, $\mathcal{O}_K=\mathbb{Z}[\rho]$, and $\gcd(a,g)=1$, it follows that $\langle\beta\rangle$ is relatively prime to $\langle 2\rangle$.

Now $K\left(\sqrt{\beta}\right)$ is wildly ramified at 2 since $\left[K\left(\sqrt{\beta}\right):K\right]=2$ and the ramification index of 2 is 2. By [2, page 21] it follows that $4\mid\delta_{L_1/K}$. Furthermore, using the norm formula for the discriminant, we have that $\delta_{L_1/K}=-N_{L_1/K}\left(2\sqrt{\beta}\right)=4\beta$. As 2 is the only ramified prime, it is the only prime dividing $\delta_{L_1/K}$, so we have $\delta_{L_1/K}=4$. Thus, $\Delta_{L_1}=\delta_{L_1/K}\Delta_K^{[L_1:K]}=4\Delta_K^2$.

Again, we know that $F\neq K$, so $\operatorname{Gal}(F/\mathbb{Q})\cong A_4$ by Proposition 35. Since $(d,e)\in E(\mathbb{Q})-E^{\circ}(\mathbb{Q})$ it follows that $d-\rho>0$ and $d-\rho', d-\rho''<0$. Then $L_1=K\left(\sqrt{d-\rho}\right)$ has two real embeddings and four complex embeddings. Recall that the m_j are zeros of $q(x)$ which has cubic resolvent $-64f\left(\frac{-x}{4}+d\right)$. The zeros of $-64f\left(\frac{-x}{4}+d\right)$ are $u=4(d-\rho)>0$, $v=4(d-\rho')<0$, and $w=4(d-\rho'')<0$. Therefore the four zeros of $q(x)$ are

$$\frac{1}{2}\left(\sqrt{u}\pm\left(\sqrt{v}+\sqrt{w}\right)\right)\quad\text{and}\quad\frac{1}{2}\left(-\sqrt{u}\pm\left(\sqrt{v}-\sqrt{w}\right)\right).$$

As $\sqrt{v},\sqrt{w}\notin\mathbb{R}$, it follows that $m_j\notin\mathbb{R}$ for $j=1,2,3,4$. Thus, M_j has no real embeddings and four complex embeddings for all j. Hence, $r_{L_1} = 2 + r_{M_j}$ and $t_{L_1} = 4 = t_{M_j}$. By Proposition 19, $|\Delta_{L_1}| = |\Delta_K \Delta_{M_j}|$. Since $\Delta_{L_1} = 64\Delta_K^2$, we have $|\Delta_{\mathbb{Q}(m_j)}| = |\Delta_{M_j}| = 64|\Delta_K|$, as claimed. □

With the exception of Proposition 40 and Corollary 41, assume $(d, e) \in E^\circ(\mathbb{Q}) - 2E(\mathbb{Q})$ for the remainder of Section 3.4. Define an action $\star$ of $\operatorname{Gal}(K/\mathbb{Q})$ on C_2 by $\sigma \star [I] = [\sigma(I)]$. To see that the action is well defined, suppose $[I] = [J]$, so $I = \langle\gamma\rangle J$ for some $\gamma \in K^\times$. For any $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ we have $\sigma(I) = \langle\sigma(\gamma)\rangle\sigma(J)$. Since $\sigma(I)$ differs from $\sigma(J)$ by a principal ideal, it follows that $\sigma \star [I] = [\sigma(I)] = [\sigma(J)] = \sigma \star [J]$, so the action is well defined.

We can extend $\star$ to $E^\circ(\mathbb{Q})/2E(\mathbb{Q})$ by the following composition

$$\operatorname{Gal}(K/\mathbb{Q}) \times E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{id\times\alpha} \operatorname{Gal}(K/\mathbb{Q}) \times C_2 \xrightarrow{\star} C_2 \xrightarrow{\alpha^{-1}} E^\circ(\mathbb{Q})/2E(\mathbb{Q}),$$

where $\alpha : E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \to C_2$ is the map defined in the proof of Theorem 27. We will call this action $*$.

Let $[I] \in C_2$ such that $I^2 = \langle d - \rho\rangle$. Then, letting $I' = \sigma_2(I)$ and $I'' = \sigma_3(I)$, the orbit of $[I]$ under $\star$ is $\{[I], [I'], [I'']\}$. We would like to translate this orbit into $E^\circ(\mathbb{Q})/2E(\mathbb{Q})$. That is, we are looking for the orbit of $(d, e) + 2E(\mathbb{Q})$ under $*$.

Note that $(I')^2 = (\sigma_2(I))^2 = \sigma_2(I^2) = \langle d - \rho'\rangle$ since $d \in \mathbb{Q}$. Also, there is some ideal J such that $[J] = [I']$ and $J^2 = \langle d' - \rho\rangle$ for some $(d', e') \in E^\circ(\mathbb{Q})$. Since $[J] = [I']$, it follows that $J = \langle\beta\rangle I'$ for some $\beta \in K^\times$. Hence $J^2 = \langle\beta\rangle^2(I')^2 = \langle\beta\rangle^2\langle d - \rho'\rangle$ and we may write

$$d' - \rho = \varepsilon\beta^2(d - \rho'),$$

for some $\varepsilon \in \mathcal{O}_K^\times$. Hence, $(d', e') + 2E(\mathbb{Q})$ is part of the desired orbit.

Next, define $(d'', e'') = (d, e) + (d', e') \in E^\circ(\mathbb{Q})$. Note that

$$\begin{aligned}\alpha((d'', e'') + 2E(\mathbb{Q})) &= \alpha((d, e) + (d', e') + 2E(\mathbb{Q})) \\ &= \alpha((d, e) + 2E(\mathbb{Q}))\alpha((d', e') + 2E(\mathbb{Q})) \\ &= [I][I'] = [II'].\end{aligned}$$

Furthermore,

$$(II')^2 = I^2(I')^2 = \langle d-\rho\rangle\langle d-\rho'\rangle = \left\langle \frac{e^2}{d-\rho''}\right\rangle = \left\langle \frac{e^2}{(d-\rho'')^2}\right\rangle \langle d-\rho''\rangle = \left\langle \frac{e^2}{(d-\rho'')^2}\right\rangle (I'')^2.$$

Therefore $II' = \left\langle \frac{e}{d-\rho''}\right\rangle I''$, so $\alpha((d'', e'') + 2E(\mathbb{Q})) = [II'] = [I'']$. Now, there is some ideal $L \in [I'']$ such that $L^2 = \langle d'' - \rho\rangle$. As above, $L = \langle\gamma\rangle I''$ for some $\gamma \in K^\times$. Hence $L^2 = \langle\gamma\rangle^2(I'')^2 = \langle\gamma\rangle^2\langle d - \rho''\rangle$ and we may write

$$d'' - \rho = \eta\gamma^2(d - \rho''),$$

for some $\eta \in \mathcal{O}_K^\times$. Hence, the orbit of $(d,e) + 2E(\mathbb{Q})$ under $*$ is $\{(d,e) + 2E(\mathbb{Q}), (d',e') + 2E(\mathbb{Q}), (d'',e'') + 2E(\mathbb{Q})\}$. Note that, as shown here, it is always possible to choose representatives of the elements in the orbit such that $(d'',e'') = (d,e) + (d',e')$.

Lemma 38. *With notation as above, the splitting fields of the quartic polynomials associated with (d,e), (d',e'), and (d'',e''), as in Proposition 13, are equal.*

Proof. By Proposition 35 it suffices to show that

$$K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right) = K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right) = K\left(\sqrt{d''-\rho}, \sqrt{d''-\rho'}\right).$$

We will show that $K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right) = K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right)$. The other equality is similar.

Recall that $d' - \rho = \varepsilon\beta^2(d-\rho')$. Since $(d,e), (d',e') \in E^\circ(\mathbb{Q})$, $d-\rho$ and $d-\rho'$ are totally positive. Therefore ε is totally positive, so ε is a square in K. Let $\eta = \sqrt{\varepsilon}\beta \in K^\times$. Then

$$d' - \rho = \eta^2(d-\rho'), \tag{23}$$

and so $K\left(\sqrt{d'-\rho}\right) = K\left(\sqrt{d-\rho'}\right)$. Applying $\sigma_2 \in \mathrm{Gal}(K/\mathbb{Q})$ to Equation (23) we have $d' - \rho' = (\eta')^2(d-\rho'')$. We showed in the proof of Proposition 35 that $\sqrt{d-\rho''} \in K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right)$, so $\sqrt{d'-\rho'} = \eta'\sqrt{d-\rho''} \in K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right)$. Therefore, $K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right) \subseteq K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right)$.

Similarly, applying $\sigma_3 \in \mathrm{Gal}(K/\mathbb{Q})$ to Equation (23) we have $d' - \rho'' = (\eta'')^2(d-\rho)$. Thus, $\sqrt{d-\rho} = (1/\eta'')^2\sqrt{d'-\rho''} \in K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right)$ and $K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right) = K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right)$, as desired. □

Note that if any two of these points are congruent modulo $2E(\mathbb{Q})$, the third point is in $2E(\mathbb{Q})$. If the third point is in $2E(\mathbb{Q})$, its associated quartic polynomial from Proposition 13 has a zero in $\mathbb{Q}$. It follows that the associated splitting field has degree less than 12 over $\mathbb{Q}$. But $(d,e) \notin 2E(\mathbb{Q})$ by assumption and so $[F : \mathbb{Q}] = 12$. This contradicts Lemma 38, so (d,e), (d',e'), and (d'',e'') are distinct modulo $2E(\mathbb{Q})$. Hence $(d',e'), (d'',e'') \notin 2E(\mathbb{Q})$.

Let S be the set of all orbits under $*$ of nonidentity elements of $E^\circ(\mathbb{Q})/2E(\mathbb{Q})$. Let T be the set of all fields, M, such that M is the splitting field of a quartic polynomial associated with a point in $E^\circ(\mathbb{Q}) - 2E(\mathbb{Q})$.

Proposition 39. *There is a one-to-one correspondence between the orbits in S and the fields in T. In particular, given $F \in T$, there is exactly one orbit in S such that F is the splitting field of the quartic polynomial associated with any representative point of any element in the orbit. Conversely, given an orbit in S, any representative point of any element in that orbit produces the same field in T.*

Table 5: $\mathrm{Gal}(F/K)$

	1	2	3	4
τ_1	1	2	3	4
τ_2	2	1	4	3
τ_3	3	4	1	2
τ_4	4	3	2	1

Proof. As above, let $q(x)$ be the quartic polynomial associated with (d, e) as in Proposition 13, and let F be the splitting field of $q(x)$. We will show that if $(x, y) \in E^\circ(\mathbb{Q})$ such that all solutions of $2\,(x_i, y_i) = (x, y)$ are in F, then (x, y) is equivalent to one of (d, e), (d', e'), (d'', e'') modulo $2E(\mathbb{Q})$. In order to prove this, we need to set up some notation. Let (x_i, y_i), (d_i', e_i'), and (d_i'', e_i'') for $i = 1, 2, 3, 4$, be the solutions to $2\,(x_i, y_i) = (x, y)$, $2\,(d_i', e_i') = (d', e')$, and $2\,(d_i'', e_i'') = (d'', e'')$, respectively. It follows from Proposition 35 that $\mathrm{Gal}(F/K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Let $\mathrm{Gal}(F/K) = \{\tau_1, \tau_2, \tau_3, \tau_4\}$. Without loss of generality, we may assume that (x_i, y_i), (d_i', e_i'), and (d_i'', e_i'') are indexed such that $\mathrm{Gal}(F/K)$ induces the action on their indices indicated in Table 5.

For all $(x, y) \in 2E(F)$, define the ordered triple

$$A_{x,y} = (\tau_2\,(x_1, y_1) - (x_1, y_1)\,, \tau_3\,(x_1, y_1) - (x_1, y_1)\,, \tau_4\,(x_1, y_1) - (x_1, y_1))$$

in $E(F) \times E(F) \times E(F)$. Note that for any $i = 1, 2, 3, 4$ and any $\tau \in \mathrm{Gal}(F/K)$, we have $\tau\,(x_i, y_i) - (x_i, y_i) \in E[2]$ since

$$2\,(\tau\,(x_i, y_i) - (x_i, y_i)) = 2\,(\tau\,(x_i, y_i)) - 2\,(x_i, y_i) = \tau\,(2\,(x_i, y_i)) - (x, y) = \tau(x, y) - (x, y) = \infty.$$

Therefore, the ordered triple $A_{x,y}$ must be one of

$$\begin{array}{ll} ((\rho, 0), (\rho', 0), (\rho'', 0)) & ((\rho, 0), (\rho'', 0), (\rho', 0)) \\ ((\rho', 0), (\rho'', 0), (\rho, 0)) & ((\rho', 0), (\rho, 0), (\rho'', 0)) \\ ((\rho'', 0), (\rho, 0), (\rho', 0)) & ((\rho'', 0), (\rho', 0), (\rho, 0))\,. \end{array}$$

Next we show that in fact, there are only three possible values that $A_{x,y}$ may take on for a given field F. In particular, either $A_{x,y}$ is always in the left column or $A_{x,y}$ is always in the right column for all $(x, y) \in 2E(F)$. Suppose for contradiction that $(x, y), (u, v) \in 2E(F)$ such that $A_{x,y}$ is in the left column and $A_{u,v}$ is in the right column. For now, say $A_{x,y} = ((\rho, 0), (\rho', 0), (\rho'', 0))$ and $A_{u,v} = ((\rho, 0), (\rho'', 0), (\rho', 0))$. A similar argument will work for any chosen pair. We have $\tau_2\,(x_1, y_1) = (\rho, 0) = \tau_2\,(u_1, v_1)$. It follows that $\tau_2\,((u_1, v_1) - (x_i, y_i)) = (u_1, v_1) - (x_i, y_i)$. Hence, $(u_1, v_1) - (x_i, y_i)$ is a point defined over the fixed field of $\{\tau_1, \tau_2\}$, call this field M. Notice that $[M:\mathbb{Q}]=6$ and $(u,v)-(x,y)\in 2E(M)$. By Proposition 13, M contains a root of the quartic polynomial associated with $(u,v)-(x,y)$. But this means that M contains a degree four extension which is impossible since $4\nmid 6$. Hence, it must be that $A_{x,y}$ is restricted to one column for all $(x,y)\in 2E(F)$.

Of course, the same is true for $\tau\left(d_i,e_i\right)-\left(d_i,e_i\right)$, $\tau\left(d_i',e_i'\right)-\left(d_i',e_i'\right)$, and $\tau\left(d_i'',e_i''\right)-\left(d_i'',e_i''\right)$. We will show that $A_{d,e}, A_{d',e'}, A_{d'',e''}$ are distinct and thus the three possible triples are represented the points (d,e), (d',e'), and (d'',e'').

Suppose that $A_{d,e}=A_{d',e'}=((\rho,0),(\rho',0),(\rho'',0))$. The other cases are similar. Then for all $\tau\in\mathrm{Gal}(F/K), \tau\left(d_1,e_1\right)-\left(d_1,e_1\right)=\tau\left(d_1',e_1'\right)-\left(d_1',e_1'\right)$. This implies that

$$\tau\left(\left(d_1,e_1\right)-\left(d_1',e_1'\right)\right)=\left(d_1,e_1\right)-\left(d_1',e_1'\right)$$

for all $\tau\in\mathrm{Gal}(F/K)$. Hence, $\left(d_1,e_1\right)-\left(d_1',e_1'\right)\in E(K)$ and $(d,e)+(d',e')\in 2E(K)$. But we've seen that $(d,e)+(d',e')=(d'',e'')\notin 2E(K)$, so we've reached a contradiction. Following similar arguments, we see that $A_{d,e}, A_{d',e'}, A_{d'',e''}$ must be distinct.

As there are only three possible for $A_{x,y}$, it must be that $A_{x,y}\in\{A_{d,e}, A_{d',e'}, A_{d'',e''}\}$. Without loss of generality assume $A_{x,y}=A_{d,e}$. By the above argument, we see that $(d,e)-(x,y)\in 2E(K)$. Let $\overline{q}(x)$ be the quartic polynomial associated with $(d,e)-(x,y)$. By Proposition 13 it follows that $\overline{q}(x)$ has a zero in K. Since $q(x)$ is a quartic polynomial and $[K:\mathbb{Q}]=3$, it must be that $\overline{q}(x)$ actually has a zero in $\mathbb{Q}$. Therefore, $(d,e)-(x,y)\in 2E(\mathbb{Q})$ by Proposition 13. Hence, $(d,e)\equiv(x,y)\pmod{2E(\mathbb{Q})}$, so they represent the same equivalence class in $E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})$. Also, $(x,y)+2E(\mathbb{Q})$ is part of the orbit of $(d,e)+2E(\mathbb{Q})$ under $*$, as desired. □

Note that Proposition 39 is related to Theorem 14. It gives an explicit way to construct the quartic fields associated with K. Also, from the correspondence that was established, we recover his result that there are $\frac{1}{3}\left(|C_2|-1\right)$ sets of conjugate quartic fields with discriminant equal to that of K and whose Galois closure contains K.

Proposition 39 only gives the correspondence between fields in T and orbits in S. These orbits are restricted to points in $E^{\circ}(\mathbb{Q})$ since the action relies on the isomorphism $E^{\circ}(\mathbb{Q})/2E(\mathbb{Q})\cong C_2$. However, we can extend the result to points in $E(\mathbb{Q})-E^{\circ}(\mathbb{Q})$ as well.

Proposition 40. *If $(d,e),(x,y)\in E(\mathbb{Q})-E^{\circ}(\mathbb{Q})$ yield the same set of conjugate quartic fields, then $(d,e)\equiv(x,y)\pmod{2E(\mathbb{Q})}$.*

Proof. Note that if $(d,e),(x,y)\in E(\mathbb{Q})-E^{\circ}(\mathbb{Q})$ yield the same set of conjugate quartic fields, then the associated splitting fields are also equal. In fact, using Proposition 35 we have

$$F=K\left(\sqrt{d-\rho},\sqrt{d-\rho'}\right)=K\left(\sqrt{x-\rho},\sqrt{x-\rho'}\right). \tag{24}$$

Suppose for contradiction that $(d,e) \not\equiv (x,y) \pmod{2E(\mathbb{Q})}$. Define

$$(d',e') = (d,e) + (x,y) \in E^\circ(\mathbb{Q}) - 2E(\mathbb{Q}).$$

By Proposition 37, the extension $K\left(\sqrt{d'-\rho}\right)/K$ is unramified. Since $\left[K\left(\sqrt{d'-\rho}\right) : K\right] = 2$, this extension is also abelian and so $K\left(\sqrt{d'-\rho}\right)$ is contained in the Hilbert class field, say H_K, of K. Since H_K is Galois over K, the Galois closure of $K\left(\sqrt{d'-\rho}\right)$ is contained in H_K and is therefore unramified. Hence $K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right)$ is unramified over K since it is the Galois closure of $K\left(\sqrt{d'-\rho}\right)$ over K.

Let $\varphi : E(K)/2E(K) \to \left(K^\times/\left(K^\times\right)^2\right)^3$ be the map defined in Corollary 17. Note that since

$$(d',e') + (d,e) + (x,y) = 2(d',e') \in 2E(\mathbb{Q}),$$

$(d',e') + (d,e) + (x,y) \in \ker\varphi$. Therefore

$$(d'-\rho)(d-\rho)(x-\rho) = \varphi\left((d',e') + (d,e) + (x,y)\right) \in \left(K^\times\right)^2.$$

It follows that $\sqrt{d'-\rho} \in K\left(\sqrt{d-\rho}, \sqrt{x-\rho}\right)$ and thus $K\left(\sqrt{d'-\rho}\right) \subseteq K\left(\sqrt{d-\rho}, \sqrt{x-\rho}\right)$. By Equation (24) we have $K\left(\sqrt{d-\rho}, \sqrt{x-\rho}\right) \subseteq F$. We will show that equality holds.

Suppose for a contradiction that $\sqrt{x-\rho} \in K\left(\sqrt{d-\rho}\right)$. Then $\sqrt{x-\rho} = r + s\sqrt{d-\rho}$ for some $r, s \in K$, so $x - \rho = r^2 + bs^2 + 2rs\sqrt{d-\rho}$. Since $\sqrt{d-\rho} \notin K$, $rs = 0$. Since $\sqrt{x-\rho} \notin K$, it must be that $r = 0$ and so $\sqrt{x-\rho} = s\sqrt{d-\rho}$. Squaring both sides yields $x - \rho = s^2(d-\rho)$, so $x-\rho$ and $d-\rho$ differ by a square in K. By Proposition 15, $(d,e)-(x,y) \in 2E(K)$. As in the proof of Proposition 39 $(d,e)-(x,y) \in 2E(\mathbb{Q})$, a contradiction. Therefore, $\sqrt{x-\rho} \notin K\left(\sqrt{d-\rho}\right)$ and so $\left[K\left(\sqrt{d-\rho}, \sqrt{x-\rho}\right) : \mathbb{Q}\right] = 12$. It follows that $K\left(\sqrt{d-\rho}, \sqrt{x-\rho}\right) = F$.

Note that since F is Galois over $\mathbb{Q}$ and $\sqrt{d'-\rho} \in K\left(\sqrt{d-\rho}, \sqrt{x-\rho}\right) = F$, we must have $K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right) \subseteq F$. Since $(d',e') \notin 2E(\mathbb{Q})$, it follows that the splitting field of the corresponding quartic polynomial, which is $K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right)$ by Proposition 35, is of degree 12 over $\mathbb{Q}$. Since $[F : \mathbb{Q}] = 12$ and $K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right) \subseteq F$, it follows that $K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right) = F$. We showed above that $K\left(\sqrt{d'-\rho}, \sqrt{d'-\rho'}\right)/K$ is unramified, so F is unramified. But since $(d,e) \in E(\mathbb{Q}) - E^\circ(\mathbb{Q})$, $F = K\left(\sqrt{d-\rho}, \sqrt{d-\rho'}\right)$ is ramified at 2 by Proposition 37. We have reached a contradiction. Therefore, it must be that $(d,e) \equiv (x,y) \pmod{2E(\mathbb{Q})}$, as claimed. □

Corollary 41 is useful in determining the form of points in $E(\mathbb{Q})$ depending on the chosen value of the parameter m.

Corollary 41. *Suppose $(d,e) \in E^\circ(\mathbb{Q})$. Let $d = \frac{a}{4^s b^2}$ with $a \in \mathbb{Z}, b$ odd, and $s \geq 0$. Then*

1. *if m is even, then $s > 0$ and $a \equiv 1 \pmod 4$*

2. *if* $m \equiv 1 \pmod 4$ *and* $s = 0$*, then* $a \equiv 3 \pmod 4$

3. *if* $m \equiv 3 \pmod 4$ *and* $s = 0$*, then* $a \equiv 2 \pmod 4$

4. *if* $m \equiv 1$ *or* $3 \pmod 4$ *and* $s > 0$*, then* $a \equiv 1 \pmod 4$.

Proof. By Lemma 36, d can be written in the stated form. Let $g^2 = 4^s b^2$.

Let $(d, e) \in E^\circ(\mathbb{Q})$, so $K\left(\sqrt{d-\rho}\right)/K$ is an unramified extension by Proposition 37. In particular, the extension is unramified at 2. Note that $g^2(d-\rho) = a - g^2\rho$ is relatively prime to 2 in $\mathcal{O}_K$ since $2\mathcal{O}_K = \{x + y\rho + z\rho^2 : x, y, z \in 2\mathbb{Z}\}$ and either a or g is odd. Hence, by Theorem 12 $g^2(d-\rho)$ is congruent to a square modulo 4. Note that since $g^2(d-\rho)$ is relatively prime to 2, it follows that $g^2(d-\rho) \not\equiv 0 \pmod 4$.

First suppose that $m \in 2\mathbb{Z}$, so $m \equiv 0, 2 \pmod 4$. According to Table 4 the only possible residue classes for an element of the form $x + y\rho$ are $0, 1, \rho + 2$ if $m \equiv 0 \pmod 4$ and $0, 1, \rho + 1$ if $m \equiv 2 \pmod 4$. We have already established that $g^2(d-\rho) \not\equiv 0 \pmod 4$. Note that if $g^2(d-\rho) \equiv \rho + 2 \pmod 4$ then equating coefficients $-g^2 \equiv 2 \pmod 4$, a contradiction since the only squares in $\mathbb{Z}/4\mathbb{Z}$ are $0, 1$. Similarly, $g^2(d-\rho) \not\equiv \rho + 1 \pmod 4$. Therefore, it must be that $g^2 d - g^2\rho \equiv 1 \pmod 4$. Equating coefficients we have $-g^2 \equiv 0 \pmod 4$ so $g^2 = 4^s b \in 2\mathbb{Z}$ so $s > 0$. Also, $a = g^2 d \equiv 1 \pmod 4$, as claimed.

Next, assume that $m \equiv 1 \pmod 4$. By Table 4 the possible residue classes are $0, 1, 3\rho + 3$. If $s = 0$ then $g^2 \not\equiv 0 \pmod 4$ and so $g^2 d - \rho \not\equiv 1 \pmod 4$. Hence, $g^2 d - g^2\rho \equiv 3\rho + 3 \pmod 4$ and so $a = g^2 d \equiv 3 \pmod 4$ as desired. If $s > 0$ then $g^2 \equiv 0 \pmod 4$ and so $g^2 d - g^2\rho \equiv 1 \pmod 4$. Thus, $a = g^2 d \equiv 1 \pmod 4$.

Finally, suppose that $m \equiv 3 \pmod 4$. By Table 4 the possible residue classes are $0, 1, 3\rho + 2$. If $s = 0$ then $g^2 d \not\equiv 0 \pmod 4$ and so $g^2 d - \rho \not\equiv 1 \pmod 4$. Hence, $g^2 d - g^2\rho \equiv 3\rho + 2 \pmod 4$ and so $a = g^2 d \equiv 2 \pmod 4$. If $s > 0$ then $g^2 d - g^2\rho \equiv 1 \pmod 4$ and $a \equiv 1 \pmod 4$ as in the case $m \equiv 1 \pmod 4$ above. □

3.5 Examples

We conclude with two examples that make use of some of the results we have proved thus far. They use theorems from Sections 3.2, 3.3.2, and 3.4. In particular, Theorem 27 is interesting because it relates the free rank of an elliptic curve to the class number of the corresponding number field. In general, both class numbers and ranks of elliptic curves are difficult to compute, so the inequality obtained from Theorem 27 can be used either as a lower bound on the 2-part of the class group or as an upper bound on the rank of the elliptic curve, depending on what information is know. The following examples [19] demonstrate how the inequality can be useful.

Example 1.

In this example we will see how knowledge of the class number of K can be used to obtain information about the rank of $E(\mathbb{Q})$ as well as the Hilbert class field of K. Consider the curve $y^2 = f(x)$ with $m = 11$,

$$f(x) = x^3 + 11x^2 - 14x + 1.$$

Three points on $E(\mathbb{Q})$ are $A = (0,1)$, $B = (2,5)$, and $C = (6,23)$. By computing $A - B$, $A - C$, and $B - C$ and checking that the corresponding quartic polynomials are irreducible, we see that A, B, and C are independent modulo $2E(\mathbb{Q})$. We show that A, B, and C are independent in $E(\mathbb{Q})$ as well. Suppose for a contradiction that $n_1A + n_2B + n_3C = \infty$ with $n_i \in \mathbb{Z}$. Without loss of generality, assume the n_i are mutually relatively prime. Reducing modulo $2E(\mathbb{Q})$ we have $\overline{n_1}A + \overline{n_2}B + \overline{n_3}C = \infty$. As A, B, and C are independent modulo $2E(\mathbb{Q})$, it follows that $\overline{n_i} = 0$ for $i = 1,2,3$. But then $2 \mid n_i$ for all i and the n_i are not mutually relatively prime, a contradiction. Thus, A, B, and C are independent. Therefore, $\mathrm{rk}(E(\mathbb{Q})) \geq 3$. Shanks [15] showed that 4 is the class number of K. Thus Theorem 27 implies that $\mathrm{rk}(E(\mathbb{Q})) = 3$. Furthermore, since $\mathrm{rk}(E(\mathbb{Q})) = 1 + \mathrm{rk}_2(C_2)$, it follows that $Ш_2 = 0$ for this curve.

Note that $B, C \in E^\circ(\mathbb{Q})$ since we showed in Section 3.1 that for any m, $\rho'' < 2$. Hence, Proposition 37 implies that $K\left(\sqrt{2-\rho}\right)/K$ and $K\left(\sqrt{6-\rho}\right)$ are unramified extensions. Thus, their composite field $L = K\left(\sqrt{2-\rho}, \sqrt{6-\rho}\right)$ is also unramified. As B and C are independent modulo $2E(\mathbb{Q})$, $K\left(\sqrt{2-\rho}\right) \neq K\left(\sqrt{6-\rho}\right)$. Therefore $[L : K] = 4$. By Proposition 39, L is the splitting field of the quartic polynomials associated with B and C, so $L/\mathbb{Q}$ is Galois, which implies that L/K is Galois. Since L is an unramified abelian extension of degree equal to $|C|$, L must be the Hilbert class field of K.

In this example, knowing the class number of K allowed us to find the free rank of $E(\mathbb{Q})$ as well as the Hilbert class field of K.

Example 2.

Next, consider the curve $y^2 = f(x)$ with $m = 143$,

$$f(x) = x^3 + 143x^2 - 146x + 1.$$

Let C be the class group of K. Shanks [15] proved that $|C| = 64$.

Note that the point $F = (90, 1369) \in E(\mathbb{Q})$ and $1369 = 37^2$. Therefore $37^4 = f(90)$ and Proposition 24 implies that $\langle 90 - \rho \rangle = I^4$ for some ideal I of $\mathcal{O}_K$. To see that $[I]$ has order four in the class group, we verify that I^2 is not a principal ideal.

Suppose for contradiction that $I^2 = \langle \beta \rangle$ for some $\beta \in \mathcal{O}_K$. Then $\langle 90 - \rho \rangle = \langle \beta^2 \rangle$, so there is some $\varepsilon \in \mathcal{O}_K^\times$ such that $90 - \rho = \varepsilon\beta^2$. Since $\rho, \rho', \rho'' < 2,\ \ 90 - \rho$ is totally positive. So ε is totally positive and hence a square, by Lemma 20. Thus $90 - \rho \in K^2$. By applying appropriate elements of $\mathrm{Gal}(K/\mathbb{Q})$, it follows that $90 - \rho', 90 - \rho'' \in K^2$ as well. By Proposition 15, it follows that $F \in 2E(\mathbb{Q})$, so by Proposition 13, the associated quartic polynomial $q(x) = x^4 - 826x^2 -$

$10952x - 29007$ has a rational zero. However, this is not the case, so we've reached a contradiction. Hence, I^2 is not principal and thus $[I]$ has order four in C.

Washington [21] shows that the 2-rank, 4-rank, and 8-rank of C are even. Since $|C| = 64$ and C contains an element of order four, either $C \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^2$ or $C \cong (\mathbb{Z}/8\mathbb{Z})^2$. We use Proposition 13 and Theorem 27 to show that $C \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^2$.

Note that $A = (0, 1)$, $B = (2, 17)$, $C = (6, 67)$, $D = (30, 389)$ are in $E(\mathbb{Q})$. By using PARI to compute the differences of these points and then checking that the corresponding quartic polynomials, from Proposition 13, are irreducible over $\mathbb{Q}$, I showed that A, B, C, D, E are independent modulo $2E(\mathbb{Q})$. As in Example 1, this implies that these five points are independent in $E(\mathbb{Q})$. Therefore, $\mathrm{rk}(E(\mathbb{Q})) \geq 5$. By Corollary 33, $\mathrm{rk}_2(C_2) \geq 4$, so $C \cong (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^2$. Finally, Corollary 33 now implies that $\mathrm{rk}(E(\mathbb{Q})) = 5$.

References

[1] C. Batut, K. Belabas, D. Benardi, H. Cohen, and M. Olivier, *User's Guide to {PARI-GP}*, by anonymous ftp from \url{ftp://megrez.math.u-bordeaux.fr/pub/pari} (1998), see also \url{http://pari.home.ml.org}.

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London (1967).

[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley and Sons, New York (1989).

[4] I. B. Fesenko and S. V. Vostokov, *Local Fields and Their Extensions: A Constructive Approach*, Translations of Mathematical Monographs, **121** American Mathematical Society (1993).

[5] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, New York (1991).

[6] H. Heilbronn, "On the 2-classgroup of cubic fields", *Studies in Pure Mathematics* (L. Mirsky, ed.), Academic Press, New York (1971), 117–119.

[7] T. Hungerford, *Algebra*, Springer, New York (1974).

[8] A. W. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ (1992).

[9] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, New York (1984).

[10] S. Louboutin, "The exponent three class group problem for some real cyclic cubic number fields", *Proc. Amer. Math. Soc.* **130** (2002), No. 2, 353–361.

[11] D. Marcus, *Number Fields*, Springer-Verlag, New York (1977).

[12] J. S. Milne, *Class field theory (v4.00)*, Available at www.jmilne.org/math (2008).

[13] J. Neukirch, *Algebraic Number Theory*, Springer, New York (1999).

[14] J. Neukirch, *Class Field Theory*, Springer-Verlag, Berlin (1986).

[15] D. Shanks, "The simplest cubic fields", *Math. Comp.* **28** (1974), 1137–1157.

[16] I. Stewart and S. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, A K Peters, Natick, MA (2002).

[17] E. Thomas, "Complete solutions to a family of cubic Diophantine equations", *J. Number Theory* **34** (1990) No. 2, 235–250.

[18] K. Uchida, "Class numbers of cubic cyclic fields", *J. Math. Soc. Japan* **26** (1974), 447–453.

[19] L. C. Washington, "Class numbers of the simplest cubic fields", *Math. Comp.* **48** (1987), No. 177, 371–384.

[20] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, New York (2003).

[21] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York (1982).

[22] H. Weber, *Lehrbuch der Algebra*, Vol. I, 3rd edition (1898); online at Cornell University Library, http://digital.library.cornell.edu/cgi/t/text/text-idx?c=math;idno=webe031.

[23] Wolfram Research, Inc., Mathematica, Version 6.0, Champaign, IL (2007).