2018

Algebraic Number Theory and Simplest Cubic Fields

Jianing Yang
Colby College

Simplest Cubic Fields

Jianing Yang

May 23, 2018

Contents

1 Introduction

We have known for a long time that there is no integer solution to the equation $x^2 + 2y^2 = 0$, but what about a near miss instead? Is there any integer solution to $x^2 - 2y^2 = \pm 1$? This problem was first considered by the ancient Greeks 2000 years ago, and was completely solved by mathematicians in India around 1000 years ago. There are indeed many solutions. From a modern point of view, it is almost irresistible to rewrite this equation as $(x + y\sqrt{2})(x - y\sqrt{2}) = \pm 1$. Then this becomes a question about some generalized integers in $\mathbb{Z}[\sqrt{2}]$. We can expand our notion of the rationals and the integers, and study the arithmetic in domains analogous to $\mathbb{Z}[\sqrt{2}]$.

The motivation behind this paper lies in understanding the meaning of integrality in general number fields. We want to look at generalizations of the rationals in the form of algebraic number fields. To talk about those, we first need to talk about domains, with $\mathbb{Q}$ as one of the most simple examples of an integral domain. Let R be an integral domain. We have the following relationship between some different types of domains:

$$\begin{aligned} & R \text{ is a field} \\ \Longrightarrow\ & R \text{ is an Euclidean domain} \\ \Longrightarrow\ & R \text{ is a principal ideal domain} \\ \Longrightarrow\ & R \text{ is a unique factorization domain} \end{aligned}$$

I spent most of my time learning algebraic number theory using Ram Murty's book[Mu] under the guidance of my advisor Fernando Gouvêa. I will discuss my understanding of the material and some important theorems in algebraic number theory in this section. Since January, I have been studying Daniel Shanks'[Sh] paper on simplest cubic fields, which I will discuss briefly in Section 3. Some of the theorems in the paper apply to cyclic cubic fields in general, and I discuss them in Section 2, where I will also elaborate on their proofs and some implications.

1.1 Number Fields

Now, to introduce the algebraic number fields, we need to define the algebraic numbers and algebraic integers.

Definition 1.1. A number $\alpha \in \mathbb{C}$ is called an *algebraic number* if α is the root of a polynomial $f(x) = a_n x^n + \cdots + a_0$ such that $a_0, \ldots, a_n$, not all zero, are in $\mathbb{Z}$. The *degree* of α is the smallest degree of such polynomials.

Definition 1.2. If α is the root of a *monic* polynomial with coefficients in $\mathbb{Z}$, we say that α is an *algebraic integer*.

The algebraic numbers form a field. It is still countable, but it is much larger than the rationals. In fact, the field of all algebraic numbers $\overline{\mathbb{Q}}$, called the algebraic closure of $\mathbb{Q} \subset \mathbb{C}$, has an infinite degree over $\mathbb{Q}$. The algebraic integers in $\mathbb{Q}$ are exactly $\mathbb{Z}$, so the algebraic integers are indeed a generalization of the integers. The algebraic integers form a subring of $\overline{\mathbb{Q}}$. Now we will look at the finite extensions of $\mathbb{Q}$, also known as algebraic number fields.

Theorem 1.3. *If α is an algebraic number with degree n, then*

$$\mathbb{Q}(\alpha) = \{f(\alpha) : f(x) \in \mathbb{Q}[x]\}$$

forms a field. It is called an algebraic number field of degree n over $\mathbb{Q}$.

We should note that for any two number fields $K \subset L$, we can find many $\theta \in L$ such that $L = K(\theta)$. Consequently, every extension of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ of finite degree can be written in the form $\mathbb{Q}(\alpha)$. Also, since a number field consists of algebraic numbers, $K \subset \overline{\mathbb{Q}}$ for any number field K.

Theorem 1.4. *The algebraic integers in a number field K form a ring, often denoted $\mathcal{O}_K$.*

If α is an algebraic integer and $K = \mathbb{Q}(\alpha)$, then $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, but it is not necessarily equal to $\mathcal{O}_K$.

Now that we have the concept of algebraic number fields, let us first look at some of their properties.

Definition 1.5. We say that $\omega_1, \omega_2, \ldots, \omega_n$ is an *integral basis* for a number field K if $\omega_i \in \mathcal{O}_K$ for all i and $\mathcal{O}_K = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} + \cdots + \omega_n\mathbb{Z}$ and $\omega_1, \omega_2, \ldots, \omega_n$ are linearly independent over $\mathbb{Q}$.

There always exists an integral basis for any number field K, and this allows us to define the (absolute) discriminant of a field. To do that, we need to introduce the embeddings of K.

Definition 1.6. The embeddings are the injective homomorphisms from K into $\overline{\mathbb{Q}}$.

Theorem 1.7. *Let $K = \mathbb{Q}(\theta)$, and let $\theta_1, \ldots, \theta_n \in \overline{\mathbb{Q}}$ be the roots of the minimal polynomial of θ. Then the field homomorphisms $\sigma_i : K \to \mathbb{Q}(\theta_i) \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ for $i = 1, \ldots, n$, defined by $\sigma_i(\theta) = \theta_i$, are the embeddings of K into $\overline{\mathbb{Q}}$.*

The main content of the theorem is that $\sigma(\theta) = \theta_i$ always defines a field homomorphism. Note that in the case where K is a Galois extension of $\mathbb{Q}$, the embeddings are just the automorphisms of K.

Definition 1.8. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K. If $a_1, a_2, \ldots, a_n \in K$, then we define the discriminant of $\{a_1, a_2, \ldots, a_n\}$ to be $d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) = [\det(\sigma_j(a_i))]^2$. We define the discriminant of K to be $d_K = d_{K/\mathbb{Q}}(\omega_1, \omega_2, \ldots, \omega_n) = [\det(\sigma_j(\omega_i))]^2$ where $\omega_1, \omega_2, \ldots, \omega_n$ is an integral basis of K.

Theorem 1.9. *For a number field K, the field discriminant d_K does not depend on the choice of integral basis.*

Theorem 1.10. *For any $a_1, a_2, \ldots, a_n \in K$, $d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) \in \mathbb{Q}$, and the discriminant of the field $d_K \in \mathbb{Z}$.*

Theorem 1.11. *For any $a_1, a_2, \ldots, a_n \in K$, $d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) \neq 0$ if and only if $a_1, a_2, \ldots, a_n$ are linearly independent over $\mathbb{Q}$.*

Proposition 1.12. *Let $a_1, a_2, \ldots, a_n \in \mathcal{O}_K$ be linearly independent over $\mathbb{Q}$. Let $N = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$ and $m = [\mathcal{O}_K : N]$, then $d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) = m^2 d_K$.*

Now let us look at an easy example to demonstrate the properties of number fields that we just discussed.

Example 1.13. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field where D is square-free. Find its ring of integers $\mathcal{O}_K$, integral basis, and field discriminant d_K.

Let $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, where $a, b \in \mathbb{Q}$. If $\alpha \in \mathcal{O}_K$, then there exists a monic polynomial $p(x) \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. The minimal polynomial of α in $\mathbb{Q}$ is

$$p(x) = x^2 - 2ax + (a^2 - b^2 D).$$

We need $2a$ and $a^2 - b^2 D$ in $\mathbb{Z}$. It turns out to be true that in the case where $D \equiv 1 \pmod 4$, we can have $a, b \in \mathbb{Z}$ or $2a, 2b$ both be odd integers, whereas when $D \not\equiv 1 \pmod 4$, we have to have $a, b \in \mathbb{Z}$.

After some further computation we get, when $D \equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$. The integral basis is $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$. Take the identity σ_1 and the homomorphism $\sigma_2(\sqrt{D}) = -\sqrt{D}$ to be the two embeddings of K into $\mathbb{C}$, then the field discriminant is

$$d_K = \begin{vmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{vmatrix}^2 = d.$$

When $D \not\equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. The integral basis is $\{1, \sqrt{D}\}$. Take σ_1 and σ_2 in the previous case to be the two embeddings of K into $\mathbb{C}$, then the field discriminant is

$$d_K = \begin{vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{vmatrix}^2 = 4d.$$

1.2 Ideal Factorization in $\mathcal{O}_K$

Since number fields are extensions of $\mathbb{Q}$, we want to explore the properties that we study in $\mathbb{Q}$, such as primality, divisibility and integrality. What are the analogue of integers in $\mathbb{Q}(\alpha)$? The natural candidate would be the algebraic integers. Unfortunately, the ring of algebraic integers of a number field K does not always satisfy unique factorization. For instance, the ring of integers of $K = \mathbb{Q}[\sqrt{-5}]$ is $\mathbb{Z}[\sqrt{-5}]$, but $21 \in \mathcal{O}_K$ can be written as $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ where all the factors are irreducible and do not differ by units.

In order for the Fundamental Theorem of Arithmetic to hold for some objects in a number field, Dedekind formulated the concept of ideals.

First, we need to introduce the prime ideals, maximal ideals and ideal products. Prime ideals in the ring of integers share many important properties with prime numbers in the integers.

Definition 1.14. An ideal $\mathfrak{p}$ in a commutative ring $\mathcal{R}$ is called a prime ideal if for any $a, b \in \mathcal{R}$, $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Definition 1.15. An ideal $\mathcal{I}$ in a commutative ring $\mathcal{R}$ is called a maximal ideal if for any ideal $\mathcal{J}$ such that $\mathcal{I} \subset \mathcal{J} \subset \mathcal{R}$, either $\mathcal{J} = \mathcal{I}$ or $\mathcal{J} = \mathcal{R}$.

It is worth noting that, to say that the quotient ring of a ideal is a domain is equivalent to saying that the ideal is prime, and that the quotient ring of a ideal is a field is equivalent to the ideal being maximal. Since every field is a domain, this implies that every maximal ideal in $\mathcal{R}$ is prime. In fact, a partial converse of this statement is true for the ring of integers. Namely, in $\mathcal{O}_K$, every non-zero prime ideal is maximal.

Definition 1.16. Given ideals $\mathcal{I}$ and $\mathcal{J}$ of the ring $\mathcal{R}$, their product is the ideal generated by $\{ab : a \in \mathcal{I}, b \in \mathcal{J}\}$. It is also an ideal of $\mathcal{R}$.

It turns out that, in any number field K, ideals of $\mathcal{O}_K$ do behave like the integers in $\mathbb{Q}$ in that they have unique prime factorization.

Theorem 1.17 (Unique Factorization of Ideals)**.**
Let K be a number field. Then every nonzero ideal in $\mathcal{O}_K$ can be written uniquely as a product of prime ideals.

One crucial question this generates is the following: suppose $p \in \mathbb{Z}$ is a prime number, so that $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. We expect that if we move to

$\mathcal{O}_K$ the ideal $p\mathcal{O}_K$ will now factor, but how? The next few theorems provide partial answers.

Definition 1.18. The *norm* of an ideal $\mathcal{I}$ in $\mathcal{O}_K$ is the index of the ideal in $\mathcal{O}_K$, $[\mathcal{O}_K : \mathcal{I}]$, i.e. the order of $\mathcal{O}_K/\mathcal{I}$.

By the Unique Factorization of Ideals, we can write $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, where $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ are distinct prime ideals in $\mathcal{O}_K$. They have the following property.

Proposition 1.19. *If $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, then the norm of the prime ideals are $N(\mathfrak{p}_i) = p^{f_i}$ for some integer f_i, and $\sum_{i=1}^{g} e_i f_i = n = [K : \mathbb{Q}]$.*

The integer e_i is called the *ramification index* of $\mathfrak{p}_i$, and if $e_i \geq 2$ for some i, then we say that p *ramifies* in K. The integer f_i is called the *residual degree* of $\mathfrak{p}_i$. Since in $\mathcal{O}_K$ every non-zero prime ideal is maximal, $\mathfrak{p}_i$ is maximal and $\mathcal{O}_K/\mathfrak{p}_i$ is a field for all i, with $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$.

For Galois extensions, we have even stronger properties of the ramification indices and residual degrees. Notice that for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\mathcal{I})$ is an ideal for ideal $\mathcal{I}$, and for prime ideal $\mathfrak{p}$, $\sigma(\mathfrak{p})$ is a prime ideal with the same residual degree. In fact, the Galois group acts transitively on the set of prime ideals dividing a rational prime p, so we get for any $\mathfrak{p}_i$ and $\mathfrak{p}_j$, there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. This symmetry forces all the numbers to be equal.

Proposition 1.20. *Let K be a Galois extension of $\mathbb{Q}$. Then the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ are all conjugate. They have the same ramification index e and the same residual degree f. Thus, $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}] = efg$.*

We will need a "relative" version of this notion of ramification indices and residual degrees, so instead of looking at number fields as extensions over $\mathbb{Q}$, let us suppose we have a tower of Galois extensions $\mathbb{Q} \subset K \subset L$, and $\mathfrak{p}_K$, $\mathfrak{p}_L$ are the prime ideals over p in K and L. As before, we can ask for how $\mathfrak{p}_K$ factors in $\mathcal{O}_L$, i.e., for a decomposition of $\mathfrak{p}_K\mathcal{O}_L$ into prime ideals. We define the relative e and f numbers as above. Since we are assuming Galois extensions it makes sense to write $e_{K/\mathbb{Q}}$, $e_{L/K}$, $f_{K/\mathbb{Q}}$, $f_{L/K}$, etc.

Proposition 1.21 (Multiplicativity of e and f)**.** *The ramification indices and residual degrees multiply in towers, i.e. in the notations above,*

$$e_{L/\mathbb{Q}} = e_{L/K} e_{K/\mathbb{Q}} \text{ and } f_{L/\mathbb{Q}} = f_{L/K} f_{K/\mathbb{Q}}.$$

The following theorem by Dedekind associates ramification with the discriminant of K.

Theorem 1.22 (Dedekind)**.**
A prime p ramifies in K if and only if $p \mid d_K$, where d_K is the discriminant of K.

In particular, only finitely many primes ramify in any given number field K. We can define the *radical* of a positive integer.

Definition 1.23. The radical of a positive integer n is $\mathrm{rad}(n) = \prod_{p \mid n, p \text{ prime}} p$.

By definition, a prime $p \mid n$ if and only if $p \mid \mathrm{rad}(n)$.

The following theorem gives an important connection between factoring polynomials mod p and factoring ideals in number fields. This version of the theorem is due to Dedekind, but it is better known as Kummer's Theorem.

Theorem 1.24 (Dedekind)**.**
Let p be a rational prime, and suppose there is a $\theta \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\theta)$ and $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let $f(x)$ be the minimal polynomial of θ in $\mathbb{Z}[x]$. Suppose

$$f(x) = f_1(x)^{e_1} f_2(x)^{e_2} \cdots f_n(x)^{e_n} \pmod{p},$$

where each $f_i(x)$ is irreducible in $\mathbb{F}_p[x]$ and are all distinct. Then $p\mathcal{O}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ where $\mathfrak{p}_i = (f_i(\theta), p)$ are distinct prime ideals.

Remark 1.25. Unfortunately, it is *not* always possible to find a θ so that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. In that case we need to use p-adic methods.

Example 1.26 (Cyclotomic Fields)**.** Now, as an example, let us look at the cyclotomic fields and their properties. This will also be helpful when we discuss the Kronecker-Weber Theorem in the next section.

Definition 1.27. A primitive nth root of unity is a number $\zeta_n \in \mathbb{C}$ such that $\zeta_n^n = 1$ and $\zeta_n^a \neq 1$ for any $0 < a < n$.

In other words, ζ_n generates the group $\mu_n = \{z \in \mathbb{C} | z^n = 1\}$. Notice that ζ_n is a root of $x^n - 1$, hence is an algebraic integer.

Definition 1.28. The nth cyclotomic field is $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity.

If ϕ is Euler's totient function, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Lemma 1.29. *Let $n = p^a$ and $K = \mathbb{Q}(\zeta_n)$. Then*

$$p\mathcal{O}_K = \langle 1 - \zeta_n \rangle^e,$$

where $e = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(p^a) = (p-1)p^{a-1}$.

In situations like this, where $f = g = 1$ and the degree of extension is contributed completely by the ramification index e, we say that p is *totally ramified* in K. On the other hand, if $n = p^a$, then any prime $l \neq p$ is unramified in $\mathbb{Q}(\zeta_n)$. Also, the residual degree for the prime ideals dividing to l is $f = \min\{k | p^k \equiv 1 \pmod{l}\}$.

Theorem 1.30. *Let $K = \mathbb{Q}(\zeta_n)$ be the nth cyclotomic field. Then its ring of integers $\mathcal{O}_K$ is equal to $\mathbb{Z}[\zeta_n]$.*

In particular, when $n = p^r$ is a prime power, the integral basis is given by the set of primitive nth roots of unity. A straightforward but intricate computation then allows us to compute the discriminant.

Theorem 1.31. *The discriminant of $K = \mathbb{Q}(\zeta_n)$ is given by*

$$d_K = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

This theorem gives us the following corollary that will be useful when we later study the relationship between the field discriminant and the conductor.

Corollary 1.32. *For $K = \mathbb{Q}(\zeta_n)$ and an arbitrary prime l, $l \mid d_K \iff l \mid n$.*

The field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is called a cyclotomic extension. Every cyclotomic extension is Galois with an abelian Galois group, and the Galois group is cyclic when n is an odd prime power. Furthermore, any intermediate extension in a cyclotomic extension is also Galois and abelian. The converse is stated by the Kronecker-Weber Theorem (Theorem 2.3).

Theorem 1.33. *Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Then we have $\sigma(\zeta_n) = \zeta_n^a$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. This defines an isomorphism between the Galois group of the nth cyclotomic field and $(\mathbb{Z}/n\mathbb{Z})^\times$.*

This isomorphism is called the *cyclotomic character*. In particular, we have

Corollary 1.34. *If $n = p^a$ where p is an odd prime, then the Galois group of $\mathbb{Q}(\zeta_n)$ is cyclic.*

1.3 Ideal Class Group

The ideal class group is a measure of the failure of unique factorization in the ring of integers of a number field K. In order to define the ideal class group in a more general setting, we first introduce the fractional ideals.

Definition 1.35. A *fractional ideal* $\mathcal{I}$ of $\mathcal{O}_K$ is a $\mathcal{O}_K$-submodule of K such that there exists a nonzero integer m with $m\mathcal{I} \subset \mathcal{O}_K$.

It is worth noting that if $\mathcal{O}_K$ is a Principal Ideal Domain, then since for any ideal $\mathcal{I}$ in $\mathcal{O}_K$, we can write $\mathcal{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are prime ideals, for some $m \in \mathcal{O}_K$, $(m) = (p_1) \cdots (p_t)$ and $m = up_1 \cdots p_t$ where u is a unit and p_i's are rational primes. Therefore, in this case, we get that $\mathcal{O}_K$ is a Unique Factorization Domain. Of course, this is also indicated by the relationship of domains at the beginning of this paper.

Note that any ideal in $\mathcal{O}_K$ is a fractional ideal. The relationship between integral ideals and fractional ideals of $\mathcal{O}_K$ is similar to the one between integers and rational numbers, further advancing the theory of using ideals to study integrality in number fields. Like in $\mathbb{Q}$, we can define the inverse of a integral ideal $\mathfrak{a}$.

Definition 1.36. Let $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ be an integral ideal. Then we define $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-e_1} \cdots \mathfrak{p}_n^{-e_n}$, where $\mathfrak{p}_i^{-1} = \{x \in K \mid x\mathfrak{p}_i \subset \mathcal{O}_K\}$.

Any fractional ideal can be written as the quotient of two integral ideals, $\mathcal{I} = \frac{\mathfrak{a}}{\mathfrak{b}}$. Consequently, any fractional ideal can be written in the form

$$\mathcal{I} = \frac{\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}}{\mathfrak{q}_1^{k_1} \cdots \mathfrak{q}_m^{k_m}}.$$

The set of fractional ideals then becomes a commutative group under multiplication with identity $\mathcal{O}_K$.

Now we define an equivalence relation $\sim$ on the fractional ideals in K: Let $\mathcal{A}, \mathcal{B}$ be two fractional ideals in K. Then $\mathcal{A} \sim \mathcal{B}$ if and only $\mathcal{A} = (\alpha)\mathcal{B}$ with $\alpha \in K^\times$. Thus, in the case of a Principal Ideal Domain, any two ideals are equivalent. We get the intuition that the principal ideals are the identity elements in the equivalence relationship.

We can define the product of two equivalence classes $\mathcal{I}$, $\mathcal{J}$ as the equivalence class of $\mathcal{AB}$ where $\mathcal{A}, \mathcal{B}$ are representatives of $\mathcal{I}, \mathcal{J}$ respectively. The equivalence classes of $\sim$ then form a multiplicative group under this operation, of which the equivalence class containing the principal ideals is the identity element.

Definition 1.37. The group of equivalence classes of $\sim$ is called the *ideal class group* of K.

Equivalently, we can obtain the ideal class group of K, denoted C_K, by taking the quotient of the fractional ideals by the subgroup of principal ideals. Looking back at our observation earlier about Principal Ideal Domains, then it is not surprising that the ideal class group of a PID is trivial. This accurately describes the fact that PID's do not fail at unique factorization.

Moreover, it follows from the definition of fractional ideals that every equivalence class in the ideal class group has an integral ideal representative. Thus we can just consider the integral representatives when we study the ideal class group.

The main result about the ideal class group is:

Theorem 1.38. *The ideal class group of every number field is finite.*

This theorem allows us to define the class number. It describes how badly unique factorization fails in a certain number field.

Definition 1.39. The *class number* of a number field K is the order of its ideal class group.

The class number is an important property of a number field, as well as an elusive one to the number theorists, compared to the discriminant, for instance. Even for real quadratic fields, we know very little about the class number. For cubic fields, we have very limited results. Thus, in section 2 and 3, the main objective is to study the class number for a simple subset of cubic fields, the cyclic cubic fields.

1.4 Units

Let K be a number field, and $\mathcal{O}_K$ its ring of integers. A *unit* in $\mathcal{O}_K$ is an invertible element of $\mathcal{O}_K$. It is not hard to see that the units form a multiplicative subgroup of K^*, called the *unit group* of K.

Definition 1.40. $\alpha \in \mathcal{O}_K$ is called a *root of unity* if there exists $m \in \mathbb{Z}$, $m \neq 0$, such that $\alpha^m = 1$.

The following theorem describes the structure of the unit group of a number field.

Theorem 1.41 (Dirichlet's Unit Theorem)**.** *Let U_K be the unit group of K. Let $n = [K : \mathbb{Q}]$ and write $n = r_1 + 2r_2$, where r_1 and $2r_2$ are the number of real and nonreal embeddings of K in $\mathbb{C}$. Then there exists a set of units $\{\epsilon_1, \ldots, \epsilon_r\}$, where $r = r_1 + r_2 - 1$, such that every unit $\epsilon \in U_K$ can be written uniquely in the form*

$$\epsilon = \zeta \epsilon_1^{n_1} \cdots \epsilon_r^{n_r},$$

where $n_1, \ldots, n_r \in \mathbb{Z}$, and ζ is a root of unity in $\mathcal{O}_K$. In other words, if W_K is the subgroup of U_K that contains all the roots of unity, then W_K is finite and cyclic, and $U_K \cong W_K \times \mathbb{Z}^r$.

The units, $\epsilon_1, \ldots, \epsilon_r$ in the Unit Theorem are called the *fundamental units*. Observe that $\mathbb{Q}$, with $r_1 = 1, r_2 = 0$, and the imaginary quadratic fields, with $r_1 = 0, r_2 = 1$, are the only number fields with finitely many units.

The existence of fundamental units encourages mathematicians to find a set of fundamental units for each number field. Since the free part of the unit group is isomorphic to $\mathbb{Z}^r$ we can take the logarithm and get a lattice. The regulator measures the covolume of that lattice.

Definition 1.42. Let $\epsilon_1, \ldots, \epsilon_r$ be a system of fundamental units of a number field K, and $r = r_1 + r_2 - 1$, where r_1, r_2 are the numbers of real and nonreal embeddings respectively. Define the homomorphism $l_i : U_K \to \mathbb{R}^{r+1}$, $1 \leq i \leq r$ as the following:

$$l_i(u) = \begin{cases} \log |\sigma_i(u)| & 1 \leq i \leq r_1 \\ \log |\sigma_i(u)|^2 & r_1 + 1 \leq i \leq r, \end{cases}$$

where σ_i is the ith embedding. Then the regulator of K is $R_K = |\det(l_i(\epsilon_j)_{i,j=1}^r)|$.

We will revisit the regulator in the next section when we use it to find the class number of number fields through the class number formula, which we will not discuss in detail in this paper.

2 Cyclic Cubic Fields

Quadratic fields have been studied extensively, as shown by Example 1.13 in Section 1, so the next interesting degree fields are the cubic fields. The "nicest" cubic fields are the ones that are Galois extensions of $\mathbb{Q}$. They are called the cyclic cubic fields and their Galois groups are isomorphic to C_3, the cyclic group of order 3.

Cyclic cubic fields are totally real fields, i.e. all three roots of the minimal polynomial are real. That is because there is always one real root, and it must generate the splitting field. Thus, $r_1 = 3, r_2 = 0$ in the definition of fundamental units (Theorem 1.41), and the group of units has rank two (and the only roots of unity are ± 1). Here we mention a theorem from [Cu] that is useful for determining whether a pair of units in a totally real cubic field are fundamental units.

Definition 2.1. If α is in a totally real cubic field F, we let $\alpha, \alpha', \alpha''$ be the conjugates of α. Then $T(\alpha) = trace(\alpha^2) = \alpha^2 + \alpha'^2 + \alpha''^2$.

Theorem 2.2 (Cusick)**.** *If $T(\epsilon_2) \geq 2^{7/6} T(\epsilon_1)$, then ϵ_1, ϵ_2 are a pair of fundamental units.*
If not, but $T(\epsilon_2) \geq 12$, then either ϵ_1, ϵ_2 are a pair of fundamental units or there exists
i) a unit $\eta = \epsilon_1^{1/2}\epsilon_2^{1/2}$ such that $T(\eta) \leq (2T(\epsilon_1\epsilon_2))^{\frac{1}{2}}$ or
ii) a unit $\eta = \epsilon_1^{2/3}\epsilon_2^{1/3}$ such that $T(\eta) \leq (4T(\epsilon_1^2\epsilon_2))^{\frac{1}{3}}$.

2.1 Kronecker-Weber Theorem

Theorem 2.3 (Kronecker-Weber)**.** *If $K/\mathbb{Q}$ is a normal extension with Abelian Galois group, then K is contained in a suitable cyclotomic field $\mathbb{Q}(\zeta_m)$.*

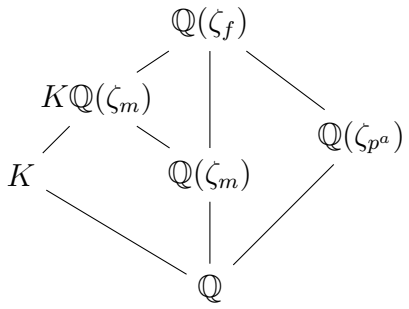
This theorem implies that, if we take $K = \cup_{m \geq 3} \mathbb{Q}(\zeta_m)$ we get a big Galois extension containing all abelian number fields. The proof of this theorem is beyond the scope of this paper. Some good references for the proof are [Na], [Ri], and [Wa]. The Kronecker-Weber Theorem allows us to introduce the concept of a *conductor*.

Definition 2.4. Let K be a normal abelian extension of $\mathbb{Q}$, then the *conductor* of K is the least integer f such that $K \subset \mathbb{Q}(\zeta_f)$.

We will now prove the following property of the conductor.

Proposition 2.5. *Let K be an abelian number field and p a prime. Then $p \mid d_K$ if and only if $p \mid f$, where f is the conductor of K.*

Proof. "$\Rightarrow$": If $p \mid d_K$, then by Dedekind's Theorem (Theorem 1.22), p ramifies in K, and since $K \subset \mathbb{Q}(\zeta_f)$, p ramifies in $\mathbb{Q}(\zeta_f)$. Again, by Dedekind's Theorem, $p \mid d_{\mathbb{Q}(\zeta_f)}$, and since $\mathrm{rad}(d_{\mathbb{Q}(\zeta_f)}) = \mathrm{rad}(f)$, $p \mid f$.



"$\Leftarrow$": Suppose $p \mid f$ but $p \nmid d_K$. Then p ramifies in $\mathbb{Q}(\zeta_f)$ but does not ramify in K. Thus the ramification index $e_{K/\mathbb{Q}}(\mathfrak{p}) = 1$ for any prime ideal $\mathfrak{p}$ in K such that $p\mathbb{Z} \subset \mathfrak{p}$. We can write $f = p^a m$, where $a \geq 1$ and $p \nmid m$. Let $N = [K\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)]$, and $\mathfrak{p}$ be any prime ideal in $\mathbb{Q}(\zeta_m)$ such that $p\mathbb{Z} \subset \mathfrak{p}$. By multiplicativity of ramification indices we have

$$\begin{aligned} & e_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}(1-\zeta_{p^a}) \\ = \; & e_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_{p^a})}(1-\zeta_{p^a}) e_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}}(1-\zeta_{p^a}) \\ = \; & e_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}}(1-\zeta_{p^a})\phi(m). \end{aligned}$$

Since $\mathbb{Q}(\zeta_f)$ is a Galois extension over $\mathbb{Q}$,

$$\begin{aligned} & e_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}(1-\zeta_{p^a}) \\ = \; & e_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}(\mathfrak{p}) \\ = \; & e_{\mathbb{Q}(\zeta_f)/K\mathbb{Q}(\zeta_m)}(\mathfrak{p}) e_{K\mathbb{Q}(\zeta_m)/K}(\mathfrak{p}) e_{K/\mathbb{Q}}(\mathfrak{p}) \\ = \; & e_{\mathbb{Q}(\zeta_f)/K\mathbb{Q}(\zeta_m)} \cdot 1 \cdot 1 \\ = \; & \phi(p^a). \end{aligned}$$

Therefore,

$$\phi(p^a) = e_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}(\mathfrak{p})$$

$$
\begin{aligned}
&= e_{\mathbb{Q}(\zeta_f)/K\mathbb{Q}(\zeta_m)}(\mathfrak{p}) \\
&\leq [\mathbb{Q}(\zeta_f) : K\mathbb{Q}(\zeta_m)] \\
&= [\mathbb{Q}(\zeta_f) : \mathbb{Q}(\zeta_m)]/N \\
&= \phi(f)/\phi(m)N \\
&= \phi(p^a)/N.
\end{aligned}
$$

Thus $N = 1$ and $K \subset \mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_f)$, contradicting the definition of the conductor f. □

2.2 The Even Rank Theorem

The Galois action of C_3 on the ideals of a cyclic cubic field $K/\mathbb{Q}$ allows us to obtain results on the class group.

Lemma 2.6. *For any ideal $\mathfrak{a} \in \mathcal{O}_K$, $\prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\mathfrak{a})$ is principal.*

Proof. $\mathfrak{a}\sigma(\mathfrak{a})\sigma^2(\mathfrak{a}) = N(\mathfrak{a})\mathbb{Z}$, and the ideal generated by the norm is principal. □

Theorem 2.7. *Suppose $K/\mathbb{Q}$ is a cyclic cubic field and $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$. Denote by σ a generator of the Galois group. Let C be the cyclic subgroup of the class group generated by the class of $\mathfrak{a}$, and let $\sigma(\mathfrak{a})$ and $\sigma^2(\mathfrak{a})$ be the conjugates of $\mathfrak{a}$. Then either*

i) $[\mathfrak{a}]$, $[\sigma(\mathfrak{a})]$ and $[\sigma^2(\mathfrak{a})]$ all belong to C,

or

ii) Neither $[\sigma(\mathfrak{a})]$ nor $[\sigma^2(\mathfrak{a})]$ belongs to C. (In particular, $[\mathfrak{a}]$, $[\sigma(\mathfrak{a})]$ and $[\sigma^2(\mathfrak{a})]$ are all distinct.)

If m denotes the order of $[\mathfrak{a}]$ and the first case holds then m cannot be divisible by any prime $p \equiv 2 \pmod 3$.

Proof. If $\sigma(\mathfrak{a}) = (x)\mathfrak{a}$, then $\sigma^2(\mathfrak{a}) = (\sigma(x))\sigma(\mathfrak{a}) = (x\sigma(x))\mathfrak{a}$.Thus $\mathfrak{a}$, $\sigma(\mathfrak{a})$ and $\sigma^2(\mathfrak{a})$ are all in the same class.

Suppose that $[\sigma(\mathfrak{a})] \notin ([\mathfrak{a}])$, and $[\sigma^2(\mathfrak{a})] \in ([\mathfrak{a}])$. Then $[\sigma^2(\mathfrak{a})] = [\mathfrak{a}]^k$ for some integer k.

By Lemma 2.6, $[\mathfrak{a}][\sigma(\mathfrak{a})][\sigma^2(\mathfrak{a})] = 1$, so

$$
\begin{aligned}
[\mathfrak{a}]^m = 1 &\implies [\sigma(\mathfrak{a})][\sigma^2(\mathfrak{a})] = [\mathfrak{a}]^{m-1} \\
&\implies [\sigma(\mathfrak{a})] = [\mathfrak{a}]^{m-1-k} \in ([\mathfrak{a}]),
\end{aligned}
$$

contradictory to our assumption that $[\sigma(\mathfrak{a})] \notin ([\mathfrak{a}])$.

Therefore, either all the conjugates are in the same cyclic subgroup, or all of them are in different classes.

In the first case, i.e. when the conjugates belong to the same cyclic subgroup, if $[\sigma(\mathfrak{a})] = [\mathfrak{a}^x]$, then $[\sigma^2(\mathfrak{a})] = [\mathfrak{a}^{x^2}]$. Since the product of all the conjugates is principal by Lemma 2.6, $1 + x + x^2 \equiv 0 \pmod{m}$. Thus

$$\begin{aligned} & 4 + 4x + 4x^2 \equiv 0 \pmod{m} \\ \Longrightarrow\ & 1 + 4x + 4x^2 \equiv -3 \pmod{m} \\ \Longrightarrow\ & (2x+1)^2 \equiv -3 \pmod{p}, \text{ for all } p|m. \end{aligned}$$

Therefore, $p = 3$ or $p \equiv 1(3)$. So if m is divisible by any prime $p \equiv 2 \pmod 3$, then the conjugates must be in different classes. □

Since the class group is a finite abelian group, it can be written as a product of finitely many cyclic groups of prime-power order, and this decomposition is unique up to permutation.[Go, 73]

Definition 2.8. The p-rank of an abelian group is the minimum number of p^r-cyclic factors.
The p^n-rank of an abelian group, $r_{p^{\alpha_i}}$, is the minimum number of cyclic factors of order p^m, $m \geq n$.
Suppose $m = \prod_i p_i^{\alpha_i}$, then the m-rank of an abelian group is $r_m = \min\{r_{p^{\alpha_i}}\}$.

Theorem 2.9. *If m is divisible only by primes $p \equiv 2 \pmod 3$, and K is a cyclic cubic field, then the m-rank of the class group of K is even.*

Proof. For $p \equiv 2 \pmod 3$, if the p-Sylow subgroup is written as the direct product of cyclic subgroups:

$$\prod_{n=1}^{\infty} [C(p^n)]^{s_n},$$

then the p-rank is

$$r_p = \sum_{m=1}^{\infty} s_m.$$

The p^n-rank is

$$r_{p^n} = r(n) = \sum_{m=n}^{\infty} s_m.$$

Let

$$P_n = \prod_{m=1}^{n} p^{ms_m}.$$

Then the number of elements M_n of order $\leq p^n$ is

$$\begin{aligned} M_n &= P_{n-1}p^{nr(n)} \\ &= P_{n-1}p^{nr(n+1)+ns_n} \\ &= P_{n-1}p^{ns_n}p^{nr(n+1)} \\ &= P_n p^{nr(n+1)}, \end{aligned}$$

so the number of elements of order exactly p^n is

$$\begin{aligned} M_n - M_{n-1} &= P_{n-1}p^{nr(n)} - P_{n-1}p^{(n-1)r(n)} \\ &= P_{n-1}p^{(n-1)r(n)}\left(p^{r(n)} - 1\right). \end{aligned}$$

By Lemma 2.7, since m is divisible by primes $p \equiv 2 \pmod 3$, the second case holds, i.e., for any ideal $\mathfrak{a} \in \mathcal{O}_K$, $\mathfrak{a}$ and its conjugates are all in different classes. Since the conjugates have the same order, $M_n - M_{n-1}$, the number of elements of order p^n, is divisible by 3.

We have $3 \nmid P_{n-1}p^{(n-1)r(n)}$, so $p^{r(n)} \equiv 1 \pmod 3$. Since $p \equiv 2 \pmod 3$, the p^n-rank $r(n)$ is even for all n.

Suppose $m = \prod_i p_i^{\alpha_i}$, then $r_m = \min\{r_{p^{\alpha_i}}\}$ is also even. □

2.3 Primes of the Form $A^2 + 3B^2$

Lemma 2.10. $p \equiv 1 \pmod 3 \implies p = A^2 + 3B^2$ *for some integers* A *and* B.

Proof. Let K be the field $\mathbb{Q}(\sqrt{-3})$, and $\mathcal{O}_K \subset \mathbb{Q}(\sqrt{-3})$ be the ring of algebraic integers in K. We know that

$$\begin{aligned} \mathcal{O}_K &= \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right], \\ \left[\mathcal{O}_K : \mathbb{Z}[\sqrt{-3}]\right] &= 2. \end{aligned}$$

Let p be a prime in $\mathbb{Z}$. Suppose $p \neq 2$, so that $p \nmid \left[\mathcal{O}_K : \mathbb{Z}[\sqrt{-3}]\right]$. The minimal polynomial $f(x)$ of $\sqrt{-3}$ is $x^2 + 3$.

We have that $f(x)$ is irreducible mod p if $p \equiv 2 \pmod 3$, since if $f(x)$ were reducible then it has roots and -3 is a square mod p. If $p \equiv 1 \pmod 3$ and $f(x) = x^2 + 3 = (x+i)(x-i) \pmod p$ where $i \in \mathbb{Z}$, then $i^2 \equiv -3 \pmod p$, and $(x+i), (x-i)$ are irreducible mod p.
Thus, by Theorem 1.24,

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2,$$

where $\mathfrak{p}_1, \mathfrak{p}_2$ are prime ideals.

Since $\mathcal{O}_K$ is a PID, $(p) = (\pi_1)(\pi_2)$, where $\pi_1 \in \mathfrak{p}_1$ and $\pi_2 \in \mathfrak{p}_2$, and $p = \pi_1\pi_2$. Let $\omega = \dfrac{-1+\sqrt{-3}}{2}$. Then

$$p = (a + b\omega)(a - b\omega),$$

where $a, b \in \mathbb{Z}$. We also have $\omega^2 = \dfrac{-1-\sqrt{-3}}{2}$, and $\omega^3 = 1$, so $\omega, \omega^2, \omega^3$ are all units.

Now let us look at three different cases.

Case I: b **is even**.

Since b is even,

$$a + b\omega = \left(a - \frac{b}{2}\right) + \frac{b}{2}\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}].$$

Then the norm of $a + b\omega$ is $N(a + b\omega) = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$.

$$\begin{aligned} N(p) &= N(a + b\omega)N(a - b\omega) \\ p^2 &= (x^2 + 3y^2)N(a - b\omega) \end{aligned}$$

Thus $p = x^2 + 3y^2$ for $x, y \in \mathbb{Z}$.

Case II: b **is odd,** a **is even**.

Since a is even,

$$\omega^2(a + b\omega) = a\omega^2 + b = \left(-\frac{a}{2} + b\right) - \frac{a}{2}\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}].$$

Then the norm of $a\omega^2 + b$ is $N(a\omega^2 + b) = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$.

$$N(p\omega^2) = N(a\omega^2 + b)N(a - b\omega)$$

$$p^2 \cdot 1 = (x^2 + 3y^2)N(a - b\omega)$$

Thus $p = x^2 + 3y^2$ for $x, y \in \mathbb{Z}$.

Case III: b is odd, a is odd.
Since a, b are both odd,

$$\omega(a + b\omega) = a\omega + b\omega^2 = \frac{-a-b}{2} + \frac{a-b}{2}\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}].$$

Then the norm of $a\omega + b\omega^2$ is $N(a + b\omega) = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$.

$$N(p\omega) = N(a\omega + b\omega^2)N(a - b\omega)$$
$$p^2 \cdot 1 = (x^2 + 3y^2)N(a - b\omega)$$

Thus $p = x^2 + 3y^2$ for $x, y \in \mathbb{Z}$.
Therefore, p is in the form of $A^2 + 3B^2$. □

Theorem 2.11. *An integer n is of the form $A^2 + 3B^2, A, B \in \mathbb{Z}, (A, B) = 1$, if and only if all its prime divisors with an odd power are of the form $A^2 + 3B^2, A, B \in \mathbb{Z}$.*

Proof. " $\Leftarrow$ ": Suppose $n = D^2 \prod_i p_i$, and $p_i = a_i^2 + 3b_i^2$ for all i. Since

$$(a^2 + 3b^2)(c^2 + 3d^2) = a^2c^2 + 9b^2d^2 + 3a^2d^2 + 3b^2c^2 = (ac + 3bd)^2 + 3(ad - bc)^2,$$

the product of p_i's is also in the form $A^2 + 3B^2$, so $n = D^2(A^2 + 3B^2) = (AD)^2 + 3(BD)^2$.
" $\Rightarrow$ ": Suppose prime p divides n. By quadratic reciprocity, either p divides n an even number of times, or $\left(\frac{-3}{p}\right) = 1$.
By quadratic reciprocity, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Thus, $p \equiv 1(3)$. By Lemma 2.10, p is of the form $A^2 + 3B^2, A, B \in \mathbb{Z}$. □

The theorem in the last section can then be interpreted as:"the class number of a cyclic cubic field is an integer of the form $A^2 + 3B^2$". This result was also proved by Hasse using the Kronecker-Weber theorem to relate the class groups of K and $\mathbb{Q}(\zeta_f)$.

3 Simplest Cubic Fields

To further study the properties of cubic fields, we have to restrict ourselves to a "simple" subset of the cyclic cubic fields, namely those generated by $f(x) = x^3 - ax^2 - (a+3)x - 1$ where $a \in \mathbb{Z}$, called the *simplest cubic fields* by Daniel Shanks[Sh]. Assuming that $a^2 + 3a + 9$ is prime, the splitting field K of this cubic equation has discriminant

$$d_K = (a^2 + 3a + 9)^2$$

The simplest cubic fields normal extensions of $\mathbb{Q}$, and all unramified primes either split completely in the fields or do not split at all since the Galois group is cyclic and if one root is in K then all roots are in K. Furthermore, there are two fundamental units, since they are totally real fields and have three real embeddings and no non-real embedding.

Observe that $(-3-a)^2+3(-3-a)+9 = a^2+3a+9$, so $\sqrt{d_K}$ is symmetric over $a = -3/2$. Therefore, we only need to study the values of $a \geq -1$. Shanks[Sh, 4] has a table of the first 100 values of a, primes P, and corresponding class numbers. The class numbers are computed using the analytic class number formula[Sh, 3].

Let ρ be a root of f. Then one may verify that the three roots of f are

$$\rho_1 = \rho,\ \rho_2 = \frac{-1}{1+\rho} \text{ and } \rho_3 = \frac{-1}{1+\rho_2}.$$

Since $\rho(\rho^2 - a\rho - a - 3) = 1$, ρ is a unit of K. Similarly, ρ_2 is a unit, so $\rho + 1 = \dfrac{-1}{\rho_2}$ is also a unit. We now verify that ρ and $\rho + 1$ are in fact a pair of fundamental units using Cusick's criterion (Theorem 2.2).

First, let $\epsilon_1 = \rho$ and $\epsilon_2 = \rho + 1$. Then the conjugates of ϵ_1 are $\epsilon_1 = \rho$, $\epsilon_1' = -\dfrac{1}{1+\rho}$ and $\epsilon_1'' = -\dfrac{1}{1+\epsilon_1'} = -\dfrac{1+\rho}{\rho}$. Thus

$$\begin{aligned} T(\epsilon_1) &= \rho^2 + \frac{1}{(1+\rho)^2} + \frac{(1+\rho)^2}{\rho^2} \\ &= \frac{\rho^4(1+\rho)^2 + \rho^2 + (1+\rho)^4}{(1+\rho)^2\rho^2}. \end{aligned}$$

Similarly, the conjugates of ϵ_2 are $\epsilon_2 = 1 + \rho$, $\epsilon_2' = -\dfrac{1}{2+\rho}$ and $\epsilon_2'' =$

$-\dfrac{1}{1+\epsilon_2'} = -\dfrac{2+\rho}{1+\rho}$. Thus

$$\begin{aligned} T(\epsilon_2) &= (1+\rho)^2 + \frac{1}{(2+\rho)^2} + \frac{(2+\rho)^2}{(1+\rho)^2} \\ &= \frac{(1+\rho)^4(2+\rho)^2 + (1+\rho)^4 + (2+\rho)^2(1+\rho)^2}{(1+\rho)^2(2+\rho)^2}. \end{aligned}$$

Then

$$\frac{T(\epsilon_2)}{T(\epsilon_1)} = \frac{\rho^2[(1+\rho)^4(2+\rho)^2 + (1+\rho)^4 + (2+\rho)^2(1+\rho)^2]}{(2+\rho)^2[\rho^4(1+\rho)^2 + \rho^2 + (1+\rho)^4]}.$$

By computation, for $a \geq -1$, $\dfrac{T(\epsilon_1)}{T(\epsilon_2)} \geq 2^{\frac{7}{6}}$. Therefore, ϵ_1 and ϵ_2 are a pair of fundamental units.

We can now determine the regulator of K. Our fundamental units are ρ and $1+\rho$, and our embeddings are $\sigma_1 : \rho \mapsto \rho$ and $\sigma_2 : \rho \mapsto \frac{-1}{1+\rho}$. The regulator

$$\begin{aligned} R_K &= \det \begin{pmatrix} \log|\rho| & \log|1+\rho| \\ \log\left|\frac{-1}{1+\rho}\right| & \log\left|\frac{\rho}{1+\rho}\right| \end{pmatrix} \\ &= \log^2|\rho| - \log|\rho| \log|1+\rho| + \log^2|1+\rho|. \end{aligned}$$

One may compute the regulator explicitly by finding the trigonometric solution of $f(x) = 0$. First, in the polynomial $x^3 - ax^2 - (a+3)x - 1$, substitute $x = y + \dfrac{a}{3}$, and then $y = \dfrac{2}{3}\sqrt{a^2+3a+9}z$. Let $z = \cos\theta$, then after simplifying and scaling by $\dfrac{216}{2}$ we get:

$$\begin{aligned} \cos 3\theta &= -\frac{2a+3}{2\sqrt{a^2+3a+9}}, \\ \sin 3\theta &= \frac{3}{2}\sqrt{3}\sqrt{\frac{1}{a^2+3a+9}}. \end{aligned}$$

Now we can solve for θ:

$$\theta = \frac{1}{3}\arctan\frac{\sqrt{27}}{2a+3}.$$

Then substitute back to find x, the root of $x^3 - ax^2 - (a+3)x - 1$, denoted ρ here.

$$\rho = \frac{1}{3}(2\sqrt{P}\cos\theta + a),$$

which allows us to compute R_K. Shanks[Sh, 3] uses power series to get an approximation to R_K, which he then combines with the class number formula to compute the class numbers. He remarks that the class numbers are smaller than expected, considering the large field discriminants. For more recent work on the class number, one can read the Cohen-Lenstra Heuristics[CL].

References

[CL] Cohen H., Lenstra H.W. *Heuristics on class groups*. In: Chudnovsky D.V., Chudnovsky G.V., Cohn H., Nathanson M.B. (eds) Number Theory. Lecture Notes in Mathematics, vol 1052. Springer, Berlin, Heidelberg (1984)

[Co] D. Cox, *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*, Pure and Applied Mathematics: A Wiley Series of Texts" Monographs and Tracts (1997)

[Cu] T. W. Cusick, *Finding fundamental units in cubic fields*, Mathematical Proceedings of the Cambridge Philosophical Society, 92(3), 385-389 (1982)

[Go] F. Gouvêa. *A Guide to Groups, Rings, and Fields*, Mathematical Association of America (2012)

[Ja] F. Jarvis, *Algebraic Number Theory*, Springer Undergraduate Mathematics Series, Springer International Publishing Switzerland (2014)

[Mu] M. R. Murty, J. Esmonde *Problems in Algebraic Number Theory*, Graduate Texts in Mathematics, Springer-Verlag New York (2005)

[Na] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer Monographs in Mathematics, Springer-Berlin Heidelberg (2013)

[Ri] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer-Verlag New York (2001)

[Sa] P. Samuel, *Algebraic Theory of Numbers*, Reprint of the Hermann, Paris, and Houghton Mifflin Company, Boston (1970)

[Sh] D. Shanks, *The Simplest Cubic Fields*, Mathematics of Computation, Volume 28, Number 128, 1137-1152 (1974)

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag New York (1997)