May 2020

The Fundamental System of Units for Cubic Number Fields

Janik Huth
University of Wisconsin-Milwaukee

THE FUNDAMENTAL SYSTEM OF UNITS FOR CUBIC NUMBER FIELDS

by

Janik Huth

A Thesis Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Master of Science

in Mathematics

at

The University of Wisconsin-Milwaukee

May 2020

ABSTRACT

THE FUNDAMENTAL SYSTEM OF UNITS FOR CUBIC NUMBER FIELDS

by

Janik Huth

The University of Wisconsin-Milwaukee, 2020
Under the Supervision of Professor Allen D. Bell

Let K be a number field of degree n. An element $\alpha \in K$ is called integral, if the minimal polynomial of α has integer coefficients. The set of all integral elements of K is denoted by $\mathcal{O}_K$. We will prove several properties of this set, e.g. that $\mathcal{O}_K$ is a ring and that it has an integral basis. By using a fundamental theorem from algebraic number theory, Dirichlet's Unit Theorem, we can study the unit group $\mathcal{O}_K^\times$, defined as the set of all invertible elements of $\mathcal{O}_K$. We will prove Dirichlet's Unit Theorem and look at unit groups for the special case of cubic number fields of type $(1,1)$. The structure of the unit group allows us to define a fundamental unit for this type of field. We will study the relation between the discriminant of the number field and this fundamental unit.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

First and foremost, I want to thank Prof. Allen Bell for supervising my thesis and working with me for the last two semesters. It was a great experience and I learned a lot while working on this thesis.

I want to thank Prof. Jeb Willenbring and Prof. Yi Ming Zou for being part of my thesis committee.

Finally, I want to thank my parents for their constant support and encouragement.

1 Introduction

Throughout this paper, we will assume that K is a finite field extension of the rational numbers $\mathbb{Q}$, a so called number field. In Chapter 2, we will study these number fields. We are mostly interested in the field homomorphisms embedding K into the field of complex numbers $\mathbb{C}$. It turns out that the number of distinct embeddings from K into $\mathbb{C}$ is the same as the degree of the number field K. Using these embeddings, we can define a norm on K, which will be useful for studying the unit group of K, which we will do in Chapter 3.

Another important definition we will look at is the set of integral elements of K, denoted by $\mathcal{O}_K$. We will prove that $\mathcal{O}_K$ is a ring and will look at several properties of this ring. It turns out that every element of $\mathcal{O}_K$ can be uniquely written as a $\mathbb{Z}$-linear combination of finitely many elements of $\mathcal{O}_K$.

In Chapter 3, we will study a fundamental result from algebraic number theory: Dirichlet's Unit Theorem. With this theorem, we will be able to understand the structure of the unit group $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \setminus \{0\} | \alpha^{-1} \in \mathcal{O}_K\}$. It turns out that for a fixed K, there is a finite number of elements in $\mathcal{O}_K^\times$, such that we can uniquely express every other element in $\mathcal{O}_K^\times$ with these finite elements. We will prove Dirichlet's Unit Theorem in Chapter 3, using results about the ideal class group of K and about ideals in $\mathcal{O}_K$ in general.

In Chapter 4, we will take a closer look at the special case of cubic field extensions. We will use SageMath to find unit groups of these cubic fields. We will also look at the relation between the discriminant of a specific class of number fields and the corresponding fundamental system of units.

2 Number fields

Definition 2.1

A *number field* is a finite field extension K of the field of the rational numbers $\mathbb{Q}$. The *degree* of K is the dimension

$$[K : \mathbb{Q}] := \dim_{\mathbb{Q}} K.$$

Let K be a fixed number field of degree n. For any element $\alpha \in K$ there is a $\mathbb{Q}$-linear relation between the first $n+1$ powers of α, i.e. there exists rational numbers $a_0, a_1, \dots, a_n \in \mathbb{Q}$ not all zero such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0. \tag{1}$$

In other words, α is a root in K of the nonzero polynomial $a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$. We say that α is *algebraic over* $\mathbb{Q}$.

Consider the ring homomorphism

$$\phi_\alpha : \mathbb{Q}[x] \to K, g \mapsto g(\alpha)$$

Then the kernel of ϕ_α,

$$I := \{f \in \mathbb{Q}[x] | f(\alpha) = 0\} \subset \mathbb{Q}[x]$$

is an ideal. Since $\mathbb{Q}[x]$ is an euclidean domain, it is also a PID. It follows that $I = (m_\alpha)$ for a nonzero polynomial m_α. We can assume that m_α is monic, i.e. $m_\alpha = b_0 + b_1x + \cdots + x^d$. This condition determines m_α uniquely.

Definition 2.2

The monic polynomial m_α just defined is called the *minimal polynomial* of α. Its degree

$d = \deg(m_\alpha)$ is called the *degree of* α *over* $\mathbb{Q}$.

By the division algorithm, we have that

$$f(\alpha) = 0 \Leftrightarrow m_\alpha | f \tag{2}$$

for all $f \in \mathbb{Q}[x]$.

Proposition 2.3

Let K be a number field of degree n and let $\alpha \in K$. Let $\mathbb{Q}[\alpha]$ denote the smallest subring of K containing α. Then $\mathbb{Q}[\alpha]$ is a subfield of K with $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg_{\mathbb{Q}}(\alpha)$.

Theorem 2.4

Let K be a number field. Then there exists an element $\alpha \in K$ such that $K = \mathbb{Q}[\alpha]$.

An element $\alpha \in K$ with $K = \mathbb{Q}[\alpha]$ is called a *primitive element* or a *generator* of the number field K.

Proof. See for example [Art11, Chapter 14,§4].

□

We can also think of number fields as subfields of the complex numbers:

Corollary 2.5

Let K be a number field of degree n. Then there are exactly n distinct field homomorphisms

$$\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$$

embedding K into the field of complex numbers.

Proof. Let $\alpha \in K$ be a primitive element for K. Over $\mathbb{C}$, the minimal polynomial m_α decomposes into n linear factors,

$$m_\alpha = \prod_{i=1}^{n} (x - \alpha_i)$$

with $\alpha_i \in \mathbb{C}$. Since m_α is irreducible over $\mathbb{Q}$, the roots α_i are pairwise distinct.

For $i \in \{1, \dots, n\}$, we define pairwise distinct homomorphisms as follows:

$$\sigma_i : K \to \mathbb{C}, f(\alpha) \mapsto f(\alpha_i).$$

This is well definied by (2) and since $m_\alpha(\alpha_i) = 0$.

Conversely, let $\sigma : K \to \mathbb{C}$ be a field homomorphism. Then

$$m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0.$$

It follows that $\sigma(\alpha) = \alpha_i$ for some i and hence $\sigma = \sigma_i$. □

Remark 2.6

Let K be a number field of degree n and let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding into $\mathbb{C}$. If we compose σ with the complex conjugation $z \mapsto \bar{z}$, we obtain another embedding $\bar{\sigma} : K \hookrightarrow \mathbb{C}$. We see that $\bar{\sigma} = \sigma \Leftrightarrow \sigma(K) \subset \mathbb{R}$. In this case we call σ a *real embedding.* Otherwise, we call $\{\sigma, \bar{\sigma}\}$ a *pair of complex conjugate embeddings.*

After we change the order of the embeddings from Corollary 2.5, we may assume that

$$\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$$

are all the real embeddings and that

$$\{\sigma_{r+2i-1}, \sigma_{r+2i}\}, \quad i = 1, \dots, s$$

are all the pairs of complex conjugate embeddings.

We have that $n = r + 2s$.

Definition 2.7

The pair (r, s) from above is called the *type* of the number field K.

Definition 2.8

Let K be a number field of degree n and let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$. Let $\alpha \in K$. Then we call

$$N_{K/\mathbb{Q}}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha)$$

the *norm* of α and

$$T_{K/\mathbb{Q}}(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha)$$

the *trace* of α.

Lemma 2.9

Let K be a number field of degree n and let $\alpha \in K$. Let $f = a_0 + a_1 x + \cdots + x^m$ be the minimal polynomial of α. Then

$$N_{K/\mathbb{Q}}(\alpha) = (-1)^n a_0^{n/m}, \qquad T_{K/\mathbb{Q}}(\alpha) = -\frac{n}{m} a_{m-1}$$

Proof. See [NS13, Chapter 1, §2]. □

Definition 2.10

Let K be a number field of degree n. An element $\alpha \in K$ is called *integral*, if the minimal polynomial of α has integer coefficients, i.e. $m_\alpha \in \mathbb{Z}[x]$.

We let $\mathcal{O}_K \subset K$ be the set of all integral elements of K.

Definition 2.11

A *$\mathbb{Z}$-submodule* $M \subset K$ is a subgroup of the additive group $(K, +)$.

It is called *finitely generated* if there exist elements $\beta_1, \ldots, \beta_k \in K$ such that

$$M = \langle \beta_1, \ldots, \beta_k \rangle_{\mathbb{Z}} := \{\sum_{i=1}^{k} a_i \beta_i | a_i \in \mathbb{Z}\}$$

Theorem 2.12

Let $\alpha \in K$. The following statements are equivalent:

(i) $\alpha \in \mathcal{O}_K$

(ii) There exists a monic polynomial $f = a_0 + a_1x + \cdots + x^k \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$

(iii) There exists a finitely generated $\mathbb{Z}$-submodule $M \subset K$ such that $\alpha M \subset M$

Proof. The implication (i)⇒ (ii) is true by definition of $\mathcal{O}_K$. Conversely, let $f = a_0 + a_1x + \cdots + x^k \in \mathbb{Z}[x]$ with $f(\alpha) = 0$. By (2), we know that $m_\alpha | f$ in $\mathbb{Q}[x]$. By the Lemma of Gauss, we know that $m_\alpha \in \mathbb{Z}[x]$ has integral coefficients as well. This proves (ii)⇒(i).

Next, assume that (ii) holds. Define

$$M := \langle 1, \alpha, \ldots, \alpha^{k-1} \rangle_{\mathbb{Z}} \subset K.$$

Then, we have that

$$\alpha\alpha^i = \begin{cases} \alpha^{i+1} \in M, & i < k-1 \\ \alpha^k = -a_0 - a_1\alpha - \cdots - a_{k-1}\alpha^{k-1} \in M, & i = k-1 \end{cases}$$

for $i = 0, \ldots, k-1$. Therefore, $\alpha M \subset M$.

Conversely, let $M = \langle \beta_1, \ldots, \beta_k \rangle_{\mathbb{Z}} \subset K$ be a finitely generated $\mathbb{Z}$-submodule with $\alpha M \subset M$. For each $i = 1, \ldots, k$, we can write

$$\alpha\beta_i = \sum_{j=1}^{k} a_{i,j}\beta_j$$

for some integers $a_{i,j} \in \mathbb{Z}$. Then, the vector $\beta := (\beta_1, \ldots, \beta_k)^t \in K^k$ is an eigenvector of the matrix $A := (a_{i,j})$. It follows that $f(\alpha) = 0$, where $f = \det(A - xI_n) \in \mathbb{Z}[x]$ is the characteristic polynomial of A. Since f is monic and integral, (ii) holds. □

Remark 2.13

For $\alpha \in K$ we denote by $\mathbb{Z}[\alpha]$ the smallest subring of K containg α. Then as a $\mathbb{Z}$-submodule of K, $\mathbb{Z}[\alpha]$ is generated by the powers of α:

$$\mathbb{Z}[\alpha] = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\mathbb{Z}}$$

From the proof of Theorem 2.12, we know that $\alpha \in \mathcal{O}_K$ if and only if $\mathbb{Z}[\alpha] \subset K$ is a finitely generated submodule.

Theorem 2.14

The subset $\mathcal{O}_K \subset K$ is a subring.

Proof. Let $\alpha, \beta \in \mathcal{O}_K$. We have to show that $\alpha \pm \beta \in \mathcal{O}_K$ and that $\alpha\beta \in \mathcal{O}_K$.

Let $\mathbb{Z}[\alpha, \beta] \subset K$ be the smallest subring of K containing α and β. As a $\mathbb{Z}$- submodule of K, $\mathbb{Z}[\alpha, \beta]$ is generated by the monomials $\alpha^i\beta^j, i, j \geq 0$. By the argument in the proof of Theorem 2.12, we have that

$$\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\alpha] + \beta\mathbb{Z}[\alpha] + \cdots + \beta^{k-1}\mathbb{Z}[\alpha] \tag{3}$$

for some $k \in \mathbb{N}$. Again, by Theorem 2.12, we know that $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-submodule. By (3), we see that $\mathbb{Z}[\alpha, \beta]$ is also a finitely generated $\mathbb{Z}$-submodule.

Then, we have that

$$(\alpha \pm \beta) \cdot \mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta] \text{ and } \alpha\beta \cdot \mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta].$$

Therefore, Theorem 2.12 shows that $\alpha \pm \beta \in \mathcal{O}_K$ and $\alpha\beta \in \mathcal{O}_K$. □

Remark 2.15

For any element $\alpha \in K$ there exists a nonzero integer $r \in \mathbb{Z}$ such that $r\alpha \in \mathcal{O}_K$:

By (1), we know that there exist elements $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. By multiplying by the lcm of the denominators of $a_i = \frac{r_i}{q_i}$, we can assume that $a_n' = r \in \mathbb{Z}$. We set $a_i' := a_i \cdot \operatorname{lcm}(q_1, \ldots, q_n)$ for $i = 0, \ldots, n-1$. Then, if we multiply the new equation

$$a_0' + a_1'\alpha + \cdots + r\alpha^n = 0$$

by r^{n-1}, we get that

$$a_0'r^{n-1} + a_1'r^{n-1}\alpha + \cdots + r \cdot r^{n-1}\alpha^n = 0$$

Rewriting this yields that

$$a_0'r^{n-1} + a_1'r^{n-2}(r \cdot \alpha) + \cdots + (r \cdot \alpha)^n = 0$$

Therefore, $r\alpha$ is integral, i.e. $r\alpha \in \mathcal{O}_K$.

Next, we need two definitions to define the discriminant of a fixed number field K, which we will need later.

Definition 2.16

An additive subgroup $M \subset K$ is called a *lattice* if there exists a $\mathbb{Q}$-basis $(\beta_1, \dots, \beta_n)$ of K such that

$$M = \langle \beta_1, \dots, \beta_n \rangle_{\mathbb{Z}}.$$

We call the tuple $\beta := (\beta_1, \dots, \beta_n)$ an *integral basis* of M.

Example 2.17

Let $D \in \mathbb{Z}$ be a nonzero, squarefree integer. Then $K := \mathbb{Q}[\sqrt{D}]$ is a quadratic number field, i.e. a number field of degree 2. In this example, we determine the ring of integral elements $\mathcal{O}_K$. An arbitrary element $\alpha \in K$ is of the form $\alpha = a + b\sqrt{D}$ for $a, b \in \mathbb{Q}$. We have that $\alpha \in \mathbb{Q}$ if and only if $b = 0$. Since $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, we may assume $b \neq 0$.
Let $\tau : K \to K$ be the unique nontrivial automorphism of K.
The minimal polynomial of α is

$$m_\alpha = (x - \alpha)(x - \tau(\alpha)) = x^2 - 2ax + (a^2 - Db^2).$$

Therefore, $\alpha \in \mathcal{O}_K \Leftrightarrow 2a \in \mathbb{Z}, a^2 - Db^2 \in \mathbb{Z}$. We look at 3 different cases:

(i) $D \equiv 1 \bmod 4$:

Since $2a \in \mathbb{Z}$, we have that $a = \frac{r}{2}$ for some $r \in \mathbb{Z}$. We also have that $a^2 - Db^2 \in \mathbb{Z}$. One can show that this implies that $b = \frac{s}{2}$ for some $s \in \mathbb{Z}$. Rewriting yields that $a^2 - Db^2 = \frac{r^2}{4} - D\frac{s^2}{4}$, which implies that $r^2 - Ds^2 \equiv 0 \bmod 4$. Since $D \equiv 1 \bmod 4$, it follows that $r \equiv s \bmod 2$, i.e. $r = s + 2t$ for some $t \in \mathbb{Z}$.
Then, $\alpha = \frac{r}{2} + \frac{s}{2}\sqrt{D} = t + s\frac{1+\sqrt{D}}{2}$, so in this case $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

(ii) $D \equiv 2 \bmod 4$:

Using the same arguments as in (i), we find that $r^2 + 2s^2 \equiv 0 \bmod 4$. The only possible solution to this congruence is $(r, s) \equiv (0, 0) \bmod 4$, which implies that $a, b \in \mathbb{Z}$. So in this case, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$.

(iii) $D \equiv 3 \bmod 4$:

Here, we find that $r^2 + s^2 \equiv 0 \bmod 4$, which again only has the solution $(r, s) \equiv (0, 0) \bmod 4$. Again, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$ in this case.

Definition 2.18

Let $M \subset K$ be a lattice with integral basis $\beta := (\beta_1, \dots, \beta_n)$. Then we define the rational number

$$d(\beta) := \det(T_{K/\mathbb{Q}}(\beta_i \beta_j))_{i,j} \in \mathbb{Q}.$$

In the following Lemma 2.19, we will show that this number only depends on the lattice M, not on the basis β.

Therefore, we define $d(M) := d(\beta)$ to be the *discriminant of* M.

Lemma 2.19

Let $M' \subset K$ be another lattice with integral basis $\beta' = (\beta'_1, \dots, \beta'_n)$.

(i) If $T \in \mathrm{GL}_n(\mathbb{Q})$ is the change of base matrix from β to β', i.e. $\beta \cdot T = \beta'$, then $d(\beta') = \det(T)^2 \cdot d(\beta)$.

(ii) If $M = M'$, then $d(\beta) = d(\beta')$.

(iii) $d(\beta) \neq 0$ and if $M \subset \mathcal{O}_K$, then $d(\beta) \in \mathbb{Z}$ is an integer.

Proof. Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$ and define

$$S := \begin{pmatrix} \sigma_1(\beta_1) & \dots & \sigma_1(\beta_n) \\ \vdots & & \vdots \\ \sigma_n(\beta_1) & \dots & \sigma_n(\beta_n) \end{pmatrix} \in M_{n,n}(\mathbb{C}).$$

Then,

$$S^t \cdot S = \left(\sum_{k=1}^{n} \sigma_k(\beta_i)\sigma_k(\beta_j)\right)_{i,j} = \left(\sum_{k=1}^{n} \sigma_k(\beta_i\beta_j)\right)_{i,j} = \left(T_{K/\mathbb{Q}}(\beta_i\beta_j)\right)_{i,j}.$$

By definition, we have that

$$d(\beta) = \det(S)^2. \tag{4}$$

Let $T = (a_{i,j}) \in \mathrm{GL}_n(\mathbb{Q})$ be the change of base matrix from β to β', where $\beta' = (\beta'_1, \ldots, \beta'_n)$. Then,

$$S' := (\sigma_i(\beta'_j))_{i,j} = S \cdot T.$$

By (4), we have

$$d(\beta') = \det(S')^2 = \det(ST)^2 = \det(T)^2 \cdot \det(S)^2 = \det(T)^2 \cdot d(\beta),$$

which proves (i).

Next, assume that $M = \langle \beta_1, \ldots, \beta_n \rangle_{\mathbb{Z}} = \langle \beta'_1, \ldots, \beta'_n \rangle_{\mathbb{Z}} = M'$. Then, the coefficients $a_{i,j}$ of the base change matrix T are integers. Moreover, the coefficients of T^{-1} are also integers. Therefore, $\det(T)^2 = 1$, so (ii) follows directly from (i).

By (i), it suffices to show (iii) for one particular $\mathbb{Q}$-basis of K. Let α be a primitive element of K. By Remark 2.13, $\beta := (1, \alpha, \ldots, \alpha^{n-1})$ is a $\mathbb{Q}$-basis of K. In the proof of Corollary 2.5, we have seen that $\alpha_i := \sigma_i(\alpha)$, $i = 1, \ldots, n$, are the n complex roots of the minimal polynomial of α. So $\alpha_i \neq \alpha_j$ for $i \neq j$. By (4), we get

$$d(\beta) = \left(\det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}\right)^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 \neq 0.$$

If $M \subset \mathcal{O}_K$, we have that the minimal polynomial of each β_i has integer coefficients. This implies that each $\beta_i\beta_j \in \mathbb{Q}$ is an algebraic integer. But then $d(\beta) = \det(T_{K/\mathbb{Q}}(\beta_i\beta_j))_{i,j} \in \mathbb{Q}$ is an algebraic integer, i.e. $d(\beta) \in \mathbb{Z}$, which completes the proof of this lemma.

□

Theorem 2.20

Let K be a number field of degree n. Then the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. This means there exist elements $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ such that every element $\alpha \in \mathcal{O}_K$ can be uniquely written as

$$\alpha = \sum_{i=1}^{n} a_i \alpha_i, \text{ with } a_i \in \mathbb{Z}.$$

Proof. Let $(\beta_1, \dots, \beta_n)$ be a $\mathbb{Q}$-basis of K. After replacing β_i by $m_i\beta_i$ for a suitable integer $m_i \in \mathbb{Z}$, we may assume that $\beta_i \in \mathcal{O}_K$ (see Remark 2.15). Then, $M := \langle \beta_1, \dots, \beta_n \rangle_{\mathbb{Z}} \subset \mathcal{O}_K$. Next, we show that

$$\mathcal{O}_K \subset d(M)^{-1} M. \tag{5}$$

Let $\alpha \in \mathcal{O}_K$. We can write α as a linear combination of the β_i's:

$$\alpha = a_1\beta_1 + \cdots + a_n\beta_n, \;\; a_i \in \mathbb{Q}.$$

To prove (5), we need to show that $d(M)a_i \in \mathbb{Z}$, for $i = 1, \dots, n$. Set

$$c_i := T_{K/\mathbb{Q}}(\alpha\beta_i) = \sum_{j=1}^{n} a_j T_{K/\mathbb{Q}}(\beta_i\beta_j),$$

for $i = 1, \dots, n$. In matrix notation, this means that

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = S \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \text{ with } S := (T_{K/\mathbb{Q}}(\beta_i\beta_j))_{i,j}. \tag{6}$$

By definition of the discriminant, we have that $d(M) = \det(S)$. By Cramer's rule, it follows that

$$S^{-1} = d(M)^{-1} \cdot S^*,$$

where S^* is the adjoint matrix of S. Multiplying this to (6), we obtain

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = d(M)^{-1} S^* \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}. \tag{7}$$

Since the trace of an integral element is integral, the coefficients c_i as well as the entries of the matrix S^* are integers. By (7), $a_i \in d(M)^{-1}\mathbb{Z}$, which proves (5). With (5), we now know that $\mathcal{O}_K$ is contained in the lattice $d(M)^{-1}M$. This means that $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module of rank n. This implies that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $m \leq n$. (For a proof, see e.g. [Art11, Theorem 14.4.11]). But by our choice of M, we also have that $M \subset \mathcal{O}_K$. Using the same result again yields $m = n$, which proves the theorem. □

Definition 2.21

A tuple $(\alpha_1, \ldots, \alpha_n)$ as in Theorem 2.20 is called an *integral basis* of K.

Example 2.22

Let $D \in \mathbb{Z}$ be a nonzero, squarefree integer and let $K := \mathbb{Q}[\sqrt{D}]$. In Example 2.17, we have seen that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}], & D \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{D}], & D \equiv 2, 3 \bmod 4 \end{cases}$$

This yields the following result:

(i) If $D \equiv 1 \bmod 4$, then $(1, \frac{1+\sqrt{D}}{2})$ is an integral basis of K.

(ii) If $D \equiv 2, 3 \bmod 4$, then $(1, \sqrt{D})$ is an integral basis of K.

Since $\mathcal{O}_K \subset K$ is a lattice, we can also define:

Definition 2.23

Let K be a number field. The *discriminant* of K is the nonzero integer

$$d_K := d(\mathcal{O}_K).$$

Example 2.24

Let $D \in \mathbb{Z}$ be squarefree and let $K := \mathbb{Q}[\sqrt{D}]$. Then, the subring $Z[\sqrt{D}] = \langle 1, \sqrt{D} \rangle_{\mathbb{Z}} \subset \mathcal{O}_K$ is a lattice contained in $\mathcal{O}_K$.

If $D \equiv 1 \bmod 4$, $\mathcal{O}_K = \mathbb{Z}[\theta] = \langle 1, \theta \rangle_{\mathbb{Z}}$, where $\theta := \frac{1+\sqrt{D}}{2}$. In this case,

$$d(\mathbb{Z}[\theta]) = \det \begin{pmatrix} T_{K/\mathbb{Q}}(1) & T_{K/\mathbb{Q}}(\theta) \\ T_{K/\mathbb{Q}}(\theta) & T_{K/\mathbb{Q}}(\theta^2) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+D}{2} \end{pmatrix} = D.$$

If $D \equiv 2, 3 \bmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}] = \langle 1, \sqrt{D} \rangle_{\mathbb{Z}}$. In this case,

$$d(\mathbb{Z}[\sqrt{D}]) = \det \begin{pmatrix} T_{K/\mathbb{Q}}(1) & T_{K/\mathbb{Q}}(\sqrt{D}) \\ T_{K/\mathbb{Q}}(\sqrt{D}) & T_{K/\mathbb{Q}}(D) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D.$$

3 Dirichlet's Unit Theorem

In this Chapter, we study the unit group of a number field K. The goal for this Chapter is to prove Dirichlet's Unit Theorem and to look at some examples.

Definition 3.1

Let K be a number field. The *unit group* $\mathcal{O}_K^\times$ is defined as:

$$\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \setminus \{0\} | \alpha^{-1} \in \mathcal{O}_K\}.$$

Lemma 3.2

We have $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K | N_{K/\mathbb{Q}}(\alpha) = \pm 1\}$.

Proof. Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the distinct embeddings of K into $\mathbb{C}$. Without loss of generality, we may assume that $K \subset \mathbb{C}$ and that σ_1 is the identity on K. By Lemma 2.9, we have that

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{Z} \tag{8}$$

for all $\alpha \in \mathcal{O}_K$.

Now let $\alpha \in \mathcal{O}_K^\times$ be a unit. Using the multiplicativity of the norm, we get that

$$1 = N_{K/\mathbb{Q}}(1) = N_{K/\mathbb{Q}}(\alpha) \cdot N_{K/\mathbb{Q}}(\alpha^{-1}),$$

where both factors on the right hand side are integers. It follows that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Conversely, assume that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Using (8) again shows that

$$\alpha^{-1} = \sigma_1(\alpha^{-1}) = \pm \sigma_2(\alpha) \dots \sigma_n(\alpha)$$

is a product of algebraic integers. We conclude that each $\sigma_i(\alpha) \in \mathcal{O}_L$ for the number field $L := \mathbb{Q}[\sigma_1(\alpha), \dots, \sigma_n(\alpha)]$ and therefore $\alpha^{-1} \in \mathcal{O}_L$. It follows that $\alpha^{-1} \in \mathcal{O}_L \cap K = \mathcal{O}_K$, so $\alpha \in \mathcal{O}_K^\times$ is a unit. □

Definition 3.3

Let K be a number field of degree n. Then we define the set of *roots of unity* contained in K as

$$\mu(K) := \{\zeta \in K | \exists k \in \mathbb{N} : \zeta^k = 1\}.$$

Remark 3.4

Clearly, $\mu(K)$ is a subgroup of $K^\times$. Moreover, we note that $\mu(K) \subset \mathcal{O}_K$, since for every root of unity $\zeta \in \mu(K)$, we have that $\zeta^k - 1 = 0$ for some $k \in \mathbb{N}$. It follows that $\mu(K) \subset \mathcal{O}_K^\times$ is a subgroup of the unit group. In fact,

$$\mu(K) = (\mathcal{O}_K^\times)_{tor}$$

is the torsion subgroup of $\mathcal{O}_K^\times$, i.e. the subgroup consisting of all elements of $\mathcal{O}_K^\times$ that have finite order. Therefore, the quotient group

$$E_K := \mathcal{O}_K^\times / \mu(K)$$

is torsion free, i.e. it has no element of finite order except the identity.

Theorem 3.5 (Dirichlet's Unit Theorem)

Let K be a number field of type (r, s). Then

(i) The group $\mu(K)$ is finite and cyclic.

(ii) $E_K = \mathcal{O}_K^\times / \mu(K)$ is a free abelian group of rank $r + s - 1$.

We can rephrase the statement of this theorem in the following way: Let $t := r + s - 1$. Then there exist units $\epsilon_1, \dots, \epsilon_t \in \mathcal{O}_K^\times$ such that every unit $\alpha \in \mathcal{O}_K^\times$ has a unique representation of the form

$$\alpha = \zeta \cdot \epsilon_1^{k_1} \dots \epsilon_t^{k_t},$$

with $\zeta \in \mu(K)$ and $k_i \in \mathbb{Z}$.

Definition 3.6

The tuple $(\epsilon_1, \ldots, \epsilon_t)$ from Theorem 3.5 is called *fundamental system of units.*

Before we can prove Dirichlet's Unit Theorem, we have to prove some Lemmas first. Also, we need the following two definitions:

Definition 3.7

Let V be a real vector space of dimension n. A *lattice* in V is a subgroup $\Gamma \subset V$ of the form

$$\Gamma = \langle v_1, \ldots, v_m \rangle_{\mathbb{Z}},$$

with m linearly independent vectors $v_1, \ldots, v_m$. The tuple $(v_1, \ldots, v_m)$ is called a *basis* of the lattice Γ. We set

$$P := \{x_1 v_1 + \cdots + x_m v_m | x_i \in \mathbb{R}, 0 \leq x_i \leq 1\} \subset V.$$

P is called the *fundamental domain* of Γ with respect to the basis $(v_1, \ldots, v_m)$.
If $n = m$, the lattice Γ is called *complete.*

Definition 3.8

Let (V, d) be a metric space. A subset $S \subset V$ is called *discrete* if for all $x \in S$ there exists a $\delta > 0$ such that $d(x, y) > \delta$ for all $y \in S \setminus \{x\}$.

Proposition 3.9

Let $\Gamma \subset V$ be a subgroup of a real vector space of dimension n. Then:

(i) Γ is a lattice if and only if it is a discrete subset of V.

(ii) Let Γ be a lattice with basis $(v_1, \ldots, v_m)$. Let P be the fundamental domain of Γ with respect to this basis. Then Γ is a complete lattice if and only if V is the disjoint union of the translates $P + \gamma$, i.e.

$$V = \bigcup_{\gamma \in \Gamma} P + \gamma$$

Proof. See e.g. [NS13, Theorem I.4.2 and I.4.3]. □

Remark 3.10

Let $(V, \langle \cdot, \cdot \rangle)$ be an euclidean vector space of dimension n. Let $v_1, \ldots, v_n \in V$ and $\Gamma := \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}} \subset V$. Then, we let

$$A := \left(\langle v_i, v_j \rangle\right)_{i,j}.$$

A is called the *Gram matrix* of $(v_1, \ldots, v_n)$. By definition, Γ is a complete lattice if and only if $n = m$. By [Fis13, Theorem 5.4.10], this is the case if and only if $\det(A) > 0$. Moreover, if $\det(A) > 0$, then

$$\operatorname{vol}(P) = \sqrt{\det(A)}$$

is the volume of the fundamental domain P with respect to the basis $(v_1, \ldots, v_n)$. This only depends on the lattice Γ, not on the basis $(v_1, \ldots, v_n)$. To see that, let $(v_1', \ldots, v_n')$ be another basis of Γ. The base change matrix T is an element of $\mathrm{GL}_n(\mathbb{Z})$, so we have that

$$A' := \left(\langle v_i', v_j' \rangle\right)_{i,j} = T^t \cdot A \cdot T$$

and therefore

$$\sqrt{\det(A')} = \sqrt{(\det(T))^2}\sqrt{\det(A)} = \sqrt{\det(A)}.$$

Definition 3.11

Let $(V, \langle \cdot, \cdot \rangle)$ be an euclidean vector space of dimension n and let $\Gamma \subset V$ be a complete lattice. Let $(v_1, \dots, v_n)$ be a basis for Γ with corresponding fundamental domain P. Then

$$\mathrm{vol}(\Gamma) := \mathrm{vol}(P) > 0$$

is called the *covolume* of the lattice Γ. Note that this is well defined by the previous Remark.

Definition 3.12

Let K be a number field of degree n. Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$. Let (r, s) be the type of K. As in Remark 2.6 ,we may assume that the first r embeddings $\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$ are real embeddings and that $\{\sigma_{r+2i-1}, \sigma_{r+2i}\}, i = 1, \dots, s$ are pairs of complex conjugate embeddings.

In the situation above, the real vector space

$$K_{\mathbb{R}} := \{(z_k) \in \mathbb{C}^n | z_1, \dots, z_r \in \mathbb{R}, \bar{z}_{r+2i-1} = z_{r+2i}, i = 1, \dots, s\}$$

is called the *Minkowski space* of K.

Remark 3.13

We note that $K_{\mathbb{R}}$ is a real vector space of dimension $r + 2s = n$, but it is not a complex vector space. There is a $\mathbb{Q}$- linear embedding

$$j : K \hookrightarrow K_{\mathbb{R}}, \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_n(\alpha)).$$

The scalar product $\langle \cdot, \cdot \rangle$ on $K_{\mathbb{R}}$ is defined as the restriction of the canonical hermitian product on $\mathbb{C}^n$, i.e.

$$\langle z, w \rangle := \sum_{i=1}^{n} \bar{z}_i w_i = \sum_{i=1}^{r} \ z_i w_i + \sum_{i=1}^{s} 2\mathcal{R}(z_{r+2i} \bar{w}_{r+2i}).$$

In particular, $\langle \cdot, \cdot \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ is indeed a symmetric and positive definite $\mathbb{R}$-bilinear form, i.e. $(K_{\mathbb{R}}, \langle \cdot, \cdot \rangle)$ is an euclidean vector space.

Lemma 3.14

Let $\beta = (\beta_1, \ldots, \beta_n)$ be a $\mathbb{Q}$-basis on K and let $M := \langle \beta_1, \ldots, \beta_n \rangle$ be the lattice spanned by β. Then, $(j(\beta_1), \ldots, j(\beta_n))$ is a $\mathbb{R}$-basis of $K_{\mathbb{R}}$. Therefore, $j(M) \subset K_{\mathbb{R}}$ is a complete lattice. Moreover,

$$\mathrm{vol}(j(M)) = \sqrt{|d(M)|}$$

Proof. Let

$$A := (\langle j(\beta_i), j(\beta_j) \rangle)_{i,j}$$

be the Gram matrix of $j(\beta_1), \ldots, j(\beta_n)$. By Remark 3.10, we have to show that $\det(A) > 0$ and that $\det(A) = |d(M)|$ to finish the proof of the lemma. By Lemma 2.19 (iii), we know that $d(M) \neq 0$, so we only need to show that $\det(A) = |d(M)|$. By definition, we have that

$$\langle j(\beta_i), j(\beta_j) \rangle = \sum_{k=1}^{n} \overline{\sigma_k(\beta_i)} \sigma_k(\beta_j)$$

for all i, j. In matrix notation, this means that

$$A = \bar{S}^t S, \text{ where } S := (\sigma_i(\beta_j))_{i,j}$$

Using (4), we conclude that

$$\det(A) = |\det(S)|^2 = |d(M)|,$$

which completes the proof. □

Corollary 3.15

The subgroup $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ is a complete lattice with covolume $\mathrm{vol}(j(\mathcal{O}_K)) = \sqrt{|d_K|}$.

Next, we look at two examples of the Minkowski space of quadratic number fields:

Example 3.16

Let $D > 0$ be a squarefree integer and let $K := \mathbb{Q}[\sqrt{-D}]$ denote the corresponding imaginary quadratic number field. The two complex conjugate embeddings $\sigma_1, \sigma_2 : K \hookrightarrow K$ are given by

$$\sigma_1(\sqrt{-D}) = i\sqrt{D}, \quad \sigma_2(\sqrt{-D}) = -i\sqrt{D}$$

The Minkowski space of K is the real vector space

$$K_{\mathbb{R}} = \{(z_1, z_2) \in \mathbb{C}^2 | \bar{z}_1 = z_2\}$$

with the scalar product

$$\langle z, w \rangle = \bar{z}_1 w_1 + \bar{z}_2 w_2 = \bar{z}_1 w_1 + z_1 \bar{w}_1 = 2\mathcal{R}(\bar{z}_1 w_1),$$

so the *Minkowski norm* is given by

$$\|(z_1, z_2)\| = \sqrt{2}|z_1|$$

If we identify $K_{\mathbb{R}}$ with $\mathbb{C}$ (considered as a real vector space) via the projection:

$$K_{\mathbb{R}} \cong \mathbb{C}, \quad (z_1, z_2) \mapsto z_1,$$

the embedding $j : K \to K_{\mathbb{R}}$ is identified with the embedding $\sigma_1 : K \hookrightarrow \mathbb{C}$.

Example 3.17

Let $D > 0$ be a squarefree integer and let $K := \mathbb{Q}[\sqrt{D}]$ denote the corresponding real quadratic number field. Let $\tau : K \to K, \alpha \mapsto \alpha'$ be the unique nontrivial automorphism of K, given by $\tau(\sqrt{D}) = -\sqrt{D}$. The Minkowski space of K is $K_{\mathbb{R}} = \mathbb{R}^2$ and the embedding of K into $K_{\mathbb{R}}$ is given by

$$j : K \hookrightarrow K_{\mathbb{R}} = \mathbb{R}^2, \quad \alpha \mapsto (\alpha, \alpha').$$

The Minkowski norm on $K_{\mathbb{R}} = \mathbb{R}^2$ is the euclidean norm.

Proof of Dirichlet's Unit Theorem.

Let K be a number field of degree n and type (r, s). Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$. Again, we assume that $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ are real embeddings and that $\{\sigma_{r+2i-1}, \sigma_{r+2i}\}, i = 1, \ldots, s$ are pairs of complex conjugate embeddings. Let

$$K_{\mathbb{R}} = \{(z_k) \in \mathbb{C}^n | z_1, \ldots, z_r \in \mathbb{R}, \bar{z}_{r+2i-1} = z_{r+2i}, i = 1, \ldots, s\}$$

be the Minkowski space of K. We let

$$j : K \hookrightarrow K_{\mathbb{R}}, \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$$

be the $\mathbb{Q}$-linear embedding from K into $K_{\mathbb{R}}$ as in Remark 3.13. From Corollary 3.15, we know that $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ is a complete lattice with covolume $\operatorname{vol}(j(\mathcal{O}_K)) = \sqrt{|d_K|}$. We define

$$\begin{aligned} K_{\mathbb{R}}^{\times} &:= \{(z_i) \in K_{\mathbb{R}} | z_i \neq 0 \ \forall i = 1, \ldots, n\}, \\ S &:= \{(z_i) \in K_{\mathbb{R}}^{\times} | \prod_{i=1}^{n} |z_i| = 1\}. \end{aligned}$$

We note that $K_{\mathbb{R}}^{\times}$ is an abelian group with respect to componentwise multiplication and $S \subset K_{\mathbb{R}}^{\times}$ is a subgroup. We also have that the restriction of j to $K^{\times}$ is an injective group homomorphism $j : K^{\times} \hookrightarrow K_{\mathbb{R}}^{\times}$. From Lemma 3.2, it follows directly that

$$j(\mathcal{O}_K^{\times}) = j(\mathcal{O}_K) \cap S.$$

Using (8), we see that for $\alpha \in K$, $j(\alpha) \in S$ if and only if $|N_{K/\mathbb{Q}}(\alpha)| = 1$. Next, we define the *logarithmic space*

$$L := \{(x_i) \in \mathbb{R}^n | x_{r+2i-1} = x_{r+2i} \text{ for } i = 1, \ldots, s\}$$

and the *logarithmic map*

$$l : K_{\mathbb{R}}^{\times} \to L, \quad (z_i) \mapsto (\log(|z_i|)).$$

We note that L is a real vector space of dimension $r+s$ and that l is a group homomorphism, which turns multiplication into addition. If we also define

$$H := \{(x_i) \in L | \sum_{i=1}^{n} x_i = 0\},$$

we see that the image of $S \subset K_{\mathbb{R}}^{\times}$ under the logarithmic map l is a subset of H. We note that H is a real vector space of dimension $r + s - 1$.

The following commutative diagram of abelian groups shows the introduced notation:

$$\begin{tikzcd}
\mathcal{O}_K^{\times} \arrow[r] \arrow[d] & S \arrow[r] \arrow[d] & H \arrow[d] \\
K^{\times} \arrow[r, "j"] & K_{\mathbb{R}}^{\times} \arrow[r, "l"] & L
\end{tikzcd}$$

The three vertical maps in this diagram are inclusion maps. For the proof of Dirichlet's Unit Theorem, we are mostly interested in the maps

$$\lambda := l \circ j|_{\mathcal{O}_K^{\times}} : \mathcal{O}_K^{\times} \to H \text{ and } \ l|_S : S \to H.$$

We note that λ is a group homomorphism and that $l|_S$ is a surjective map, since the logarithm $\log : \mathbb{R}_{>0} \to \mathbb{R}$ is surjective.

The following Lemma proves part (i) of Dirichlet's Unit Theorem:

Lemma 3.18

In the situation above, $\ker(\lambda) = \mu(K)$ and this group is finite and cyclic.

Proof. Let $\zeta \in \mu(K)$ be a root of unity. Then, $\zeta_i := \sigma_i(\zeta) \in \mathbb{C}$ is also a root of unity, which means that $|\zeta_i| = 1$ for $i = 1, \ldots, n$. We get that $\lambda(\zeta) = (\log(|\zeta_i|)) = 0$, so $\zeta \in \ker(\lambda)$.

Conversely, let $\alpha \in \ker(\lambda)$, i.e. $|\sigma_i(\alpha)| = 1$ for all $i = 1, \dots, n$. This implies that $j(\ker(\lambda))$ is contained in the compact subgroup

$$(S^1)^n := \{(z_i) \in K_{\mathbb{R}} \big| |z_i| = 1 \text{ for } i = 1, \dots, n\}.$$

Since $j(\ker(\lambda))$ is also a subset of the discrete set $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$, it follows that $\ker(\lambda)$ is finite. This implies that every element of $\ker(\lambda)$ has finite order, so by definition, we have that $\ker(\lambda) \subset \mu(K)$. So we did prove that $\ker(\lambda) = \mu(K)$ and that this group is finite. To see that it is a cyclic group, we can use the fact that every finite subgroup of $K^\times$ is cyclic (for a proof, see e.g. [Wei95, Chapter 1, Lemma 1]). □

Next, we define

$$\Lambda := \lambda(\mathcal{O}_K^\times) \subset H.$$

Λ is a subgroup of H. By Lemma 3.18 and the first isomorphism theorem, Λ is isomorphic to the quotient group $E_K := \mathcal{O}_K^\times / \mu(K)$. To prove part (ii) of Dirichlet's Unit Theorem, we will show that Λ is a free abelian group of rank $r + s - 1$. To see that, we will prove that Λ is a complete lattice in the real vector space H. By construction, $\dim_{\mathbb{R}} H = r + s - 1$, which then implies that $\Lambda \cong E_K$ is a free abelian group of rank $r + s - 1$.

Lemma 3.19

$\Lambda \subset H$ is a discrete subgroup.

Proof. To prove this Lemma, we see Λ as a subgroup of the vector space L containing H. Then, the set

$$U := \{(x_i) \in L \big| |x_i| \leq 1 \text{ for } i = 1, \dots, n\}$$

is a neighborhood of $0 \in L$. The preimage of U under the logarithmic map l is given by

$$W := l^{-1}(U) = \{(z_i) \in K_{\mathbb{R}} \big| e^{-1} \leq |z_1| \leq e\}.$$

Clearly, W is a compact subset of $K_{\mathbb{R}}$. We have seen that $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ is a lattice. By Proposition 3.9(i), this implies that $j(\mathcal{O}_K)$ is a discrete subset. Therefore, $W \cap j(\mathcal{O}_K)$ is a finite set. Then, $U \cap \Lambda$ is a finite set too. We conclude that $\Lambda \subset L$ is a discrete subgroup. □

Remark 3.20

We note that by Proposition 3.9 (i), the previous lemma implies that $\Lambda \subset H$ is a lattice. Therefore, $E_K = \mathcal{O}_K/\mu(K)$ is a free abelian group of rank $\leq r+s-1$. We still have to show that this lattice is complete. For this part of the proof, we will need some theory on ideals in $\mathcal{O}_K$ and the so called class group of a number field, which we will provide without proof. A good reference for this theory is [NS13, Chapter I].

Lemma 3.21

(i) $\mathcal{O}_K$ is a noetherian ring, i.e. for every ideal $\mathfrak{a} \subset \mathcal{O}_K$ there exist $\alpha_1, \dots, \alpha_n \in \mathfrak{a}$ such that $\mathfrak{a} = (\alpha_1, \dots, \alpha_n)$.

(ii) For any ideal $\mathfrak{a} \subset \mathcal{O}_K$, the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite.

Proof. See [NS13, Theorem I.3.1]. □

With this Lemma, the following is well defined:

Definition 3.22

Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal. The *norm* of $\mathfrak{a}$ is defined as

$$N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}| \in \mathbb{N}.$$

The following Lemma provides a useful way to determine the norm of a principal ideal in $\mathcal{O}_K$:

Lemma 3.23

Let $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. Then,

$$N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Proof. See [NS13, Chapter I.6]. □

Definition 3.24

A *fractional ideal* of K is a finitely generated $\mathcal{O}_K$-submodule $\mathfrak{a} \subset K$, with $\mathfrak{a} \neq \{0\}$, i.e.

$$\mathfrak{a} = (\alpha_1, \dots, \alpha_m) = \left\{ \sum_{i=1}^{m} \alpha_i \beta_i \middle| \beta_i \in \mathcal{O}_K \right\}$$

for $\alpha_1, \dots, \alpha_m \in K^\times$.

Lemma 3.25

Let $\mathfrak{a} \subset K$ be a fractional ideal. Then

$$\mathfrak{a}^{-1} := \{\beta \in K | \beta \cdot \mathfrak{a} \subset \mathcal{O}_K\}$$

is also a fractional ideal and $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathcal{O}_K$.

Proof. See [NS13, Lemma I.3.5]. □

Definition 3.26

Let J_K be the set of fractional ideals of K. The previous Lemma shows that J_K is an abelian group with respect to multiplication. J_K is called the *ideal group* of K. If we define P_K as the set of all principal fractional ideals, $P_K \subset J_K$ is a subgroup.
The *ideal class group* of K is defined as

$$Cl_K := J_K / P_K$$

Theorem 3.27

Let K be a number field of type (r, s) and let

$$C_K := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

Then, every ideal class in Cl_K is represented by an integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ with $N(\mathfrak{a}) \leq C_K$ and the class group Cl_K is finite.

Proof. See e.g. [NS13, Lemma I.6.2 and Theorem I.6.3]. □

Definition 3.28

The order $h_K := |Cl_K|$ is called the *class number* of K.

Theorem 3.29 (**Minkowski's Theorem**)

Let $(V, \langle \cdot, \cdot, \rangle)$ be an euclidean vector space of dimension n and $\Gamma \subset V$ be a complete lattice. Let $X \subset V$ be a nonempty set with

(i) X is symmetric, i.e. $-X = X$,

(ii) X is convex,

(iii) $\mathrm{vol}(X) > 2^n \ \mathrm{vol}(\Gamma)$.

Then, $X \cap \Gamma$ contains a nonzero vector.

Proof. See for example [NS13, Theorem I.4.4]. □

Lemma 3.30

Let K be a number field and $C > 0$ be a constant. Then, there exist only finitely many ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $N((\mathfrak{a})) \leq C$.

Proof. See [NS13, Lemma I.7.2]. □

We will use these results to finish the proof of Dirichlet's Unit Theorem:

Lemma 3.31

Let $c_1, \ldots, c_n > 0$ be positive constants such that

$$C := \prod_{i=1}^{n} c_i > C_K = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

and let $S = \{(y_i) \in K_{\mathbb{R}}^{\times} \,|\, \prod_{i=1}^{n} |y_i| = 1\}$. Then, for all $y = (y_i) \in S$, there exists an element $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that

$$|\sigma_i(\alpha)| < |y_i| c_i \text{ for } i = 1, \ldots, n.$$

This means that

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| < C.$$

Proof. Let $X := \{(z_i) \in K_\mathbb{R} \big| |z_i| < c_i \text{ for } i = 1, \ldots, n\}$. This is a convex and symmetric subset of $K_\mathbb{R}$ and by [NS13, Lemma III.2.15], we have that

$$\mathrm{vol}(X) = 2^{r+s}\pi^s C > 2^n \sqrt{|d_K|} = 2^n \mathrm{vol}(j(\mathcal{O}_K)).$$

This means we can apply Minkowski's Theorem 3.29 to X.

Also, for any $(y_i) \in S$, we can consider the set

$$y \cdot X = \{(z_i) \in K_\mathbb{R} \big| |z_i| < |y_i| c_i \text{ for } i = 1, \ldots, n\}.$$

Since $\prod_{i=1}^{n} |y_i| c_i = C$, we have that $\mathrm{vol}(y \cdot X) = \mathrm{vol}(X)$. By [NS13, Theorem I.5.3], there exists $\alpha \in \mathcal{O}_K \backslash \{0\}$ such that $j(\alpha) \in y \cdot X$. This means that $|\sigma_i(\alpha)| \leq |y_i| c_i$ for all $i = 1, \ldots, n$, which completes the proof of this lemma.

□

We note that by Lemma 3.30, there are finitely many ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $N(\mathfrak{a}) < C$. Let $(\alpha_1), \ldots, (\alpha_N)$ be all nonzero principal ideals with this property. By Lemma 3.23, $\alpha_j \neq 0$ and $|N_{K/\mathbb{Q}}(\alpha_j)| < C$ for $j = 1, \ldots, N$. Also, we note that for any $\alpha \in \mathcal{O}_K \setminus \{0\}$, there exists $j \in \{1, \ldots, N\}$ such that $(\alpha) = (\alpha_j)$.

Lemma 3.32

In the setting from above, we let

$$T := S \cap \left(\bigcup_{j=1}^{N} j(\alpha_j^{-1}) \cdot X \right).$$

Then, T is a bounded subset of S with

$$S = \bigcup_{\epsilon \in \mathcal{O}_K^\times} j(\epsilon) \cdot T \tag{9}$$

Proof. T is bounded as a finite union of bounded subsets of S. By definition, we also have that $j(\epsilon) \in S$ for all $\epsilon \in \mathcal{O}_K^\times$, which implies that

$$\bigcup_{\epsilon \in \mathcal{O}_K^\times} j(\epsilon) \cdot T \subset S.$$

To show the other inclusion, we let $y = (y_i) \in S$ be arbitrary. By Lemma 3.31, there exists an element $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $|\sigma_i(\alpha)| < |y_i| c_i$ for $i = 1, \ldots, n$, i.e.

$$j(\alpha) \in y \cdot X. \tag{10}$$

This means that $|N_{K/\mathbb{Q}}(\alpha)| < C$. Therefore, there exists an index $j \in \{1, \ldots, N\}$ such that $(\alpha) = (\alpha_j)$. This implies that

$$\alpha_j = \epsilon \alpha \tag{11}$$

for some $\epsilon \in \mathcal{O}_K^\times$. By (10), there exists $x \in X$ with $j(\alpha) = y \cdot x$. Applying (11) yields

$$y = j(\alpha^{-1}) \cdot x = j(\epsilon \alpha_j^{-1}) \cdot x = j(\epsilon) \cdot j(\alpha_j^{-1}) \cdot x \in j(\epsilon) \cdot T,$$

which completes the proof of this lemma.

□

With these results, we can now finish the proof of Dirichlet's Unit Theorem:

In Remark 3.20, we have already seen that $\Lambda \subset H$ is a lattice. Assume that Λ is not a complete lattice, i.e. $\Lambda \subset H'$ for a proper subspace $H' \subsetneq H$. Let

$$T = S \cap \left(\bigcup_{j=1}^{N} j(\alpha_j^{-1}) \cdot X \right)$$

as in Lemma 3.32. Since T is bounded, the image of T under the logarithmic map l is a bounded subset of H. We have seen that the the map $l|_S : S \to H$ is surjective. Then, (9) implies that

$$H = l(S) = \left(\bigcup_{\gamma \in \Lambda} (\gamma + l(T)) \right). \tag{12}$$

Let $v \in (H')^{\perp}$ be a vector in H which is orthogonal to H' with $\|v\| > \|w\|$ for all $w \in l(T)$. This implies that

$$\|v + \gamma\| \geq \|v\| > \|w\|$$

for all $\gamma \in \Lambda$ and $w \in l(T)$, since $v \perp \gamma$ by assumption. Therefore, $v + \gamma \notin l(T)$ for all $\gamma \in \Lambda$, which is a contradiction to (12). Therefore, $\Lambda \subset H$ is a complete lattice, which completes the proof of Dirichlet's Unit Theorem. □

Remark 3.33

We note that the fundamental system of units $(\epsilon_1, \ldots, \epsilon_t)$ in the statement of Dirichlet's Unit Theorem is not unique. For example, we can replace each ϵ_i by $\pm\epsilon_i$ or $\pm\epsilon_i^{-1}$ and still get a system of fundamental units.

If $t = 1$, i.e. if we only have one fundamental unit, we can replace it by one of these four choices to get $\epsilon_1 > 1$.

Example 3.34

Let $D > 0$ be a squarefree integer with $D \equiv 2, 3 \bmod 4$ and let $K := \mathbb{Q}[\sqrt{D}]$ denote the corresponding real quadratic number field. In Example 2.17, we have seen that $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. For each $\alpha = x + y\sqrt{D} \in \mathcal{O}_K$, $N_{K/\mathbb{Q}}(\alpha) = x^2 - Dy^2$. This means that the units in $\mathcal{O}_K$ correspond to the solutions of

$$x^2 - Dy^2 = \pm 1 \text{ for } x, y \in \mathbb{Z} \tag{13}$$

Equation (13) is called *Pell's equation.* By Dirichlet's Unit Theorem, there exists an element $\epsilon_1 \in \mathcal{O}_K^{\times}$ such that every other unit $\epsilon \in \mathcal{O}_K^{\times}$ can be uniquely written as $\epsilon = \pm\epsilon_i^k$ for some $k \in \mathbb{Z}$. This fundamental unit is of the form $\epsilon_1 = x_1 + y_1\sqrt{D}$, where (x_1, y_1) is a solution to Pell's equation.

4 Examples for cubic number fields

In this Chapter, we will look at the special case of cubic number fields K, i.e. number fields of degree 3.

We look at the relation between the discriminant of K and the unit group $\mathcal{O}_K$. By definition, we have that the discriminant of K is given by the discriminant of the lattice $\mathcal{O}_K$. We can use SageMath to find the discriminant of a given cubic number field (for the code, see the Appendix).

Example 4.1

Let $f_1 = x^3 - 2, f_2 = x^3 - 3, f_3 = x^3 - 5 \in \mathbb{Q}[x]$. Each f_i has exactly one real root α_i. Let $K_i = \mathbb{Q}(\alpha_i)$ be the smallest field extension of $\mathbb{Q}$ containing α_i, for $i = 1, 2, 3$.

Using the code given in Appendix Code 1, Code 2 and Code 3, we see that

$$\begin{aligned} d(K_1) &= -108 \\ d(K_2) &= -243 \\ d(K_3) &= -675 \end{aligned}$$

Also, we see that each of these number fields is of type $(1, 1)$. By Dirchlet's Unit Theorem, the fundamental system of units consists of one element in each case. In Remark 3.33, we have seen that we can choose this fundamental unit to be bigger than 1.

If we estimate the fundamental unit ϵ_i for each K_i using SageMath, we get the following results:

$$\begin{aligned} \epsilon_1 &\approx 3.84732 \\ \epsilon_2 &\approx 12.48692 \\ \epsilon_3 &\approx 122.97567 \end{aligned}$$

We note that for a bigger absolute value of the discriminant $|d(K_i)|$, we get a bigger fundamental unit ϵ_i.

Example 4.2

We look at another set of polynomials f_i, for $i = 4, 5, 6, 7$, defined by:

$$f_4 = x^3 - 6x^2 + 11x - 5$$

$$f_5 = x^3 - 6x^2 + 11x - 4$$

$$f_6 = x^3 - 6x^2 + 11x - 3$$

$$f_7 = x^3 - 6x^2 + 11x - 2$$

As in the Example before, each f_i has exactly one real root α_i. Again, we let $K_i = \mathbb{Q}(\alpha_i)$. Using the code given in Appendix Code 4 - Code 7, we see that

$$\begin{aligned} d(K_4) &= -23 \\ d(K_5) &= -104 \\ d(K_6) &= -239 \\ d(K_7) &= -107 \end{aligned}$$

Here, the fundamental units ϵ_i of K_i are

$$\begin{aligned} \epsilon_4 &\approx 1.32472 \\ \epsilon_5 &\approx 4.83598 \\ \epsilon_6 &\approx 8.13798 \\ \epsilon_7 &\approx 3.51155 \end{aligned}$$

We still note a general trend that the values of the fundamental units seem to increase with large discriminants. However, this example tells us that the absolute value of the ϵ_i is not a strictly increasing function of $|d(K_i)|$, since $|d(K_7)| > |d(K_5)|$, but $\epsilon_7 < \epsilon_5$.

Example 4.3

Let $f_8 = x^3 + x^2 - 1$. f_8 has a unique real root α_8. Let $K_8 = \mathbb{Q}(\alpha_8)$.

Using Code 8 from the Appendix, we see that $d(K_8) = -23$ and that the fundamental unit of K_8 is $\epsilon_8 \approx 1.32472$.

Let $f_4 = x^3 - 6x^2 + 11x - 5$ as in Example 4.2. We have seen that $d(K_4) = -23$ and $\epsilon_4 \approx 1.32472$.

So we have two different cubic field extensions with the same discriminant. Here, the fundamental units of these fields are equal, too. This indicates that the trend we noticed in the previous two examples might be true.

Remark 4.4

Using the observations from the previous three examples, we suggest that there is a relation between the absolute value of the discriminant of a cubic number field K_i of type $(1, 1)$ and the fundamental unit ϵ_i. Based on these examples, we try to find a lower bound for ϵ_i using $|d(K_i)|$.

Our first approach is to look at the fraction $q_i := \frac{\epsilon_i}{|d(K_i)|}$. We get the following results for our previous examples:

$$\begin{aligned}
q_1 &= \frac{3.84732}{108} = 0.03562\\
q_2 &= \frac{12.48692}{243} = 0.05139\\
q_3 &= \frac{122.94567}{675} = 0.18214\\
q_4 &= \frac{1.32472}{23} = 0.05760\\
q_5 &= \frac{4.83598}{104} = 0.04650\\
q_6 &= \frac{8.13798}{239} = 0.03405\\
q_7 &= \frac{3.51155}{107} = 0.03282\\
q_8 &= \frac{1.32472}{23} = 0.05760
\end{aligned}$$

We note that each quotient q_i is less than 1. In Example 3.34, we have see that the fundamental unit in the quadratic case can be expressed in terms of $\sqrt{d}$. For that reason, it is a natural choice to compare the fundamental unit in the cubic case to $\sqrt[3]{d}$. So to get a better lower bound, we try to use $\sqrt[3]{|d(K_i)|}$ instead of $|d(K_i)|$. i.e. we define $p_i := \frac{\epsilon_i}{\sqrt[3]{|d(K_i)|}}$ and calculate theses quotients similar to before. Then, we see that

$$\begin{aligned}
p_1 &= \frac{3.84732}{\sqrt[3]{108}} = 0.80789 \\
p_2 &= \frac{12.48692}{\sqrt[3]{243}} = 2.00103 \\
p_3 &= \frac{122.94567}{\sqrt[3]{675}} = 14.01561 \\
p_4 &= \frac{1.32472}{\sqrt[3]{23}} = 0.46582 \\
p_5 &= \frac{4.83598}{\sqrt[3]{104}} = 1.02835 \\
p_6 &= \frac{8.13798}{\sqrt[3]{239}} = 1.31135 \\
p_7 &= \frac{3.51155}{\sqrt[3]{107}} = 0.73967 \\
p_8 &= \frac{1.32472}{\sqrt[3]{23}} = 0.46582
\end{aligned}$$

We see that these fractions are closer to 1 now, but we also notice that we have some $p_i's$, e.g. p_4 and p_8 that still seem to be too small. We also note that these two correspond to fields with a small discriminant $|d(K_i)| = 23$, so we suggest that the inequality we are looking for does not holds for fields with a small discriminant.

Next, we try to only look at fields with a large discriminant. We can therefore adjust the inequality to be

$$\epsilon_i > a\sqrt[3]{|d(K_i)| - 27} \geq 1$$

We get a system of 6 inequalities, using the values we found in the previous three examples, for $i \in \{1,2,3,5,6,7\}$. Solving these inequalities yields:

$$\begin{aligned}
3.84732 > a \cdot 4.32675 \geq 1 &\Rightarrow a \in [0.23112, 0.88919) \;=: I_1 \\
12.48692 > a \cdot 6 \geq 1 &\Rightarrow a \in [0.16667, 2.08115) \;=: I_2 \\
122.94567 > a \cdot 8.65350 \geq 1 &\Rightarrow a \in [0.11556, 14.20763) =: I_3 \\
4.83598 > a \cdot 4.25432 \geq 1 &\Rightarrow a \in [0.23506, 1.13672) \;=: I_5 \\
8.13798 > a \cdot 5.96273 \geq 1 &\Rightarrow a \in [0.16771, 1.36481) \;=: I_6 \\
3.51155 > a \cdot 4.30887 \geq 1 &\Rightarrow a \in [0.23208, 0.81496) \;=: I_7
\end{aligned}$$

We see that

$$\bigcap_{\substack{j=1 \\ j \neq 4}}^{7} I_j \neq \emptyset.$$

More precisely, we get the following bounds for a:

$$a \in \bigcap_{\substack{j=1 \\ j \neq 4}}^{7} I_j = [0.23506, 0.81496)\,.$$

Using the observations from the previous three examples and from Remark 4.4, we get the following conjecture:

Conjecture 4.5

There exist constants $0 < a < 1$ and $b > 27$ such that for every cubic number field K_i of type $(1,1)$ with $|d(K_i)| > b$ and fundamental unit $\epsilon_i > 1$, the following inequality holds:

$$\epsilon_i > a\sqrt[3]{|d(K_i)| - 27} \geq 1$$

Next, we try to use a similar method to find out if there is evidence for an upper bound of the fundamental unit $\epsilon_i > 1$ depending on the absolute value of the discriminant $|d(K_i)|$ for cubic number fields of type $(1, 1)$.

Example 4.6

We start by looking at examples of number fields with increasingly large $|d(K_i)|$. We look at the following polynomials:

$$\begin{aligned} f_9 &= x^3 - 3x - 5 \\ f_{10} &= x^3 + 15x + 7 \\ f_{11} &= x^3 + 23x + 7 \\ f_{12} &= x^3 + 37x + 7 \end{aligned}$$

Each f_i has a uniqe real root α_i. As before, we look at the number fields $K_i = \mathbb{Q}(\alpha_i)$, $i = 9, 10, 11, 12$ of type $(1, 1)$. Using Code 9 - Code 12 from the Appendix, we see that

$$\begin{aligned} d(K_9) &= -567 \\ d(K_{10}) &= -1647 \\ d(K_{11}) &= -49991 \\ d(K_{12}) &= -230935 \end{aligned}$$

and that the fundamental units ϵ_i of K_i are

$$\begin{aligned} \epsilon_9 &\approx 11.75196 \\ \epsilon_{10} &\approx 57.21006 \\ \epsilon_{11} &\approx 768.06380 \\ \epsilon_{12} &\approx 43993408.0 \end{aligned}$$

We try to find an upper bound for ϵ_i by using the inequality

$$c \cdot \sqrt[3]{|d(K_i)| - 27} > \epsilon_i$$

For the fields $K_9, K_{10}, K_{11}, K_{12}$ from this example, we solve these inequalities and get

$$\begin{aligned}
c \cdot 8.14325 &> 11.75196 && \Rightarrow c > 1.44315 \\
c \cdot 11.47760 &> 57.21006 && \Rightarrow c > 4.87118 \\
c \cdot 36.83147 &> 768.06380 && \Rightarrow c > 20.85347 \\
c \cdot 61.34978 &> 43993408.0 && \Rightarrow c > 717091.5364
\end{aligned}$$

We note that with increasing $|d(K_i)|$, the quotient $\frac{\epsilon_i}{\sqrt[3]{|d(K_i)|}}$ is increasing too.
For that reason, we suggest that there is no constant c such that

$$c \cdot \sqrt[3]{|d(K_i)| - 27} > \epsilon_i$$

for every cubic number field K_i of type $(1, 1)$ with fundamental unit $\epsilon_i > 1$.

5 Bibliography

[Art11] M. Artin. *Algebra.* Pearson Prentice Hall, 2011.

[Fis13] G. Fischer. *Lineare Algebra: Eine Einführung für Studienanfänger.* Grundkurs Mathematik. Springer Fachmedien Wiesbaden, 2013.

[NS13] J. Neukirch and N. Schappacher. *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[Wei95] Andre Weil. *Basic Number Theory.* Classics in Mathematics. Springer, 3rd edition edition, 1995.

Appendix: SageMath Code

This Chapter contains the SageMath code we use for Chapter 4.

Code 1

```
K.<a> = NumberField(x^3-2)
K.absolute_discriminant()
K.signature()
U = K.unit_group(); U
U.fundamental_units()
e = K.embeddings(RR)[0];
e(a)
e(a-1)
e(1/(a-1))
```

Output:

```
-108
(1, 1)
Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3
    - 2
[a - 1]
1.25992104989487
0.259921049894873
3.84732210186307
```

Code 2

```
K.<a> = NumberField(x^3-3)

K.absolute_discriminant()

K.signature()

U = K.unit_group(); U

U.fundamental_units()

e = K.embeddings(RR)[0];

e(a)

e(a^2-2)

e(1/(a^2-2))
```

Output:

```
-243

(1, 1)

Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3

    - 3

[a^2 - 2]

1.44224957030741

0.0800838230519041

12.4869163570260
```

Code 3

```
K.<a> = NumberField(x^3-5)
K.absolute_discriminant()
K.signature()
U = K.unit_group(); U
U.fundamental_units()
e = K.embeddings(RR)[0];
e(a)
e(2*a^2 - 4*a + 1)
e(1/(2*a^2 - 4*a + 1))
```

Output:

```
-675
(1, 1)
Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3
    - 5
[2*a^2 - 4*a + 1]
1.70997594667670
0.00813168971894440
122.975671055221
```

Code 4

```
K.<a> = NumberField(x^3-6*x^2+11*x-5)
K.absolute_discriminant()
K.signature()
U = K.unit_group(); U
U.fundamental_units()
e = K.embeddings(RR)[0];
e(a)
e(a-2)
e(-(a-2))
```

Output:

```
-23
(1, 1)
Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3
    - 6*x^2 + 11*x - 5
[a - 2]
0.675282042755254
-1.32471795724475
1.32471795724475
```

Code 5

```
K.<a> = NumberField(x^3-6*x^2+11*x-4)
K.absolute_discriminant()
K.signature()
U = K.unit_group(); U
U.fundamental_units()
e = K.embeddings(RR)[0];
e(a)
e(a^2 - 3*a + 1)
e(-1/(a^2 - 3*a + 1))
```

Output:

```
-104
(1, 1)
Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3
    - 6*x^2 + 11*x - 4
[a^2 - 3*a + 1]
0.478620293195432
-0.206783494527816
4.83597591908132
```

Code 6

```
K.<a> = NumberField(x^3-6*x^2+11*x-3)

K.absolute_discriminant()

K.signature()

U = K.unit_group(); U

U.fundamental_units()

e = K.embeddings(RR)[0];

e(a)

e(a^2 - 3*a + 1)

e(1/(a^2 - 3*a + 1))
```

Output:

```
-239

(1, 1)

Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3

    - 6*x^2 + 11*x - 3

[a^2 - 3*a + 1]

0.328300118342839

0.122880612675405

8.13798025764689
```

Code 7

```
K.<a> = NumberField(x^3-6*x^2+11*x-2)

K.absolute_discriminant()

K.signature()

U = K.unit_group(); U

U.fundamental_units()

e = K.embeddings(RR)[0];

e(a)

e(1/2*a^2 - 3/2*a)

e(-1/(1/2*a^2 - 3/2*a))
```

Output:

```
-107

(1, 1)

Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3

    - 6*x^2 + 11*x - 2

[1/2*a^2 - 3/2*a]

0.203678096740558

-0.284774761564910

3.51154714169453
```

Code 8

```
K.<a> = NumberField(x^3+x^2-1)

K.absolute_discriminant()

K.signature()

U = K.unit_group(); U

U.fundamental_units()

e = K.embeddings(RR)[0];

e(a)

e(a^2+a)
```

Output:

```
-23

(1, 1)

Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3

   + x^2 - 1

[a^2 + a]

0.754877666246693

1.32471795724475
```

Code 9

```
K.<a> = NumberField(x^3-3*x-5)

K.absolute_discriminant()

K.signature()

U = K.unit_group(); U

U.gens_values()

U.fundamental_units()

e = K.embeddings(RR)[0];

e(a)

e(a^2-a-3)

e(-1/(a^2-a-3))
```

Output:

```
-567

(1, 1)

Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3

    - 3*x - 5

[-1, a^2 - a - 3]

[a^2 - a - 3]

2.27901878616659

-0.0850921584663409

11.7519642000334
```

Code 10

```
K.<a> = NumberField(x^3+15*x+7)
K.absolute_discriminant()
K.signature()
U = K.unit_group(); U
U.gens_values()
U.fundamental_units()
e = K.embeddings(RR)[0];
e(a)
e((1/3*a^2 - 4/3*a - 2/3))
e(1/(1/3*a^2 - 4/3*a - 2/3))
```

Output:

```
-1647
(1, 1)
Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3
    + 15*x + 7
[-1, 1/3*a^2 - 4/3*a - 2/3]
[1/3*a^2 - 4/3*a - 2/3]
-0.460170386569158
0.0174794436506132
57.2100588547577
```

Code 11

```
K.<a> = NumberField(x^3+23*x+7)

K.absolute_discriminant()

K.signature()

U = K.unit_group(); U

U.gens_values()

U.fundamental_units()

e = K.embeddings(RR)[0];

e(a)

e(a^2 - 3*a - 1)

e(1/(a^2 - 3*a - 1))
```

Output:

```
-49991

(1, 1)

Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3

    + 23*x + 7

[-1, a^2 - 3*a - 1]

[a^2 - 3*a - 1]

-0.303136704517169

0.00130197517703690

768.063798478814
```

Code 12

```
K.<a> = NumberField(x^3+37*x+7)
K.absolute_discriminant()
K.signature()
U = K.unit_group(); U
U.gens_values()
U.fundamental_units()
e = K.embeddings(RR)[0];
e(a)
e(43*a^2 + 1061*a + 199)
e(1/(43*a^2 + 1061*a + 199))
```

Output:

```
-203935
(1, 1)
Unit group with structure C2 x Z of Number Field in a with defining polynomial x^3
    + 37*x + 7
[-1, 43*a^2 + 1061*a + 199]
[43*a^2 + 1061*a + 199]
-0.189006703044760
2.27306600208976e-8
4.39934080000588e7
```