Number Theory and Group Theory with a view towards Homogeneous Dynamics

Constantin Kogler

Contents

I Algebraic Number Theory 4

1 Basic Algebraic Number Theory 5
1.1 A Review of Field Extensions 5
1.2 Norm, Trace and Discriminant 8
1.3 Integral Ring Extensions 12
1.4 Ideals and Dedekind Rings 18

2 Gauss's Reciprocity Law 22
2.1 The Decomposition of Primes in $\mathcal{O}_K$ 22
2.2 The Splitting of Primes 23
2.3 Gauss's Reciprocity Law 24

3 Lattices 26
3.1 Lattices in Vector Spaces 26
3.2 The Space of Unimodular Lattices 29
3.3 Lattices in Topological Groups and Haar Measures 31
3.4 Lattices for Unipotent Subgroups 32

4 Class Numbers and Units 34
4.1 Minkowski Theory 34
4.2 Finiteness of the Class Number 38
4.3 Dirichlet's Unit Theorem 40
4.4 Orders and the Picard Group 44
4.5 Orders and Periodic Orbits 46
4.6 Duke's Theorem and the Height of Lattices 49

5 Binary Quadratic Forms 55
5.1 The Narrow Class Group 55
5.2 Binary Quadratic Forms and Number Fields 55
5.3 Binary Quadratic Forms and Proper Ideals 62
5.4 Binary Quadratic Forms and Duke's Theorem 67

6 p-adic Numbers 73
6.1 Definition of the p-adic Numbers 73
6.2 Algebraic Properties of the p-adic Integers 77
6.3 Topological Properties 78

7 Valuations and Local Fields 82
7.1 Valuations 82
7.2 Global and Local Fields 82

II The Theory of Linear Algebraic Groups 83

8 Essence of Algebraic Geometry **84**
8.1 Zariski Topology 84
8.2 Affine Algebraic Varieties 88
8.3 Prevarieties and Varieties 90
8.4 F-structures and affine F-varieties 91
8.5 Projective Variety 94
8.6 Complete Varieties 94
8.7 Smooth Points 94
8.8 Dimension 94

9 Linear Algebraic Groups **96**
9.1 Definitions and Examples 96
9.2 Basic Properties 96
9.3 Group Actions and Representations 98
9.4 Jordan Decomposition 101
9.5 Commutative Algebraic Groups 102
9.6 Linear Algebraic Groups defined over $\mathbb{R}$ 103

10 Compact Orbits and Orders **104**
10.1 Closed Orbits for Rational Representations 104
10.2 Compact Orbits and Dirichlet's Unit Theorem 104
10.3 Compact Orbits and Ideals 109

11 The Borel-Harish-Chandra Theorem **113**
11.1 Quantitive Non-Divergence for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})$ 113

References **116**

Part I
Algebraic Number Theory

1 Basic Algebraic Number Theory

1.1 A Review of Field Extensions

In this subsection we recall central terms and statements concerning field extensions. Many of the statements in this subsection are inspired by [Pin16b]. The proofs in this section will be rather brief – for more details we refer to the books by [Bos93] or [Rot10].

Definition 1.1. Let $K \subset L$ be fields. Then the tuple (L, K) is called a *field extension*.

A *ring extension* is defined analogously. Note that for any field extension (L, K) the field L can be seen as a vector space over K.

Definition 1.2. Let (L, K) be a field extension. The dimension of L viewed as a vector space over K is called the *degree* of the field extension and is denoted by $[L : K]$. Further, a field extension (L, K) is called *finite* if it has finite degree.

Example 1.3. The field extension $(\mathbb{R}, \mathbb{Q})$ is not finite, since finiteness of $(\mathbb{R} : \mathbb{Q})$ would imply that $\mathbb{R}$ is countable.

A central object of study in Algebraic Number Theory is a so called *number field*.

Definition 1.4. A *number field* is a finite field extension of the rational numbers.

Definition 1.5. Let (L, K) be a field extension. An element $a \in L$ is called *algebraic over* K if there are coefficients $k_1, \ldots, k_n \in K$ such that

$$a^n + k_1 a^{n-1} + \ldots + k_n = 0.$$

The field extension (L, K) is called *algebraic* if every element of L is algebraic over K. We further say that a complex number is *algebraic* if it is algebraic over $\mathbb{Q}$.

A field extension that is not algebraic is called *transcendental*.

One easily checks that an element $a \in L$ is algebraic over K if and only if there is a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$. Furthermore, recall that for an algebraic element element $a \in L$, the *minimal polynomial of* a is the unique irreducible normed polynomial $f \in K[X]$ with $f(a) = 0$. We next recall some basic facts about algebraic field extension.

Proposition 1.6. *Let (L, K) be a field extension and $a \in L$ an element. Then the following properties are equivalent:*

(i) a is algebraic over K.

(ii) $K[a]$ is a field of finite degree over K.

Proof. Assume that a is algebraic and let f be the minimal polynomial of a. Then consider the homomorphism

$$\varphi : K[X] \to L, \qquad f \mapsto f(\alpha).$$

We thus have that $K[\alpha] \cong K[X]/\ker(\varphi)$, with $\ker(\varphi) = (f)$. Since f is irreducible and $K[X]$ is a principle ideal domain, we conclude that (f) is a maximal ideal and thus $K[a]$ is a field and hence equal to $K(a)$. A basis for $K[a]$ is given by $1, a, a^2, \ldots, a^{n-1}$, where n is the degree of f.

Conversely assume that $K[a]$ is a field of finite degree over K. Then a basis over K represents any power of a. Thus choosing a high enough power of a, we see that a is algebraic. □

Proposition 1.7. *Let (L, K) be a field extension and let $a_1, \ldots, a_n \in L$. Then $a_1, \ldots, a_n$ are algebraic over K, if and only if is the field extension $(K(a_1, \ldots, a_n), K)$ is finite.*

Proof. We use the proceeding proposition together with induction. □

Proposition 1.8. *Every finite field extension is algebraic.*

Proof. This follows directly form any of the last two propositions. □

Example 1.9. The converse of the above proposition does not hold. For example consider the set $A = \{\sqrt{n} : n \in \mathbb{N}_{\geq 2}\}$ and the field extension $(\mathbb{Q}(A), \mathbb{Q})$.

Proposition 1.10. *If (M, L) and (L, K) are field extensions. Then (M, K) is algebraic if and only if (M, L) and (L, K) are algebraic.*

Proof. If (M, K) is algebraic, then it follows directly that (M, L) and (L, K) are algebraic. Conversely if (M, L) and (L, K) are algebraic, then for any element $a \in M$, there are coefficients $b_1, \ldots, b_n \in L$ such that $a^n + b_1 a^{n-1} + \ldots + b_n = 0$. Since (L, K) is algebraic, the field extension $(K(b_1, \ldots, b_n), K)$ is finite. By the above, it follows that $K(b_1, \ldots, b_n, a)$ is finite and hence a is algebraic over K. □

We next study *homomorphisms over K*.

Definition 1.11. Let (L, K) and (L', K) be field extensions. A field homomorphism $\varphi : L \to L'$ that is the identity on K is called a *field homomorphism over K*. The set of homomorphisms $L \to L'$ over K is denoted $\mathrm{Hom}_K(L, L')$.

Proposition 1.12. *If $[L : K] = [L' : K] < \infty$, then every homomorphism $\varphi : L \to L'$ over K is is an isomorphism.*

Proof. Recall that every field homomorphism is injective. Furthermore, we can view φ as a injective vector space homomorphism between two vector spaces of the same dimension. Thus φ is an isomorphism. □

Proposition 1.13. *Let (L, K) and (L', K) be field extensions and $\varphi : L \to L'$ be a homomorphism over K. Then $a \in L$ is algebraic if and only if $\varphi(a)$ is algebraic. In this case, a and $\varphi(a)$ have the same minimal polynomial.*

Proof. If $a \in L$ is algebraic, then there are coefficients $b_1, \ldots, b_n \in K$ such that $a^n + b_1 a^{n-1} + \ldots + b_n = 0$. Then by applying φ to this expression and using that φ is constant on K, we see that $\varphi(a)$ is algebraic. The converse follows analogously since φ is injective. For the last statement let f be the minimal polynomial of a. Then since $f(\varphi(a)) = \varphi(f(a)) = 0$, we conclude that f is also the minimal polynomial of $\varphi(a)$. □

Proposition 1.14. *Let (L, K) and (L', K) be field extensions, $\varphi : L \to L'$ a homomorphism over K and let $a \in L$ be an algebraic element with minimal polynomial f. Then the map*

$$\mathrm{Hom}_K(K(a), L') \to \{a' \in L' \,:\, f(a) = 0\},$$

is a bijection.

Proof. The map is well defined by the last proposition. Furthermore it is injective, since any such homomorphism is determined by the image of the basis elements $1, a, \ldots, a^{n-1}$. Lastly, surjectivity is left as an exercise. □

Proposition 1.15. *If (L, K) is a finite field extension and (L', K) is any field extension, then*

$$|\mathrm{Hom}_K(L, L')| \leq [L : K].$$

Proof. Assume first that $L = K(a)$ for some element $a \in L$. Then by the last proposition $|\mathrm{Hom}_K(L, L')| = |\{a' \in L' \,:\, f(a) = 0\}|$ for f the minimal polynomial. Since the degree of the minimal polynomial f equals $[K(a) : K]$, we conclude that the minimal polynomial has at most as many zeros as the degree of the extension $[K(a) : K]$.

For the general case, where $L = K(a_1, \ldots, a_n)$ have with the first case that

$$\begin{aligned}
&|\mathrm{Hom}_K(K(a_1, \ldots, a_n), L')| \\
&= |\mathrm{Hom}_K(K(a_1, \ldots, a_n) : K(a_1, \ldots, a_{n-1}))| \cdot \ldots \cdot |\mathrm{Hom}_K(K(a_1), K)| \\
&\leq [K(a_1, \ldots, a_{n-1})(a_n), K(a_1, \ldots, a_{n-1})] \cdot \ldots \cdot [K(a_1) : K] = [L : K].
\end{aligned}$$

□

We next recall, what is means for a field extension to be separable. For this we first define separable polynomials.

Definition 1.16. Let K be a field with algebraic closure $\overline{K}$. A non-zero polynomial $f \in K[X]$ that does not have multiple zeros in $\overline{K}$ is called *separable*.

Proposition 1.17. *An non-zero polynomial $f \in K[X]$ is separable, if and only if the polynomial f and the formal derivative f' have no common divisor in $K[X]$.*

Proof. Assume that $f \in K[X]$ is separable. If f and f' had a common divisor, then, since $\overline{K}$ is algebraically closed, there was some $\alpha \in \overline{K}[X]$ such that

$$(X - \alpha) \mid f \qquad \text{and} \qquad (X - \alpha) \mid f'$$

and so by using the Leibniz rule $(X - \alpha)^2 \mid f$, contradiction the assumption of separability. The converse follows analogously. □

Proposition 1.18. *An irreducible non-zero polynomial $f \in K[X]$ is separable, if and only if the formal derivative $f' \neq 0$.*

Proof. This follows straightforwardly from the last proposition. □

Definition 1.19. Let (L, K) be an algebraic field extension. An element $a \in L$ is called *separable*, if the minimal polynomial of a is separable. If every element of L is separable, then the field extension (L, K) is called separable.

Proposition 1.20. *Let $L = K(a_1, \ldots, a_n)$ be a finite extension of K and let $\overline{K}$ be an algebraic closure of K. Then the following properties are equivalent:*

(i) (L, K) *is separable.*

(ii) Every a_i *is separable.*

(iii) $|\mathrm{Hom}_K(L, \overline{K})| = [L : K]$.

Proof. That (i) and (ii) are equivalent is left as an exercise. That (ii) and (iii) are equivalent follows very analogous to Proposition 1.14. □

We next state a few properties of separable extensions without proof. Proofs of these statements can be found for example in [Bos93].

Proposition 1.21. *An algebraic field extension $(K(A), K)$ for a set A is separable if and only if every element of A is separable.*

Proposition 1.22. *Let (M, L) and (L, K) be separable field extension. Then (M, K) is separable if and only if (M, L) and (L, K) are separable.*

Example 1.23. Every separable field extension of a field of characteristic zero is separable. This follows by Proposition 1.18.

1.2 Norm, Trace and Discriminant

Let (L, K) be a field extension. Denote for $x \in L$ the map

$$T_x : L \to L, \qquad T_x(a) = xa.$$

We view T_x as a linear map of vector spaces over K.

Definition 1.24. Let (L, K) be a field extension. We define the *norm* and *trace* of an element $x \in L$ as

$$\mathrm{Tr}_{(L,K)}(x) = \mathrm{Tr}(T_x), \qquad \mathrm{N}_{(L,K)}(x) = \det(T_x).$$

Denote by $f_x(t) = \det(t\mathrm{Id} - T_x) = t^n - a_1 t^{n-1} + \ldots + (-1)^n a_n \in K[t]$ the characteristic polynomial of T_x, then we have that $n = [L : K]$ and

$$a_1 = \mathrm{Tr}_{(L,K)}(x) \qquad a_n = \mathrm{N}_{(L,K)}(x).$$

Furthermore, note that since $T_{x+y} = T_x + T_y$ and $T_{xy} = T_x \circ T_y$ we have homomorphisms

$$\mathrm{Tr}_{(L,K)} : L \to K, \qquad N_{(L,K)} : L^* \to K^*.$$

For finite separable extensions we have the following expression for the norm an trace of an element $x \in L$.

Theorem 1.25. *Let (L, K) be a finite separable field extension and $x \in L$. Then we have that*

$$f_x(t) = \prod_{\sigma \in \mathrm{Hom}(L, \overline{K})} (t - \sigma x)$$

and thus by expanding

$$\mathrm{Tr}_{(L,K)}(x) = \sum_{\sigma \in \mathrm{Hom}(L, \overline{K})} \sigma x \qquad \textit{and} \qquad \mathrm{N}_{(L,K)}(x) = \prod_{\sigma \in \mathrm{Hom}(L, \overline{K})} \sigma x.$$

Before proving Theorem 1.25, we state the following lemma.

Lemma 1.26. *Let (L, K) be a finite separable field extension and $x \in L$. Denote by $\overline{K}$ an algebraic closure of K and by $p_x \in K[X]$ the minimal polynomial of x. Then we have in $\overline{K}[X]$*

$$p_x(t) = \prod_{\sigma \in \mathrm{Hom}(K(x), \overline{K})} (t - \sigma x).$$

Proof. This follows by Proposition 1.14 and the definition of separability. □

Proof. (of Theorem 1.25) We first claim that $f_x(t) = p_x(t)^d$ where $d = [L : K(x)]$ and $p_x(t)$ is the minimal polynomial of x. To see this write

$$p_x(t) = t^m + c_1 t^{m-1} + \ldots + c_m$$

with $m = [K(x) : K]$. Recall that $1, x, \ldots, x^{m-1}$ is a basis of $(K(x), K)$. Thus if $\alpha_1, \ldots, \alpha_n$ is a basis of $(L : K(x))$ we have that

$$\alpha_1, x\alpha_1, \ldots, x^{m-1}\alpha_1, \ldots, \alpha_d, x\alpha_d, \ldots, x^{m-1}\alpha_d$$

is a basis for $(L : K)$. The representation matrix of the endomorphism T_x with respect to this basis consists of d diagonal blocks of the form

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \ldots & -c_1 \end{pmatrix}.$$

Hence we conclude inductively by using the Laplace expansion that the characteristic polynomial of this block matrix is equal to $p_x(t)$ and thus $f_x(t) = p_x(t)^d$.

To derive the theorem we note that the set $\mathrm{Hom}_K(L, \overline{K})$ decomposes under the relation

$$\sigma \sim \tau \Leftrightarrow \sigma x = \tau x$$

into m equivalence classes with d elements. By the last lemma, if we choose representatives $\sigma_1, \ldots, \sigma_m$, then $p_x(t) = \prod_{i=1}^{m}(t - \sigma_i x)$ and the theorem follows. □

Corollary 1.27. *Let (M, L) and (L, K) be finite and separable extensions. Then*

$$\mathrm{Tr}_{(L,K)} \circ \mathrm{Tr}_{(M,L)} = \mathrm{Tr}_{(M,K)}, \qquad \textit{and} \qquad \mathrm{N}_{(L,K)} \circ \mathrm{N}_{(M,L)} = \mathrm{N}_{(M,K)}$$

Proof. The set $\mathrm{Hom}_K(M, \overline{K})$ decomposes under the equivalence relation

$$\sigma \sim \tau \quad \Longleftrightarrow \quad \sigma|_L = \tau|_L$$

into $m = [L : K]$ equivalence classes. If $\sigma_1, \ldots, \sigma_m$ is a system of representatives, then

$$\begin{aligned}\mathrm{Tr}_{(M,K)}(x) &= \sum_{i=1}^{m} \sum_{\sigma \sim \sigma_i} \sigma_x \\ &= \sum_{i=1}^{m} \mathrm{Tr}_{(\sigma_i M, \sigma_i L)}(\sigma_i x) \\ &= \sum_{i=1}^{m} \sigma_i \mathrm{Tr}_{(M,L)}(x) = \mathrm{Tr}_{(L,K)}(\mathrm{Tr}_{(M,L)}(x)).\end{aligned}$$

The same calculation also works for the norm. □

Example 1.28. As a simple example, we consider the number field $(\mathbb{Q}(\sqrt{p}), \mathbb{Q})$ for a prime number p and the element $x = \sqrt{p} \in \mathbb{Q}(\sqrt{p})$. Consider the basis $1, \sqrt{p}$ of $\mathbb{Q}(\sqrt{p})$ and note that $T_x(1) = \sqrt{p}$ and $T_x(\sqrt{p}) = p$. This shows that

$$T_x = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$$

with respect to the basis $1, \sqrt{p}$ and so

$$\mathrm{Tr}_{(\mathbb{Q}(\sqrt{p}),\mathbb{Q})}(x) = 0, \qquad \mathrm{N}_{(\mathbb{Q}(\sqrt{p}),\mathbb{Q})}(x) = -p.$$

To check the validity of Theorem 1.25, we note that by Proposition 1.14 the set $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{p}), \overline{\mathbb{Q}})$ consists of the two homomorphisms $\sigma_1, \sigma_{-1} : \mathbb{Q}(\sqrt{p}) \to \overline{\mathbb{Q}}$, where

$$\sigma_{\pm 1}(\sqrt{p}) = \pm\sqrt{p}.$$

So we have that

$$\mathrm{Tr}_{(\mathbb{Q}(\sqrt{p}):\mathbb{Q})}(x) = \sum_{\sigma \in \mathrm{Hom}(\mathbb{Q}(\sqrt{p}), \overline{\mathbb{Q}})} \sigma x = \sigma_1(\sqrt{p}) + \sigma_{-1}(\sqrt{p}) = \sqrt{p} + (-\sqrt{p}) = 0$$

and

$$\mathrm{N}_{(\mathbb{Q}(\sqrt{p}):\mathbb{Q})}(x) = \prod_{\sigma \in \mathrm{Hom}(\mathbb{Q}(\sqrt{p}), \overline{\mathbb{Q}})} \sigma x = \sigma_1(\sqrt{p}) \cdot \sigma_{-1}(\sqrt{p}) = \sqrt{p} \cdot (-\sqrt{p}) = -p.$$

We next discuss the discriminant with respect to some basis.

Definition 1.29. Let (L, K) be a finite separable field extension and $\alpha_1, \ldots, \alpha_n$ a basis of L over K. Furthermore denote by $\sigma_1, \ldots, \sigma_n$ the n elements of $\mathrm{Hom}_K(L, \overline{K})$. Then we define the discriminant of this basis as

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j))^2.$$

Note that the discriminant is well defined. More precisely, observe that for any other choice of order of the σ_i, the expression $\det((\sigma_i \alpha_j))$ might at most change by the sign. As the discriminant is the square of $\det((\sigma_i \alpha_j))$, it does not depend on the choice of order of σ_i.

Example 1.30. Let p be a prime number. Then the discriminant of $(\mathbb{Q}(\sqrt{p}), \mathbb{Q})$ with respect to the basis $(1, \sqrt{p})$ is $4p^2$.

Lemma 1.31. *Let (L, K) be a finite separable field extension and $\alpha_1, \ldots, \alpha_n$ be a basis. Then*

$$d(\alpha_1, \ldots, \alpha_n) = \det\big(\mathrm{Tr}_{(L,K)}(\alpha_i \alpha_j)\big).$$

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the elements of $\mathrm{Hom}_K(L, \overline{K})$. Then we have that

$$\mathrm{Tr}_{(L,K)}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k \alpha_i \alpha_j = \sum_{k=1}^{n} (\sigma_k \alpha_i)(\sigma_k \alpha_j).$$

Thus $\mathrm{Tr}_{(L,K)}(\alpha_i \alpha_j)$ is the product of the matrices $(\sigma_k \alpha_i)^T$ and $(\sigma_k \alpha_j)$. So the statement follows. □

Lemma 1.32. *Let (L, K) be a finite separable extension with basis $1, \theta, \ldots, \theta^{n-1}$ for some $\theta \in L$. Then*

$$d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2$$

for $\theta_i = \sigma_i \theta$, where $\sigma_1, \ldots, \sigma_n$ are the elements of $\mathrm{Hom}_K(L, \overline{K})$.

Proof. This follows since the matrix $\sigma_i \theta^j$ is of the form

$$\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}$$

and the formula for the Vandermonde determinant. □

Proposition 1.33. *Let (L, K) be a finite separable extension and $\alpha_1, \ldots, \alpha_n$ a basis, then we have that the discriminant*

$$d(\alpha_1, \ldots, \alpha_n) \neq 0$$

and the bilinear form

$$(x, y) = \mathrm{Tr}_{(L,K)}(xy)$$

is non-degenerate.

Proof. We first consider the case $L = K(\theta)$ for $\theta \in L$. Thus $1, \theta, \ldots, \theta^{n-1}$ is a basis. Then the above bilinear form with respect to this basis is of the form

$$(x, y) = x^T M y$$

for $M = (\mathrm{Tr}_{(L,K)}(\theta^{i-1} \theta^{j-1}))_{1 \leq i,j \leq n}$. By the last lemma

$$\det(M) = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0$$

and we conclude that the bilinear form is non-degenerate. For a general finite separable field extension (L, K) Corollary 1.27 implies that $(x, y) = \mathrm{Tr}_{(L,K)}(xy)$ is non-degenerate.

For the general case, where $\alpha_1, \ldots, \alpha_n$ is a basis of (L, K), the bilinear form with respect to this basis is given by $(\mathrm{Tr}(\alpha_i \alpha_j))_{1 \leq i,j \leq n}$. As $(x, y) = \mathrm{Tr}_{(L,K)}(xy)$ is non-degenerate

$$d(\alpha_1, \ldots, \alpha_n) = \det(M) \neq 0.$$

□

1.3 Integral Ring Extensions

In analogy to field extensions, we can also study ring extensions. In this section we examine *integral* ring extensions, the analogue of algebraic extensions in the setting of rings. The theory of field extensions heavily uses the theory of vector spaces. In the setting of ring extension, we need to cope with the more subtle theory of modules over a ring R. This has some draw backs. For example, there is no notion of dimension for modules imitating the concept of dimension for vector spaces. Thus we can't define the *degree* of a ring extension. However, some aspects of the theory of ring extension are similar.

Definition 1.34. Let (B, A) be a ring extension. We call an element $b \in B$ *integral* over A if there are coefficients $a_1, \ldots, a_n \in A$ such that

$$b^n + a_1 b^{n-1} + \ldots + a_{n-1} b + a_n = 0.$$

The ring extension $A \subset B$ is called *integral* if every element of B is integral over A.

An important fact about integral elements is, that a sum or product of integral numbers is also integral. This is generalized in the next theorem.

Theorem 1.35. *Let (B, A) be a ring extension and consider $b_1, \ldots, b_n \in B$. The elements $b_1, \ldots, b_n$ are integral over A if and only if the A-module $A[b_1, \ldots, b_n]$ is finitely generated.*

Before starting the proof, we recall that we call a module M over a ring A finitely generated if there is some finite set I such that $R^I \cong M$.

Proof. Assume that b is integral. Then the ring $A[b]$ is generated by $1, b_1, \ldots, b_{n-1}$. The general case $A[b_1, \ldots, b_n]$ follows from this via induction and the fact that $A[b_1, \ldots, b_n] \cong A[b_1, \ldots, b_{n-1}][b_n]$.

The other direction follows from some considerations involving linear algebra over rings, which we won't recall here for simplicity. A proof of this direction can be found in Chapter 10 of [Pin16a] or on Page 7 of [Neu07]. □

With the help of this theorem we can easily deduce the next two corollaries, one of which is the aforementioned fact that the sum or product of integral elements is integral.

Corollary 1.36. *Let (B, A) be a ring extension. If $a, b \in B$ are integral over A, then so is $a + b$ and $a \cdot b$.*

Proof. We note that

$$A[a, b] = A[a, b, a + b, a \cdot b].$$

Thus the last Theorem implies that $a + b$ and $a \cdot b$ are integral over A. □

Corollary 1.37. *Let (C, B) and (B, A) be ring extensions. Then (C, A) is integral if and only if (C, B) and (B, A) are integral.*

Proof. If (C, A) is integral, then clearly (C, B) and (B, A) are integral.

Conversely assume that (C, B) and (B, A) are integral and let $c \in C$. Since c is integral over B, there are coefficients $b_1, \ldots, b_n \in B$ with

$$c^n + b_1 c^{n-1} + \ldots + b_{n-1} c + b_n = 0.$$

Thus c is integral over $A[b_1, \ldots, b_n]$. Hence by Theorem 1.35 the ring $A[b_1, \ldots, b_n][c]$ is a finitely generated module over $A[b_1, \ldots, b_n]$. Further note that $A[b_1, \ldots, b_n]$ is a finitely generated module over A, since B is integral over A. This implies that $A[b_1, \ldots, b_n][c] = A[b_1, \ldots, b_n, c]$ is a finitely generated A-module and hence c is integral by using again Theorem 1.35. □

Definition 1.38. Let $A \subset B$ be a ring extension. The *integral closure* $\overline{A}$ of A in B is defined as

$$\overline{A} = \{b \in B : b \text{ is integral over } A\}.$$

Note that it follows from Corollary 1.36 that $\overline{A}$ is a subring of B.

If $\overline{A} = A$, then A is called *integrally closed* in B.

Definition 1.39. An integral domain R is called *normal* if it is integrally closed in its field of fractions.

The next proposition shows that for example $\mathbb{Z}$ is a normal ring.

Proposition 1.40. *Any unique factorization domain is normal.*

Proof. Consider $\frac{a}{b} \in \mathrm{Quot}(R)$ an element in the quotient field that is integral over R. So there exists $a_1, \ldots, a_n \in R$ with

$$\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \ldots + a_n = 0.$$

Multiplying by b^n yields

$$a^n + a_1 b a^{n-1} + \ldots + a_n b^n = 0$$

Thus every prime element that divides b also divides a. Since in a unique factorization domain, we can write every element as a product of prime elements and some units, it follows that $\frac{a}{b} \in R$. □

An *integral basis*, which is defined next, imitates the notion of a basis in the setting of vector spaces. However, in contrast to the theory of vector spaces, integral bases do not always exist

Definition 1.41. Let (B, A) be an integral ring extension. A system of elements $\omega_1, \ldots, \omega_n \in B$ is called an *integral basis* of B over A if every element $b \in B$ can be written uniquely as

$$b = a_1\omega_1 + \ldots + a_n\omega_n$$

for coefficients $a_i \in A$.

In the following, we consider A be a normal integral domain with quotient field K. Furthermore let (L, K) be a finite separable extension and let B the integral closure of A in L. Note that by Corollary 1.37, then ring B is integrally closed in L. If furthermore $x \in B$ is an integral element of L then we also have that σx is integral for any field homomorphism $\sigma \in \mathrm{Hom}_K(L, \overline{K})$. With the help of Theorem 1.25 we derive that

$$\mathrm{Tr}_{(L,K)}(x), \mathrm{N}_{(L,K)}(x) \in A.$$

Proposition 1.42. *In the above setting, any integral basis of B over A is also a basis of L over K. Thus the length of any integral basis of B over A is equal to the degree $[L : K]$.*

Proof. It suffices to show that every element $\beta \in L$ can be written as

$$\beta = \frac{b}{a},$$

where $b \in B$ and $a \in A$. To see this, choose some $\beta \in L$. Since β is algebraic, there is $n \geq 1$ and $k_1, \ldots, k_n \in K$ such that

$$\beta^n + k_1\beta^{n-1} + \ldots + k_n = 0.$$

If we write $k_i = \frac{a_i''}{a_i'}$ for $a_i', a_i'' \in A$, we derive after multiplying with $a_1''a_2'' \ldots a_n''$ that

$$a_n\beta^n + a_{n-1}\beta^{n-1} + \ldots + a_0 = 0$$

for some $a_i \in A$. By multiplying the last equation with a_n^{n-1}, we conclude that the element $b = a_n\beta$ is integral over A and thus contained in B. So the claim is proved. □

If A is a principle ideal domain the next theorem guarantees the existence of an integral basis.

Theorem 1.43. *Let A be a principle ideal domain with quotient field K. Furthermore let (L, K) be a finite separable extension and let B be the integral closure of A in L. Then every finitely generated B-submodule $M \neq 0$ of L is a free A-module of rank $[L : K]$. In particular, the ring B has an integral basis over A.*

We first prove the following lemma.

Lemma 1.44. *Let $\alpha_1, \ldots, \alpha_n$ be a basis of L over K that is contained in B with discriminant $d = d(\alpha_1, \ldots, \alpha_n)$. Then we have that*

$$dB \subset A\alpha_1 + \ldots + A\alpha_n.$$

Proof. If $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \in B$ with $a_j \in K$ then the a_j solve the linear system of equations

$$\mathrm{Tr}_{(L,K)}(\alpha_i\alpha) = \sum_j \mathrm{Tr}_{(L,K)}(\alpha_i\alpha_j)a_j.$$

Note that $\mathrm{Tr}_{(L,K)}(\alpha_i\alpha_j), \mathrm{Tr}_{(L,K)}(\alpha_i\alpha_j) \in A$ and that $\det\big(\mathrm{Tr}_{(L,K)}(\alpha_i\alpha_j)\big) = d(\alpha_1, \ldots, \alpha_n) \neq 0$. Hence each coefficient of the inverse of the matrix $\mathrm{Tr}_{(L,K)}(\alpha_i\alpha_j)$ can be expressed as a fraction between an element of A and d. Thus a_j is also a fraction of an element in A by d. Thus $da_j \in A$ and hence

$$d\alpha \in A\alpha_1 + \ldots + A\alpha_n.$$

□

Proof. (of Theorem 1.43) Let $M \neq 0$ be a finitely generated B-submodule of L and $\alpha_1, \ldots, \alpha_n$ a basis of L over K. By the proof of Proposition 1.42 we can multiply with a suitable element from A to achieve that the basis is contained in B. By the last Lemma we then have that

$$dB \subset A\alpha_1 + \ldots + A\alpha_n =:$$

for $d = d(\alpha_1, \ldots, \alpha_n)$. Note that M_0 is a free A-module of rank n, as $\alpha_1, \ldots, \alpha_n$ is a basis of (L, K).

If $\mu_1, \ldots, \mu_r \in M$ is a generating set of the B-module M, there again is some $a \in A$ with $a\mu_i \in B$ for all $1 \leq i \leq n$. Thus $aM \subset B$. So we derive that

$$adM \subset dB \subset A\alpha_1 + \ldots + A\alpha_n$$

By the fundamental theorem of modules over a principle ideal domain, we conclude that since M_0 is a free A-module, the module adM and so also the module M is free over A. Since

$$\operatorname{rank}(M) = \operatorname{rank}(dM) \leq \operatorname{rank}(M_0) \leq \operatorname{rank}(M),$$

where the last inequality follows as $M_0 \subset B$. So we proved $\operatorname{rank}(M) = \operatorname{rank}(M_0) = [L : K]$. □

We now reduce to the case $A = \mathbb{Z}$, $K = \mathbb{Q}$ and consider a number field K and denote by $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in K. We usually call $\mathcal{O}_K$ the *ring of integers* of K. It turns out, as we show next, that in this setting the discriminant is independent of the choice of basis as long as we choose integral bases.

Proposition 1.45. *Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Then the discriminant*

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j))^2$$

does not depend on the choice of the integral basis.

We then call

$$d_K = d(\alpha_1, \ldots, \alpha_n)$$

the *discriminant of the number field K* where $\alpha_1, \ldots, \alpha_n$ is any integral basis of $\mathcal{O}_K$.

Proof. Let $\alpha_1', \ldots, \alpha_n'$ be another integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Then the transformation matrix $T = (a_{ij})$, $\alpha_i' = \sum_j a_{ij}\alpha_j$ is an integer matrix, where the inverse of this matrix also consists of integers. Hence $\det(T) = \pm 1$. Note that

$$\begin{aligned}
\operatorname{Tr}_{(L,K)}(\alpha_i'\alpha_j') &= \operatorname{Tr}_{(L,K)}\left(\sum_l a_{il}\alpha_l \sum_k a_{jk}\alpha_k\right) \\
&= \sum_{\sigma \in \operatorname{Hom}(K, \overline{\mathbb{Q}})} \sigma\left(\sum_l a_{il}\alpha_l \sum_k a_{jk}\alpha_k\right) \\
&= \sum_{l,k} a_{il}a_{jk} \sum_{\sigma \in \operatorname{Hom}(K, \overline{\mathbb{Q}})} \sigma(\alpha_l\alpha_k) \\
&= \sum_{l,k} a_{il}a_{jk} \operatorname{Tr}(\alpha_l\alpha_k)
\end{aligned}$$

This implies

$$\begin{aligned} d(\alpha'_1,\dots,\alpha'_n) &= \det\big(\mathrm{Tr}_{(L,K)}(\alpha'_i\alpha'_j)\big) \\ &= \det\big(T^2\mathrm{Tr}_{(L,K)}(\alpha_i\alpha_j)\big) \\ &= \det(T)^2 d(\alpha_1,\dots,\alpha_n) = d(\alpha_1,\dots,\alpha_n). \end{aligned}$$

□

Proposition 1.46. *If $\mathfrak{a} \subset \mathfrak{a}'$ are two non-zero finitely generated $\mathcal{O}_K$ modules of K, then the index $(\mathfrak{a}' : \mathfrak{a})$ is finite and we have*

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}').$$

Proof. The two modules $\mathfrak{a}$ and $\mathfrak{a}'$ both have rank $n = [K : \mathbb{Q}]$. So any integral basis of $\mathfrak{a}$ and $\mathfrak{a}'$ have the same length. Thus let $\alpha_1,\dots,\alpha_n$ be an integral basis of $\mathfrak{a}$ and $\alpha'_1,\dots,\alpha'_n$ be an integral basis of $\mathfrak{a}'$. Let A be the transformation matrix from $\alpha_1,\dots,\alpha_n$ to $\alpha'_1,\dots,\alpha'_n$. Then by the same calculation as in the last proposition we have that

$$d(\mathfrak{a}) = \det(A)^2 d(\mathfrak{a}').$$

So we need to prove $\det(A) = (\mathfrak{a}' : \mathfrak{a})$. (How to prove this?) □

We next give two the following example.

Proposition 1.47. *Let d be a square free integer and consider $K = \mathbb{Q}(\sqrt{d})$. Then we have that the ring of integers is*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \mod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \mod 4. \end{cases}$$

Moreover the discriminant of K is

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \mod 4, \\ 4d & \text{if } d \equiv 2,3 \mod 4. \end{cases}$$

Before proving this proposition we start with the following lemma.

Lemma 1.48. *Let K be a number field. Then an element $x \in K$ is an algebraic integer if and only if the minimal polynomial of x has integer coefficients.*

Proof. If the minimal polynomial of $x \in K$ has integer coefficients, then x is clearly algebraic. Conversely assume that $x \in K$ is algebraic. Then it is the root of a monic polynomial with integer coefficients. So it will be the root of one of its irreducible factors which has again integers coefficients. □

Proof. (of Proposition1.47) First note that in any case

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \subset \mathcal{O}_K.$$

Using the last lemma we see that if $x = a + b\sqrt{d} \in \mathcal{O}_K$ with $a, b \in \mathbb{Q}$ we have that the minimal polynomial of x over $\mathbb{Q}$ has integer coefficients and is of degree 2 as $[K : \mathbb{Q}] = 2$. Thus we have

$$\mathrm{Tr}_{(K:\mathbb{Q})}(x) = 2a \in \mathbb{Z} \quad \text{and} \quad \mathrm{N}_{(\mathbb{Q}:K)}(x) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d \in \mathbb{Z}.$$

This shows that there is an integer n with $a = \frac{n}{2}$. Thus

$$a^2 - b^2 d = \frac{n^2}{4} + b^2 d \in \mathbb{Z} \quad \text{or equivalently} \quad n^2 + 4b^2 d \in 4\mathbb{Z}.$$

We note that if $b \notin \frac{1}{2}\mathbb{Z}$, then we have that $4|d$, which is a contradiction. Thus we have that $b \in \frac{1}{2}\mathbb{Z}$. Thus we conclude that

$$\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K \subset \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}\sqrt{d}.$$

To determine $\mathcal{O}_K$ it this suffices to consider

$$x = \frac{a}{2} + \frac{b}{2}\sqrt{d} \in \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}\sqrt{d}$$

with $a, b \in \mathbb{Z}$, we note that

$$\mathrm{Tr}_{(K:\mathbb{Q})}(x) = a \in \mathbb{Z} \quad \text{and} \quad \mathrm{N}_{(\mathbb{Q}:K)}(x) = \frac{1}{4}(a^2 - b^2 d).$$

So we see that $x \in \mathcal{O}_K$ if and only if $a^2 - b^2 d \in 4\mathbb{Z}$.

To determine for which such x this holds. we proceed by a case distinction. First, note that if both a and b are even, then this is clearly the case. Next if a is even and b odd then we have $b^2 \equiv 1 \mod 4$ and thus

$$a^2 - b^2 d \equiv d \not\equiv 0 \mod 4$$

as d is square-free. The case where a is odd and b is even yields

$$a^2 - b^2 d \equiv a^2 \equiv 1 \mod 4.$$

So this shows that if a and b do not have the same parity then $x \notin \mathcal{O}_K$.

Lastly consider the case where both a and b are odd. Then we have that

$$a^2 - b^2 d \equiv 1 - d \mod 4.$$

So we see that in this case $x \in \mathcal{O}_K$ if and only if $d \equiv 1 \mod 4$. To summarize we see that

$$\mathcal{O}_K = \begin{cases} \{\frac{a}{2} + \frac{b}{2}\sqrt{d} : a, b \in \mathbb{Z} \text{ such that } a \equiv b \mod 2\} & \text{if } d \equiv 1 \mod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \mod 4. \end{cases}$$

$$= \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \mod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \mod 4. \end{cases}$$

We conclude by calculating the discriminant. First assume $d \equiv 1 \mod 4$. By the above, $1, \frac{1+\sqrt{d}}{2}$ is an integral basis of $\mathcal{O}_K$. So we have

$$d_K = \det\left(\begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}\right)^2 = d.$$

Second, let $d \equiv 2, 3 \mod 4$. In this case $1, \sqrt{d}$ is an integral basis of $\mathcal{O}_K$. Then

$$d_K = \det\left(\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}\right)^2 = 4d.$$

□

1.4 Ideals and Dedekind Rings

Let K be a number field and denote by $\mathcal{O}_K$ the ring of integers in K. In general, the ring of integers is not a unique factorization domain and hence also not a principle ideal domain. However, the ideals of $\mathcal{O}_K$ can be factored uniquely into prime ideals. The main aim of this section is to prove this for a larger class of rings, namely so called *Dedekind rings*.

Definition 1.49. A *Dedekind ring* is a noetherian normal integral domain of Krull dimension 1, i.e. every non-zero prime ideal is maximal.

We first show that the rings $\mathcal{O}_K$ are indeed Dedekind rings.

Proposition 1.50. *Let K be a number field and denote by $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in K. Then $\mathcal{O}_K$ is a Dedekind ring.*

Proof. We proved in Theorem 1.43 that every ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, thus it is also a finitely generated $\mathcal{O}_K$-module. This implies that $\mathcal{O}_K$ is noetherian. Furthermore we claim that the field of fractions of the ring $\mathcal{O}_K$ is the ring K. To see this, let $\alpha_1, \ldots, \alpha_n$ be an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$ whose existence is guaranteed by Theorem 1.43. So we have that $\mathcal{O}_K = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Furthermore by Proposition 1.42, we have that $\alpha_1, \ldots, \alpha_n$ is also an integral basis of L over K. Thus we have that

$$\mathrm{Quot}(\mathcal{O}_K) = \mathrm{Quot}(\mathrm{Z})(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) = K.$$

Then by Corollary 1.37 we have that $\mathcal{O}_K$ is integrally closed in K and so $\mathcal{O}_K$ is integrally closed in its field of fractions and thus is normal.

Recall that if $A \subset B$ is an integral ring extension, then the Krull dimension of A and B are equal. Thus $\dim(\mathcal{O}_K) = 1$ since $\dim(\mathbb{Z}) = 1$. □

For two ideals $\mathfrak{a}$ and $\mathfrak{b}$ we define

$$\mathfrak{a} + \mathfrak{b} := \{a + b \,:\, a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

and

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{n} a_i b_i \,:\, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

We usually write $\mathfrak{ab}$ instead of $\mathfrak{a} \cdot \mathfrak{b}$. Furthermore note that $\mathfrak{ab}$ is contained in $\mathfrak{a}$ as well as in $\mathfrak{b}$. The main aim of this subsection is to prove the following theorem.

Theorem 1.51. *Let $\mathcal{O}$ be a Dedekind ring. Then every non-trivial ideal $\mathfrak{a}$ of $\mathcal{O}$ has a decomposition*

$$\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$$

into prime ideals $\mathfrak{p}_i \subset \mathcal{O}$. This decomposition is unique up to reordering.

We first prove two lemmas.

Lemma 1.52. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}$. Then there are non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ with*

$$\mathfrak{a} \supset \mathfrak{p}_1 \ldots \mathfrak{p}_n.$$

Proof. To prove the statement by contradiction assume that the set $\mathscr{M}$ of ideals not satisfying this property is not empty. Since $\mathcal{O}$ is noetherian, the set $\mathscr{M}$ together with the inclusion of sets satisfies the assumption of Zorn's Lemma and so there is a maximal element $\mathfrak{a}$. The ideal $\mathfrak{a}$ can't be prime, since no element of $\mathscr{M}$ is prime. Hence there are elements $a_1, a_2 \notin \mathfrak{a}$ such that $a_1 a_2 \in \mathfrak{a}$. So consider the ideals $\mathfrak{a}_1 = \mathfrak{a} + (a_1)$ and $\mathfrak{a}_2 = \mathfrak{a} + (a_2)$ and note then that $\mathfrak{a} \subsetneq \mathfrak{a}_1$ and $\mathfrak{a} \subsetneq \mathfrak{a}_2$ but $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$. Since $\mathfrak{a}$ is a maximal element of $\mathscr{M}$, the ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are not an element of $\mathscr{M}$. Thus they contain a product of prime ideals. Since $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$, the ideal $\mathfrak{a}$ also contains a product of prime ideals. This is a contradiction to the assumption. □

Next denote by K the quotient field of $\mathcal{O}$ and for any prime ideal $\mathfrak{p} \subset \mathcal{O}$ we define

$$\mathfrak{p}^{-1} := \{x \in K \,:\, x\mathfrak{p} \subset \mathcal{O}\} \supset \mathcal{O}.$$

Lemma 1.53. *For any non-zero ideal $\mathfrak{a} \subset \mathcal{O}$ and for any prime ideal $\mathfrak{p} \subset \mathcal{O}$ we have that*

$$\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}.$$

Proof. We first claim that $\mathfrak{p}^{-1} \neq \mathcal{O}$. To see this choose some non-zero element $a \in \mathfrak{p}$. With the last lemma we can choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathcal{O}$ with r minimal such that

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}.$$

One of the ideals $\mathfrak{p}_i$ has to be contained in $\mathfrak{p}$, since otherwise we can choose $p_i \in \mathfrak{p}_i \backslash \mathfrak{p}$ with $p_1 \ldots p_r \in \mathfrak{p}$. Assume without loss of generality that $\mathfrak{p}_1 \subset \mathfrak{p}$ and by maximality of $\mathfrak{p}_1$ we conclude $\mathfrak{p}_1 = \mathfrak{p}$. Since r is minimal, we have that $\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\subset (a)$, so we can choose $b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r$ with $b \notin (a)$ or equivalently $a^{-1}b \notin \mathcal{O}$. On the other hand $b\mathfrak{p} = b\mathfrak{p}_1 \subset (a)$, which is again equivalent to $a^{-1}b\mathfrak{p} \subset \mathcal{O}$. So $a^{-1}b \in \mathfrak{p}^{-1}$ and this shows that $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Next let $\mathfrak{a}$ be an ideal in $\mathcal{O}$ with generators $\alpha_1, \ldots, \alpha_n$. We assume for a contradiction $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. So for any $x \in \mathfrak{p}^{-1}$ we have that

$$x\alpha_i = \sum_j a_{ij}\alpha_j$$

with $a_{ij} \in \mathcal{O}$. Denote $A = (x\delta_{ij} - a_{ij})$ and so $A(\alpha_1, \ldots, \alpha_n)^T = 0$. Thus $\det(A)\alpha_1 = \ldots = \det(A)\alpha_n = 0$ (This follows from Theorem 2.2. of [Neu07]). Since $\mathcal{O}$ is an integral domain, we conclude $\det(A) = 0$. This implies that x is a zero of the normed polynomial $f(X) = \det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$, in conclusion since $\mathcal{O}$ is integrally closed in K we have $x \in \mathcal{O}$. So we proved $\mathfrak{p}^{-1} = \mathcal{O}$, a contradiction to the first step. □

We now prove Theorem 1.51.

Proof. (of Theorem 1.51) We first prove existence by an analogous method to Lemma 1.52. Denote again by $\mathscr{M}$ the set of non-trivial ideals of $\mathcal{O}$ that do not have a decomposition into prime ideals and assume that $\mathscr{M}$ is not empty. So there is an element $\mathfrak{a} \in \mathscr{M}$ that is maximal with respect to inclusion. Let $\mathfrak{p}$ be a maximal ideal that strictly contains $\mathfrak{a}$. Using $\mathcal{O} \subset \mathfrak{p}^{-1}$ and $\mathfrak{a} \subset \mathfrak{p}$ we derive the chain of inclusions

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}.$$

Applying the last lemma twice, we see that $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$. The maximality of $\mathfrak{p}$ implies $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Furthermore, since $\mathfrak{a}$ is a maximal element in $\mathscr{M}$, the ideal $\mathfrak{a}\mathfrak{p}^{-1}$ has a decomposition into prime ideals, say

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

and so we conclude

$$\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}.$$

To prove uniqueness, recall that for a prime ideal $\mathfrak{p}$ the following property holds: If $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ then we have that $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$. So if we have two decompositions of the ideal $\mathfrak{a}$ into prime ideals

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n = \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_m,$$

then we have that $\mathfrak{q}_1 \dots \mathfrak{q}_m \subset \mathfrak{p}_1$ and so there is some $\mathfrak{q}_i \subset \mathfrak{p}_1$. Since $\mathfrak{q}_i$ is a maximal ideal we get $\mathfrak{q}_i = \mathfrak{p}_1$. Continuing this process, uniqueness of the decomposition into prime ideals follows. □

Definition 1.54. Let $\mathcal{O}$ be a Dedekind ring and denote by K the field of fractions of $\mathcal{O}$. A *fractional ideal* is a non-zero finitely generated $\mathcal{O}$-submodule of K. We denote by J_K the set of fractional ideals.

The next theorem states that the set J_K together with the multiplication of ideals forms a group. Thus J_K is called the *ideal group of* K.

Theorem 1.55. *Let $\mathcal{O}$ be a Dedekind ring and denote by K the field of fractions of $\mathcal{O}$. Then the set of fractional ideals J_K forms an abelian group together with the multiplication of ideals. The unit element is $(1) = \mathcal{O}$ and the inverse of a fractional ideal $\mathfrak{a}$ is*

$$\mathfrak{a}^{-1} = \{x \in K \,:\, x\mathfrak{a} \subset \mathcal{O}\}.$$

We first prove the following lemma.

Lemma 1.56. *For every fractional ideal $\mathfrak{a}$ of K there is some non-zero element $c \in \mathcal{O}$ such that $c\mathfrak{a} \subset \mathcal{O}$.*

Proof. By definition, $\mathfrak{a}$ is generated by elements $\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}$ for $a_i, b_i \in \mathcal{O}\backslash\{0\}$. So we have that $b_1 \dots b_n\mathfrak{a} \subset \mathcal{O}$. □

Proof. (of Theorem 1.55) The group operation is associative and commutative, since these properties hold for the multiplication in $\mathcal{O}$. Furthermore, we clearly have $\mathfrak{a}(1) = \mathfrak{a}$. Next, we note that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, then we have by Lemma 1.53 that $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$ and so $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Second, we consider an ideal $\mathfrak{a}$ in $\mathcal{O}$. This is a fractional ideal, since $\mathcal{O}$ is noetherian. By Theorem 1.51 we have a

decomposition into prime ideals $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n$ and we claim that $\mathfrak{b} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1}$ is equal to $\mathfrak{a}^{-1}$. The inclusion $\mathfrak{b} \subset \mathfrak{a}^{-1}$ follows by $\mathfrak{b}\mathfrak{a} = \mathcal{O}$. For the second inclusion consider an element $x \in K$ with $x\mathfrak{a} \subset \mathcal{O}$. So $x\mathfrak{a}\mathfrak{b} = x\mathcal{O} \subset \mathfrak{b}$ and this shows $x \in \mathfrak{b}$. So we proved $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}\mathfrak{b} = \mathcal{O}$ for any ideal $\mathfrak{a}$ in $\mathcal{O}$.

Using the last lemma, the general case where $\mathfrak{a}$ is a fractional ideal can be reduced to $\mathfrak{a}$ being an ideal in $\mathcal{O}$. More precisely, there is an element $c \in \mathcal{O}$ such that $c\mathfrak{a} \subset \mathcal{O}$ and hence $c^{-1}\mathfrak{a}^{-1}$ is an inverse of $c\mathfrak{a}$ in $\mathcal{O}$. This shows $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

Corollary 1.57. *The ideal group J_K is the free abelian group generated by the nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.*

Proof. We need to show that every fractional ideal $\mathfrak{a}$ can be written uniquely as a product

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$$

with $\nu_\mathfrak{p} \in \mathbb{Z}$ and $\nu_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$. This follows since every prime ideal is a quotient $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$, where $\mathfrak{b}$ and $\mathfrak{c}$ are two ideals of $\mathcal{O}$. Thus the statement is implied since every ideal of $\mathcal{O}$ can be written in a unique way as a product of prime ideals as provided by Theorem 1.51. □

With this in mind, we can define the so called *ideal class group* that measures how far the ring $\mathcal{O}$ is from being a principle ideal domain and thus also a unique factorization domain.

Definition 1.58. Let $\mathcal{O}$ be a Dedekind ring and denote by K the field of fractions of $\mathcal{O}$. We call a fractional ideal $\mathfrak{a}$ *principal* if it is of the form $\mathfrak{a} = (a) = a\mathcal{O}$ for $a \in K$. We denote by P_K the subgroup of the ideal group J_K consisting of the principal fractional ideals. The factor group

$$\mathrm{Cl}_K = J_K / P_K$$

is called the *ideal class group* or just the *class group* of the field K. The order of Cl_K is called the *class number* of K.

2 Gauss's Reciprocity Law

2.1 The Decomposition of Primes in $\mathcal{O}_K$

The aim of this subsection is to study the question whether an integer a is a quadratic residue for a prime p, i.e. whether the congruence

$$x^2 \equiv a \mod p$$

has a solution or not. We will study this question in the next subsection and first introduce some new terminology which will turn out to be useful towards.

Let K be a number field of degree n and $\mathcal{O}_K$ be its ring of integers. If $p \in \mathbb{Z}$ is a prime, then the ideal $p\mathcal{O}_K \subset \mathcal{O}_K$ does not have to be a prime ideal, but we have a decomposition

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}.$$

Definition 2.1. In the above setting, any of the $\mathfrak{p}_i$ is called a *prime divisor* of p. The exponent e_i is called the *ramification index*, and the degree of the field extension $f_i := [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ is called the *inertia degree* of $\mathfrak{p}_i$ over p.

Proposition 2.2. *(Fundamental identity) We have*

$$\sum_{i=1}^{r} e_i f_i = [K : \mathbb{Q}] = n.$$

We now simplify the above situation. We consider the case where $K = \mathbb{Q}(\theta)$ for some algebraic element θ with minimal polynomial $p(X) \in \mathbb{Z}[X]$. We define the *conductor* of $\mathcal{O}_K$ which is contained in $\mathbb{Z}[\theta]$ as

$$\mathcal{F} = \{\alpha \in \mathcal{O}_K \,:\, \alpha\mathcal{O}_K \subset \mathbb{Z}[\theta]\}.$$

Since $\mathcal{O}_K$ is a finitely generates $\mathbb{Z}$-module, we see that the conductor is non-empty.

Example 2.3. We consider the case $K = \mathbb{Q}(\sqrt{d})$ for d a non-square integer. We have seen that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{d+\sqrt{d}}{2}] & \text{if } d \equiv 1 \mod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \mod 4. \end{cases}$$

We claim that in any case, the conductor $\mathcal{F} = \mathbb{Z}[\sqrt{d}]$. In the case $d \equiv 2, 3 \mod 4$ this is clear as $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. For $d \equiv 1 \mod 4$, let $\alpha \in \mathcal{F}$. Then $\alpha = \alpha \cdot 1 \in \mathbb{Z}[\sqrt{d}]$ and so we see that

$$\mathcal{F} = \{n + m(\tfrac{d+\sqrt{d}}{2}) \,:\, n \in \mathbb{Z} \text{ and } m \in 2\mathbb{Z}\} = \mathbb{Z}[\sqrt{d}].$$

Proposition 2.4. *Let $p \in \mathbb{Z}$ be a prime number and assume that $p\mathcal{O}_K$ is relatively prime to the conductor $\mathcal{F}$ of $\mathbb{Z}[\theta]$, and let*

$$\overline{p}(X) = \overline{p}_1(X)^{e_1} \cdot \ldots \cdot \overline{p}_r(X)^{e_r}$$

be the factorization of the polynomial $\overline{p}(X) = p(X) \mod p$ into irreducible polynomials $\overline{p}_i(X) = p_i(X) \mod p$ with all $p_i(X) \in \mathbb{Z}[X]$ monic. Then

$$\mathfrak{p}_i = p\mathcal{O}_K + p_i(\theta)\mathcal{O}$$

for $i = 1, \dots r$. The inertia degree f_i of $\mathfrak{p}_i$ is the degree of $\overline{p}_i(X)$ and one has

$$\mathfrak{p} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}.$$

2.2 The Splitting of Primes

Notations are as in the last subsection.

Definition 2.5. We say that the prime $p \in \mathbb{Z}$ *splits completely* in K if in the decomposition

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

we have $r = n = [K : \mathbb{Q}]$ and so $e_i = f_i = 1$ for all $r = 1, \dots, n$. The prime number p is called non-split if $r = 1$, i.e. there is only a single prime ideal of L over p.

The prime ideal $\mathfrak{p}_i$ in the decomposition $p\mathcal{O}_K = \prod_{i=1}^{e_i}$ is called *unramified* over $\mathbb{Z}$ of $e_i = 1$ and the residue class field extension $\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}$ is separable. If not, it is called *ramified* and totally ramified if furthermore $f_i = 1$.

We next introduce the *Legendre symbol*. Let p be a prime number and let $a \in \mathbb{Z}$ so that $\gcd(a, p) = 1$. We then define $\left(\frac{a}{p}\right) = 1$ or -1 according as $x^2 \equiv a \mod p$ has or does not have a solution.

Lemma 2.6. *The Legendre symbol satisfies the following properties:*

1. *For a and b integers with $\gcd(a, p) = 1 = \gcd(b, p)$ we have*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

2. *For $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$,*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

3. *We have,*

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) = 0.$$

4. *For $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$,*

$$\left(\frac{a}{p}\right) = \left(\frac{a^{-1}}{p}\right)$$

Proof. We consider the group of units $\mathbb{F}_p^*$ and recall that it is cyclic of order $p - 1$. Thus the subgroup $\mathbb{F}_p^{*2}$ has index 2 and so $\mathbb{F}_p^*/\mathbb{F}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z}$. This shows 1. and 2. and 3. The last claim follows as $b^2 \equiv a \mod p$ if and only if $b^{-2} \equiv a \mod p$. □

Proposition 2.7. *For a square-free a and $(p, 2a) = 1$, we have the equivalence*

$$\left(\frac{a}{p}\right) = 1 \quad \Longleftrightarrow \quad p \text{ is totally split in } \mathbb{Q}(\sqrt{a}).$$

Proof. By assumption $p \neq 2$ and so $p\mathcal{O}_K$ is relatively prime to the conductor $\mathcal{F} = \mathbb{Z}[\sqrt{a}]$. Hence we can apply Proposition 2.4, to see that p splits totally in $\mathbb{Q}(\sqrt{a})$ if and only if the polynomial $X^2 - a \mod p$ decomposes into linear factor.

If for $\alpha, \beta \in \mathbb{F}_p$ we have $X^2 - a = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta$ then $\beta = -\alpha$ and $\alpha\beta = -\alpha^2$. This calculation shows that $X^2 - a \mod p$ decomposes into linear factor if and only if $\left(\frac{a}{p}\right) = 1$. □

Example 2.8. By Proposition 2.7 we see that 11 is split in $\mathbb{Q}(\sqrt{5})$ but $3, 5$ and 7 are non-split.

2.3 Gauss's Reciprocity Law

Theorem 2.9. *(Gauss's Reciprocity Law) Let ℓ and p be two distinct odd primes, then*

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}.$$

We defer the proof for a moment, in order to prove a useful lemma.

Lemma 2.10. *For p any odd prime,*

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \quad \text{and} \quad \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}.$$

Proof. As $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$ and as $p \neq 2$ we have that $\left(\frac{-1}{p}\right) = (-1^{\frac{p-1}{2}})$.

To calculate $\left(\frac{2}{p}\right)$, we work in the Gaussian integers $\mathbb{Z}[i]$. As $(1 + i) = 2i$ we have

$$(1+i)^p = (1+i)((1+i)^2)^{\frac{p-1}{2}} = (1+i)2^{\frac{p-1}{2}} i^{\frac{p-1}{2}}.$$

As $(1 + i)^p \equiv 1 + i^p \mod p$ and $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \mod p$, it follows that

$$\left(\frac{2}{p}\right)(1+i)i^{\frac{p-1}{2}} \equiv 1 + i(-1)^{\frac{p-1}{2}} \mod p.$$

If $\frac{p-1}{2}$ is even, then the above equation simplifies to

$$\left(\frac{2}{p}\right)(1+i)(-1)^{\frac{p-1}{4}} \equiv 1 + i \mod p$$

and so $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} \mod p$. In this case $\frac{p+1}{2}$ is odd and as $\frac{p^2-1}{8} = \frac{p-1}{4}\frac{p+1}{2}$ we conclude that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. A similar calculation applies to the case where $\frac{p-1}{2}$ is odd. □

Proof. (of Theorem 2.9) We now work in the ring $\mathbb{Z}[\zeta]$, where ζ is a primitive ℓ-th root of unity. We consider the Gauss sum

$$\tau = \sum_{a \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{a}{\ell}\right) \zeta^a.$$

A calculation yields

$$\begin{aligned}
\left(\frac{-1}{\ell}\right) \tau^2 &= \sum_{a,b \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{-ab}{\ell}\right) \zeta^{a+b} \\
&= \sum_{a,b \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{ab}{\ell}\right) \zeta^{a-b} \\
&= \sum_{a,b \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{ab^{-1}}{\ell}\right) \zeta^{a-b} \\
&= \sum_{b,c \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{c}{\ell}\right) \zeta^{bc-b} \\
&= \sum_{c \neq 1} \left(\frac{c}{\ell}\right) \sum_{b \in (\mathbb{Z}/\ell\mathbb{Z})^*} \zeta^{b(c-1)} + \sum_{b \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{1}{\ell}\right),
\end{aligned}$$

where we made in the third fourth line a change of variables given by $c = ab^{-1}$. By 3. of 2.6 and as $\left(\frac{1}{\ell}\right) = 1$, we derive $\sum_{c \neq 1} \left(\frac{c}{\ell}\right) = -1$. As $\xi = \zeta^{c-1}$ is again an ℓ-th root of unity and as $\sum_{b \in (\mathbb{Z}/\ell\mathbb{Z})^*} \zeta^{b(c-1)} = \xi + \xi^2 + \ldots + \xi^{\ell-1} = -1$ we conclude

$$\left(\frac{-1}{\ell}\right) \tau^2 = (-1)(-1) + \ell - 1 = \ell$$

or equivalently $\tau^2 = \left(\frac{-1}{\ell}\right) \ell$

As $\left(\frac{\ell}{p}\right) \equiv \ell^{\frac{p-1}{2}} \mod p$ and $\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}}$, we conclude

$$\begin{aligned}
\tau^p &\equiv \tau(\tau^2)^{\frac{p-1}{2}} \mod p \\
&\equiv \tau \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}} \ell^{\frac{p-1}{2}} \mod p \\
&\equiv \tau(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \left(\frac{\ell}{p}\right) \mod p.
\end{aligned}$$

On the other hand one has

$$\tau^p \equiv \sum_a \left(\frac{a}{\ell}\right) \zeta^{ap} \equiv \left(\frac{p}{\ell}\right) \sum_a \left(\frac{a}{\ell}\right) \zeta^{ap} \equiv \left(\frac{p}{\ell}\right) \tau \mod p,$$

so that

$$\tau \left(\frac{p}{\ell}\right) \equiv \tau(-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} \left(\frac{\ell}{p}\right) \mod p$$

and so multiplying by τ^{-1} and $\left(\frac{\ell}{p}\right)$ the claim follows. □

3 Lattices

3.1 Lattices in Vector Spaces

Throughout this section denote by V an n-dimensional vector space over $\mathbb{R}$.

Definition 3.1. A *lattice* Γ in the vector space V is a discrete subgroup of V of the form

$$\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n,$$

where $v_1, \ldots v_n$ form a basis of V.

We aim at giving an equivalent characterization of lattices in V. In order to achieve this, we first describe discrete subgroups of V in a uniform way.

Theorem 3.2. *A subgroup Γ of V is discrete if and only if*

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

where $v_1, \ldots, v_m$ are linearly independent vectors and $m \leq n$.

Proof. First assume that Γ is of the above form. Let $\gamma = z_1v_1 + \ldots + z_mv_m \in \Gamma$ with $z_1, \ldots, z_m \in \mathbb{Z}$. Then the open set

$$\{x_1v_1 + \ldots + x_nv_m \,:\, |x_i - z_i| < \frac{1}{2} \text{ for } 1 \leq i \leq m\}$$

contains γ but does not contain any other element of Γ. Hence Γ is a discrete subgroup.

Conversely assume that Γ is a discrete subgroup. Denote by V_0 the vector space generated by Γ. So there is a basis $v_1, \ldots, v_m$ of V_0 which is contained in Γ. Next we consider the following subgroup

$$\Gamma_0 = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m \subset \Gamma$$

and note that, as Γ is abelian, the quotient Γ/Γ_0 forms an abelian group. As a preliminary step, we show that the group Γ/Γ_0 is finite. Therefore choose a set of representatives $\gamma_i \in \Gamma/\Gamma_0$ for $i \in I$, where I is some index set. We denote

$$\Phi = \{x_1v_1 + \ldots + x_mv_m \,:\, 0 \leq x_i < 1 \text{ for } 1 \leq i \leq m\}$$

and observe that $\Phi + \Gamma_0 = V_0$. So we can write

$$\gamma_i = \mu_i + \gamma_i^0$$

with $\mu_i \in \Phi$ and $\gamma_i^0 \in \Gamma_0$. Consequently $\mu_i = \gamma_i - \gamma_i^0 \in \Gamma \cap \Phi$. This implies that the index set I must be finite since Γ is discrete and Φ is bounded.

Denote by d the order of Γ/Γ_0. Hence there are elements $\gamma_1, \ldots, \gamma_d \in \Gamma$ such that

$$\Gamma = (\gamma_1 + \Gamma_0) + \ldots + (\gamma_d + \Gamma_0).$$

As Γ/Γ_0 is a group of order d, every element has an order divisible by d. We conclude $d\gamma_i \in \Gamma_0$ and so

$$d\Gamma = (d\gamma_1 + \Gamma_0) + \ldots + (d\gamma_d + \Gamma_0) \subset \Gamma_0$$

or equivalently

$$\Gamma \subset \frac{1}{d}\Gamma_0 = \mathbb{Z}\frac{v_1}{d} + \ldots + \mathbb{Z}\frac{v_m}{d}.$$

The last relation shows that Γ is a finitely generated abelian group. Hence the fundamental theorem of finitely generated abelian groups shows that $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ for $v_1, \ldots, v_m$ linearly independent vectors in V. □

With the help of this we can prove the following two corollaries, that characterize lattices in V and in the special case $V = \mathbb{R}^n$.

Corollary 3.3. *A subgroup Γ in V is a lattice if and only if Γ is discrete and generates V.*

Proof. This follows immediately from the last theorem and the definition of a lattice. □

Corollary 3.4. *A subgroup of $\mathbb{R}^n$ is a lattice if and only if Γ is discrete and the quotient $\mathbb{R}^n/\Gamma$ is compact.*

Proof. (of Theorem 3.4) First assume that $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$ is a lattice in $\mathbb{R}^n$. Then Γ is by the last theorem discrete. To see that $\mathbb{R}^n/\Gamma$ is compact, we note that we have a homeomorphism

$$\mathbb{T}^n \to \mathbb{R}^n/\Gamma, \qquad (t_1, \ldots, t_n) \mapsto t_1v_1 + \ldots + t_nv_n,$$

where $\mathbb{T}^n := \mathbb{R}^n/\mathbb{Z}^n \cong [0,1)^n$. Thus $\mathbb{R}^n/\Gamma$ is compact, as $\mathbb{T}^n$ is.

For the other direction, we note that if $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ for $m < n$, then we have analogously to the first part a homeomorphism

$$\mathbb{T}^m \times \mathbb{R}^{n-m} \to \mathbb{R}^n/\Gamma \qquad (t_1, \ldots, t_n) \mapsto t_1v_1 + \ldots + t_mv_m + t_{m+1} + \ldots + t_n.$$

So we conclude that $\mathbb{R}^d/\Gamma$ is not compact. □

In the following we consider the n-dimensional real vector space V with an inner product $\langle \cdot, \cdot \rangle$, elevating the vector space V to a euclidean vector space. We want to study V together with a measure. The natural choice in this setting is to take the Haar measure on V that gives measure 1 to the cube spanned by any orthonormal basis of V with respect to the inner product. This measure defines the *volume* of any set X in $(V, \langle \cdot, \cdot \rangle)$.

Let next $v_1, \ldots, v_n$ be some vectors in V and consider the set

$$\Phi = \{x_1v_1 + \ldots + x_nv_n \,:\, 0 \leq x_i < 1 \text{ for } 1 \leq i \leq n\}.$$

The volume of Φ is then

$$\mathrm{vol}(\Phi) = |\det A|,$$

where $A = (a_{ij})$ is the transformation matrix from an orthonormal basis $e_1, \ldots, e_n$ to the vectors $v_1, \ldots, v_n$, i.e. $Av_i = \sum_{k=1}^n a_{ik}e_k$. Note that

$$(\langle v_i, v_j \rangle) = (\sum_{k,l} a_{ik}a_{jl}\langle e_i, e_j \rangle) = (\sum_k a_{ik}a_{jk}) = AA^t.$$

Hence we can also write

$$\mathrm{vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{\frac{1}{2}}.$$

With all this in mind we define the volume of a lattice.

Definition 3.5. Let V be a n-dimensional euclidean vector space and

$$\Gamma = v_1\mathbb{Z} + \ldots + v_n\mathbb{Z}$$

be a lattice in V. Then we define the *volume* of Γ to be

$$\mathrm{vol}(\Gamma) = |\det(\langle v_i, v_j\rangle)|^{\frac{1}{2}} = \mathrm{vol}(\Phi).$$

We furthermore call Φ the cube spanned by Γ. If $\mathrm{vol}(\Gamma) = 1$, we call the lattice *unimodular*.

Recall that a set $X \subset V$ is called centrally symmetric if for all $x \in X$ we also have $-x \in X$.

Theorem 3.6. *(Minkowski's Lattice Theorem) Let V be a n-dimensional euclidean vector space and Γ be a lattice in V. Furthermore assume that X is a centrally symmetric convex set in V and assume that*

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

Then X contains a nonzero element of Γ.

Proof. We claim that there are distinct elements γ_1 and γ_2 of Γ such that

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

Assuming this we have $x_1, x_2 \in X$ with

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$$

or equivalently using convexity of X

$$\frac{1}{2}x_1 - \frac{1}{2}x_2 = \gamma_2 - \gamma_1 \in (X \cap \Gamma)\backslash\{0\}.$$

To prove the claim assume that the sets $\frac{1}{2}X + \gamma$ are distinct for all $\gamma \in \Gamma$. Thus

$$\begin{aligned}
\mathrm{vol}(\Phi) &\geq \sum_{\gamma\in\Gamma} \mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right) \\
&\geq \sum_{\gamma\in\Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) \\
&= \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{vol}(X),
\end{aligned}$$

where we used in the second line translation invariance of the Haar measure and in the third the fact that $\Phi - \gamma$ with $\gamma \in \Gamma$ covers V. Thus we derived a contradiction to the assumption $\mathrm{vol}(X) > 2^n\mathrm{vol}(\Gamma)$. □

Remark. The bound in the above theorem is sharp. More precisely for the lattice $\Gamma = v_1\mathbb{Z} + \ldots + v_n\mathbb{Z}$ note that the set

$$\{x_1v_1 + \ldots + x_nv_n \,:\, -1 < x_i < 1 \text{ for } 1 \leq i \leq n\}$$

is convex centrally symmetric and of volume $2^n\mathrm{vol}(\Gamma)$ but does not contain any nonzero element of Γ.

Corollary 3.7. *Consider $\mathbb{R}^n$ with the standard inner product and let Γ be a lattice in $\mathbb{R}^n$. Then there is a nonzero element of Γ with length less that $r_n \mathrm{vol}(\Gamma)$ for some constant r_n only depending on n.*

Proof. We show that we can choose $r_n = 2\sqrt{n}$. To apply Theorem 3.6, choose the centrally symmetric and convex set

$$X = \{x \in \mathbb{R}^d : x_i \in (-2\mathrm{vol}(\Gamma)^{\frac{1}{n}}, 2\mathrm{vol}(\Gamma)^{\frac{1}{n}}) \text{ for } 1 \leq i \leq n\}$$

which has

$$\mathrm{vol}(X) = 4^n \mathrm{vol}(\Gamma) > 2^n \mathrm{vol}(\Gamma)$$

and hence X contains a nonzero element $\gamma \in \Gamma$. Note that the length of γ can be bounded by

$$||\gamma||_2 < \sqrt{4\mathrm{vol}(\gamma)^{\frac{2}{n}} + \ldots 4\mathrm{vol}(\gamma)^{\frac{2}{n}}} = 2\sqrt{n} \cdot \mathrm{vol}(\Gamma).$$

□

3.2 The Space of Unimodular Lattices

In this section we reduce to the case $V = \mathbb{R}^n$ together with the standard inner product. Consider a lattice

$$\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$$

in $\mathbb{R}^n$ for $v_1, \ldots, v_n \in \mathbb{R}^n$ linearly independent vectors. Write g for the matrix whose columns consist of the vector $v_1, \ldots, v_n$, i.e.

$$g = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_3 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{R}).$$

Then

$$\Gamma = \mathbb{Z}^n g,$$

where we view $\mathbb{Z}^n$ as column vectors. Thus we can view the space of lattices as the orbit of the vector $\mathbb{Z}^n$ with respect to the right action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$. Note that the volume of Γ is equal to the volume of $[0,1)^n g$ and hence

$$\mathrm{vol}(\Gamma) = |\det(g)|.$$

We denote by X_n the space of unimodular lattices in $\mathbb{R}^n$, i.e. of lattices of volume 1. By the above, X_n is the orbit of $\mathbb{Z}^n$ for the $\mathrm{SL}_n(\mathbb{R})$ left action $\mathbb{R}^n$. We observe that the stabilizer of this action has the following form.

Lemma 3.8. *The stabilizer of $\mathbb{Z}^d$ is*

$$\mathrm{Stab}_{\mathrm{SL}_n(\mathbb{R})}(\mathbb{Z}^d) = \mathrm{SL}_n(\mathbb{Z}).$$

Proof. If $g \in \mathrm{SL}_n(\mathbb{R})$ satisfies $\mathbb{Z}^n g = \mathbb{Z}^n$, then clearly every coefficient of g is an integer so $g \in \mathrm{SL}_n(\mathbb{Z})$. Conversely if $g \in \mathrm{SL}_n(\mathbb{Z})$, then the lattice $\mathbb{Z}^n g$ satisfies $\mathbb{Z}^n g \subset \mathbb{Z}^n$ and has volume 1. Thus $g\mathbb{Z}^n = \mathbb{Z}^n$. □

This lemma shows that we can write the space of unimodular lattices as

$$X_n = \mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R}).$$

By transporting the topological structure on $\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})$ to X_n we can view the space X_n as a topological space.

We conclude this section by characterizing compact sets in X_n. In order to achieve this, we consider for any $\Gamma \subset \mathbb{R}^n$ a lattice the number

$$\lambda(\Gamma) = \min\{r \,:\, \Gamma \text{ contains a non-trivial vector of length } \leq r\}.$$

Theorem 3.9. *(Mahler's compactness criterion) A subset $C \subset X_n$ has compact closure if and only if they are uniformly discrete, i.e. there is some $\delta > 0$ such that $\lambda(\Gamma) \geq \delta$ for all $\Gamma \in C$.*

Proof. Let $K \subset X_n$ be compact and assume for a contradiction that K is not uniformly discrete. Hence there are lattices $\Gamma_n \in K$ with

$$\lambda(\Gamma_n) \leq \frac{1}{n}$$

for all n. By compactness there is some $\Gamma \in X_n$ such that $\Gamma_n \to \Gamma$. As $\lambda(\Gamma)$ depends continuously on Γ this contradicts the assumption that $\lambda(\Gamma_n) \leq \frac{1}{n}$ for all n.

Assume conversely that $K \subset X_n$ be uniformly discrete and let $\Gamma \in K$. We show by induction that we can find a basis of vectors $b_1, \ldots, b_n \in \Gamma$ that belong to a given ball of radius depending on δ. First note that the case $n = 1$ is clear.

Next assume $n \geq 2$ and assume that the claim is proven for $(n-1)$. Choose $b_1 \in \Gamma$ with the property that

$$||b_1|| = \lambda(\Gamma) \geq \delta.$$

As b_1 is the smallest vector in Γ note that we can bound the covolume of Γ from the volume of $B_{||b_1||}(0)$. As Γ is unimodular, we that have a constant C_d only depending on the dimension d such that $||b_1|| \leq C_d$. Denote by W the orthogonal complement of $\mathbb{R}b_1$ with respect to the standard inner product of $\mathbb{R}^n$ and by $\pi : \mathbb{R}^d \to W$ the canonical projection. Then

$$\Gamma_W = \pi_W(\Gamma)$$

is a $(d-1)$-dimensional lattice, which doesn't have to be unimodular but has covolume $\frac{1}{||b_1||}$. So after rescaling we may assume that Γ_W is unimodular. By the inductive hypothesis we can find a basis we have a suitable basis for Γ_W that can be lifted to a suitable basis for Γ. □

Corollary 3.10. *For $\delta > 0$ any set of the form*

$$X_n(\delta) = \{\Gamma \in X_n \,:\, \lambda(\Gamma) \geq \delta\}$$

is compact.

Proof. This follows from Theorem 3.9. □

3.3 Lattices in Topological Groups and Haar Measures

In this subsection we generalize the notion of a lattice to a more general setting. In order to discuss this properly we first discuss discrete subgroups and Haar measures.

Throughout this section we consider by G a locally compact, σ-compact metric group G with a left invariant metric d_G on G. If Γ is a discrete subgroup we denote $X := \Gamma\backslash G$. We say that X is a *locally homogeneous space*. The metric d_G descends to a metric on X defined for $g_1, g_2 \in G$ as

$$d_X(\Gamma g_1, \Gamma g_2) = \inf_{\gamma_1,\gamma_2\in\Gamma} d_G(\gamma_1 g_1, \gamma_2 g_2) = \inf_{\gamma\in\Gamma} d(\gamma g_1, g_2).$$

For $g \in G$, we write $B_r^G(g)$ and $B_r^X(\Gamma g)$ for the metric r-ball in G and respectively X.

Definition 3.11. A *left Haar measure* on a topological group G is a Borel measure μ that satisfies the following three properties:

1. $\mu(K) < \infty$ for any compact subset $K \subset G$.
2. $\mu(O) > 0$ for any open subset $O \subset G$.
3. $\mu(gB) = \mu(B)$ for any $g \in G$ and measurable $B \subset G$.

A *right Haar measure* is defined accordingly.

Theorem 3.12. *Any metric, σ-compact and locally compact topological group G has a left (or right) Haar measure, which is unique up to scalar multiples.*

Proof. For a proof see [EW18] Chapter 10. □

Proposition 3.13. *Let G be a locally compact topological group with left (or right) Haar measure μ. Then G is compact if and only if μ is finite.*

Proof. If G is compact, then by definition of a Haar measure we conclude $\mu(G) < \infty$. Let conversely G be a topological group with finite left (or right) Haar measure μ. Assume that G is not compact and let U be a compact neighborhood of the identity element $e \in G$. Then we can cover G by infinitely many disjoint translates of U an conclude that the Haar measure on G is not finite. □

Definition 3.14. We call a group G unimodular if any left Haar measure is also a right Haar measure and any right Haar measure is also a left Haar measure.

Definition 3.15. Let $\Gamma \leq G$ be a discrete subgroup and write $X = \Gamma\backslash G$. A *fundamental domain* for X is a measurable subset $F \subset G$ with the property that

$$G = \bigsqcup_{\gamma\in\Gamma} \gamma F.$$

Write

$$\pi_X : G \to X$$

for the natural projection.

Proposition 3.16. *For any locally homogeneous space X there exists a fundamental domain. Moreover any two fundamental domains of X have the same measure.*

Proof. Can be found in Page 10 and 11 of [EW]. □

Given a fundamental domain F for X, we thus define a measure μ_X on X by

$$\mu_X(B) = \mu(\pi_X^{-1}(B) \cap F),$$

where μ is a left Haar measure on G.

Proposition 3.17. *Then the following properties are equivalent:*

1. *There exists a G-invariant probability measure on X.*
2. *There is a fundamental domain for X that has finite measure with respect to any left invariant Haar measure.*
3. *There is a fundamental domain for X that has finite measure with respect to any right invariant Haar measure and any right Haar measure is left Γ-invariant.*

If any of these conditions hold, the group G is unimodular.

Definition 3.18. A discrete subgroup $\Gamma \leq G$ is called a *lattice* if any of the three equivalent conditions of the Proposition 3.17 hold. In particular, X admits a G-invariant probability measure.

Corollary 3.19. *If a G admits a lattice, then G is unimodular.*

Proof. This follows from Proposition 3.17. □

3.4 Lattices for Unipotent Subgroups

We denote the upper triangular group

$$\mathbb{U}_n = \left\{ \begin{pmatrix} 1 & * & * & \dots & * \\ & 1 & * & \dots & * \\ & & & \ddots & \vdots \\ & & & & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_n(\mathbb{R})$$

with the Lie algebra of strict upper triangular matrices

$$\mathfrak{n} = \left\{ \begin{pmatrix} 0 & * & * & \dots & * \\ & 0 & * & \dots & * \\ & & & \ddots & \vdots \\ & & & & 0 \end{pmatrix} \right\} \subset \mathfrak{sl}_n(\mathbb{R}).$$

We call a subgroup $G < \mathrm{SL}_d(\mathbb{R})$ *unipotent* if there is some $g \in \mathrm{SL}_n(\mathbb{R})$ such that gGg^{-1} is a subgroup of $\mathbb{U}_n$.

Recall furthermore that a subspace V of $\mathbb{R}^n$ is called *rational*, if there is a basis consisting of vectors from $\mathbb{Q}^n$.

We are now ready to prove the next theorem, which gives us a large class of examples of lattices and describes them in a suitable manner.

Theorem 3.20. *Let $G \leq \mathrm{SL}_n(\mathbb{R})$ be a ℓ-dimensional connected unipotent subgroup whose Lie algebra $\mathfrak{g}$ is a rational subspace of $\mathfrak{sl}_d(\mathbb{R})$. Then*

$$G(\mathbb{Z}) = G \cap \mathrm{SL}_d(\mathbb{Z})$$

is a cocompact lattice in G. Furthermore, there exists a Mal'cev basis $v_1, \ldots, v_\ell \in \mathfrak{g} \cap \mathfrak{sl}_d(\mathbb{Q})$ (see below for a definition).

In the setting of Theorem 3.20 we call vectors $v_1, \ldots, v_\ell \in \mathfrak{g} \cap \mathfrak{sl}_d(\mathbb{Q})$ are called a *Mal'cev basis* if we have that

$$\begin{aligned} G(\mathbb{Z}) &= \{\exp(k_1 v_1)\exp(k_2 v_2)\ldots\exp(k_\ell v_\ell) \,:\, k_1, \ldots, k_\ell \in \mathbb{Z}\} \\ G &= \{\exp(s_1 v_1)\exp(s_2 v_2)\ldots\exp(s_\ell v_\ell) \,:\, s_1, \ldots, s_\ell \in \mathbb{R}\} \end{aligned}$$

and if

$$F = \{\exp(s_1 v_1)\exp(s_2 v_2)\ldots\exp(s_\ell v_\ell) \,:\, s_1, \ldots, s_\ell \in [0,1)\}$$

is a fundamental domain for $G(\mathbb{Z})$ in G.

Proof. Denote by $\mathfrak{g}$ the Lie algebra of G. Then by assumption $\mathfrak{g}$ is conjugated to a a subalgebra of $\mathfrak{n}$ and hence $\mathfrak{g}$ nilpotent and the exponential map is given explicitly for $v \in \mathfrak{g}$ by

$$\exp(v) = I + v + \frac{1}{2}v^2 + \ldots + \frac{1}{(d-1)!}v^{d-1}$$

and hence is a polynomial on $\mathfrak{g}$ and the logarithm is thus given for $g \in G$ by

$$\log(g) = g - I - \frac{1}{2}(g-I)^2 + \ldots + (-1)^d \frac{1}{d-1}(g-I)^{d-1}$$

and hence exists for all g. This shows that the Lie group exponential is a diffeomorphism. All this allows us to define a group structure on $\mathfrak{g}$ given by

$$v * w = \log(\exp(v)\exp(w))$$

for $v, w \in \mathfrak{g}$ such that the exponential map can be viewed as an isomorphism of Lie groups.

Consider $\mathfrak{g}_1 = [\mathfrak{g}, \mathfrak{g}]$ and note that

$$[\mathfrak{g}_1, \mathfrak{g}] \subset [\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}_1$$

and hence $\mathfrak{g}_1$ is a Lie ideal. Denote by G_1 the normal Lie subgroup of G associated to $\mathfrak{g}_1$. Thus G/G_1 is an abelian subgroup with Lie algebra $\mathfrak{g}/\mathfrak{g}_1$. As $\mathfrak{g}_1 * \mathfrak{g}_1 \subset \mathfrak{g}$, we conclude that the group G/G_1 can be identified with $\mathfrak{g}/\mathfrak{g}_1$ via the exponential map.

Finish later... □

4 Class Numbers and Units

4.1 Minkowski Theory

Let K be a number field of degree n and let $\mathcal{O}_K$ be the ring of integers of K. Denote by

$$H := \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$$

the set of field homomorphisms from K to the algebraically closed field $\mathbb{C}$ that are fix $\mathbb{Q}$. Recall that the set H has by Proposition 1.20 the cardinality n. Throughout this subsection we write τ for elements of H. If $\tau \in H$, we write $\overline{\tau}$ for the complex conjugate of τ, which is again a field homomorphism. We write for r the number of totally real embeddings $\tau \in H$ and for $2s$ the number of complex embeddings (see below for a more precise discussion). The aim of this section is to prove the following theorem, which will turn out to be essential in the proof of the finiteness of the class number.

Theorem 4.1. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Let $c_\tau > 0$ for $\tau \in H$ be a collection of real numbers with $c_\tau = c_{\overline{\tau}}$ such that*

$$\prod_{\tau \in H} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

Then there is a nonzero element $a \in \mathfrak{a}$ with

$$|\tau a| < c_\tau$$

for all $\tau \in H$.

This statements resembles Minkowski's Lattice Theorem, which was proved in section 2.1, in the following way: We are given a certain *discrete* set and want to conclude that any large enough set intersects the discrete set non-trivially. The strategy of proof for Theorem 4.1 is to exploit this yet vague connection. More precisely, we aim at associating to each number field K, a euclidean real vector space $K_{\mathbb{R}}$ in a way such that we can associate to ideals of $\mathcal{O}_K$ lattices in that vector space $K_{\mathbb{R}}$. After having constructed this connection between ideals and lattices, Theorem 4.1 follows by applying Minkowski's Lattice Theorem.

In pursuit of the above outlined strategy we first consider the complex vector space

$$K_{\mathbb{C}} = \prod_{\tau \in H} \mathbb{C}$$

together with the hermitian scalar product

$$\langle (x_\tau), (y_\tau) \rangle = \sum_{\tau \in H} x_\tau \overline{y}_\tau.$$

Furthermore denote

$$j : K \longrightarrow K_{\mathbb{C}}, \qquad a \longmapsto (\tau a)_{\tau \in H}$$

and

$$F : K_{\mathbb{C}} \longrightarrow K_{\mathbb{C}}, \qquad (x_\tau) \longmapsto (\overline{x}_{\overline{\tau}})_{\tau \in H}.$$

Note that

$$\langle F(x_\tau), F(y_\tau)) = \sum_{\tau \in H} \overline{x}_{\overline{\tau}} y_{\overline{\tau}} = \overline{\langle (x_\tau), (y_\tau) \rangle}.$$

The vector space we are interested in is

$$K_{\mathbb{R}} = \{(x_\tau) \in K_{\mathbb{C}} \,:\, F(x_\tau) = (x_\tau)\},$$

i.e. the vector space of F-invariant elements. On $K_{\mathbb{R}}$ the hermitian scalar product restricts to a real scalar product since

$$\overline{\langle (x_\tau), (y_\tau) \rangle} = \langle F(x_\tau), F(y_\tau) \rangle = \langle (x_\tau), (y_\tau) \rangle$$

for any $(x_\tau), (y_\tau) \in K_{\mathbb{R}}$. Thus $K_{\mathbb{R}}$ together with $\langle \cdot, \cdot \rangle$ forms a euclidean vector space.

In the following want to find an isomorphism between $K_{\mathbb{R}}$ and $\mathbb{R}^n$ in order to make volume calculations in $K_{\mathbb{R}}$ simpler. We proceed by decomposing the set H into a real and complex part. We write

$$R = \{\rho_1, \ldots, \rho_r\} \subset H$$

for the homomorphisms $\rho \in H$ with $\rho(K) \subset \mathbb{R}$ and note that the complement

$$H \backslash R = \{\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s\}$$

consists of pairs of field homomorphisms. Denote by

$$C = \{\sigma_1, \ldots, \sigma_s\}$$

and by

$$\overline{C} = \{\overline{\sigma}_1, \ldots, \overline{\sigma}_s\}.$$

So we decomposed

$$H = R \cup C \cup \overline{C},$$

where $|R| = r$ and $|C| = |\overline{C}| = s$.

Finally consider on $\mathbb{R}^n = \mathbb{R}^{r+2s}$ the scalar product

$$(x, y) = \sum_\tau \alpha_\tau x_\tau y_\tau,$$

where $\alpha_\tau = 1$ if $\tau \in R$ is field homomorphism with image in $\mathbb{R}$ and $\alpha_\tau = 2$ if $\tau \in H \backslash R$. We then have the following isomorphism.

Proposition 4.2. *The map between the two euclidean vector spaces*

$$f : K_{\mathbb{R}} \longrightarrow \mathbb{R}^n = \mathbb{R}^{r+2s}, \qquad (z_\tau) \longmapsto (x_\tau),$$

where $x_\rho = z_\rho$ if $\rho \in R$ and $x_\sigma = \mathrm{Re}(z_\sigma), x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma)$ if $\sigma \in C$, is an isometric isomorphism of vector spaces.

Proof. It is clear that f is a vector space homomorphism. To see that f is injective choose, recall $K_{\mathbb{R}}$ consists of elements with $\overline{z}_{\overline{\tau}} = z_\tau$. Surjectivity of f follows from the same reason.

To prove that f is isometric, choose elements $z = (z_\tau) = (x_\tau + iy_\tau)$ and $z' = (z'_\tau) = (x'_\tau + iy'_\tau)$ and note that

$$z_\rho \overline{z}'_\rho = x_\rho x'_\rho$$

if $\rho \in R$ and for $\sigma \in C$ we have that

$$z_\sigma \overline{z}'_\sigma + z_{\overline{\sigma}} \overline{z}'_{\overline{\sigma}} = z_\sigma \overline{z}'_\sigma + \overline{z}_\sigma z'_\sigma = 2\mathrm{Re}(z_\sigma \overline{z}'_\sigma) = 2(x_\sigma x'_\sigma + y_\sigma y'_\sigma).$$

Thus implies

$$\begin{aligned}\langle (z_\tau), (z'_\tau) \rangle &= \sum_{\tau \in H} z_\tau \overline{z}'_\tau \\ &= \sum_{\rho \in R} z_\rho \overline{z}'_\rho + \sum_{\sigma \in C} (z_\sigma \overline{z}'_\sigma + z_{\overline{\sigma}} \overline{z}'_{\overline{\sigma}}) \\ &= \sum_{\rho \in R} x_\rho x'_\rho + \sum_{\sigma \in C} 2(x_\sigma x'_\sigma + y_\sigma y'_\sigma) \\ &= (f(z_\tau), f(z'_\tau)).\end{aligned}$$

□

The next proposition finally relates ideals of $\mathcal{O}_K$ and lattices of $K_\mathbb{R}$.

Proposition 4.3. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then $\Gamma = j\mathfrak{a}$ is a lattice in $K_\mathbb{R}$ with volume*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

Proof. The ideal $\mathfrak{a}$ can be viewed as a finitely generated $\mathcal{O}_K$-module. This implies by Theorem 1.43 that there is an integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathfrak{a}$ over $\mathbb{Z}$. Then

$$\Gamma = \mathbb{Z}j\alpha_1 + \ldots + \mathbb{Z}j\alpha_n$$

is a lattice in $K_\mathbb{R}$. Choose next an enumeration $\tau_1, \ldots, \tau_n$ of the elements in H and denote $A = (\tau_l \alpha_i)$. Then we have

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = \det(A)^2$$

and by Proposition 1.46

$$d(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})^2 d(\mathcal{O}_K) = (\mathcal{O}_K : \mathfrak{a})^2 d_K.$$

Furthermore

$$(\langle j\alpha_i, j\alpha_k \rangle) = \left(\sum_{l=1}^{n} \tau_l \alpha_i \overline{\tau}_l \alpha_k \right) = A\overline{A}^t.$$

This implies

$$\mathrm{vol}(\Gamma) = |\det(A)| = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

□

We are now ready to prove Theorem 4.1.

Proof. (of Theorem 4.1) Denote by

$$X = \{(z_\tau) \in K_{\mathbb{R}} : |z_\tau| < c_\tau \text{ for all } \tau \in H\}$$

and note that the set is centrally symmetric. Since the map f from Proposition 4.2 is an isometric isomorphism of vector spaces we have that $f(X)$ is also centrally symmetric and

$$\mathrm{vol}(X) = \mathrm{vol}(f(X)).$$

Observe

$$f(X) = \{(x_\tau) : |x_\rho| < c_\rho \text{ for } \rho \in R \text{ and } x_\sigma^2 + x_{\overline{\sigma}}^2 < |c_\sigma| \text{ for } \sigma \in C\}.$$

For $s = |C|$ we have that

$$\mathrm{vol}(S) = 2^s \mathrm{vol}_{\mathrm{Lebesgue}}(S)$$

for any set $S \subset \mathbb{R}^n$. Thus

$$\begin{aligned}
\mathrm{vol}(X) &= \mathrm{vol}(f(X)) \\
&= 2^s \prod_{\rho \in R} 2c_\rho \prod_{\sigma \in C} \pi c_\sigma^2 \\
&= 2^{s+r} \pi^s \prod_{\tau \in H} c_\tau \\
&> 2^{s+r} \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}) = 2^n \mathrm{vol}(\Gamma),
\end{aligned}$$

where we used the assumption and Proposition 4.3 in the last line. Thus we conclude by Minkowski's Lattice Theorem that there is some nonzero element $a \in X$ with $a \in \Gamma = j\mathfrak{a}$, so $|\tau a| < c_\tau$. □

Corollary 4.4. *Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$. Then there is some nonzero element $a \in \mathfrak{a}$ such that*

$$|N_{(K:\mathbb{Q})}(a)| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

Proof. For all $\varepsilon > 0$ we can choose coefficients $c_\tau > 0$ for each $\tau \in H$ and with $c_\tau = c_{\overline{\tau}}$ such that

$$\prod_{\tau \in H} c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}) + \varepsilon.$$

Thus there is by Theorem 4.1 a nonzero element $a \in \mathfrak{a}$ such that

$$|N_{(K:\mathbb{Q})}(a)| = \prod_{\tau \in H} |\tau a| < \prod_{\tau \in H} c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}) + \varepsilon.$$

Since $N_{(K:\mathbb{Q})}(a)$ is an integer and the term $\left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a})$ is irrational, we derive the existence of some $a \in \mathfrak{a}$ such that

$$|N_{(K:\mathbb{Q})}(a)| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

□

4.2 Finiteness of the Class Number

As in the last section denote by K a number field and by $\mathcal{O}_K$ the ring of integers of K. Denote as in section 1.4 by J_K the abelian group of fractional ideals, i.e. non-zero finitely generated $\mathcal{O}_K$ modules of K, and by P_K the set of principle fractional ideals. The class group of K is defined as

$$\mathrm{Cl}_K = J_K/P_K$$

and the class number is the order of Cl_K. We state next the main theorem of this subsection.

Theorem 4.5. *The class number of any number field is finite.*

In order to prove the theorem we introduce the *norm* of an nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, which is defined as

$$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}).$$

We first prove two statements about the norm.

Lemma 4.6. *For any $\alpha \in \mathcal{O}_K$ we have that*

$$\mathfrak{N}((\alpha)) = |N_{(K:\mathbb{Q})}(\alpha)|$$

Proof. Let $\alpha \in \mathcal{O}_K$ and consider the image of the $\mathbb{Z}$-linear map

$$T_\alpha : \mathcal{O}_K \to \mathcal{O}_K, \qquad x \mapsto \alpha x,$$

which is a $\mathbb{Z}$-submodule of $\mathcal{O}_K$. By the elementary divisors theorem (see [Lan02] Chapter III Theorem 7.8) there exists an integral basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_K$ and elements $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ such that $a_1\omega_1, \ldots, a_n\omega_n$ form a $\mathbb{Z}$-basis of $\mathrm{Im}(T_\alpha)$. The diagonal matrix $\mathrm{diag}(a_1, \ldots, a_n)$ is hence the representation matrix of T_α with respect to the basis $y_1, \ldots, y_n$. Thus we have that

$$|\mathrm{coker}(T_\alpha)| = |\mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}| = a_1 \cdot \ldots \cdot a_n = \det(\mathrm{diag}(a_1, \ldots, a_n)).$$

So we conclude

$$\mathfrak{N}((\alpha)) = |\mathrm{coker}(T_\alpha)| = |N_{(K:\mathbb{Q})}(\alpha)|.$$

□

Proposition 4.7. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$ with the decomposition into prime ideals*

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_r^{\nu_r}.$$

Then

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a}_1)^{\nu_1} \ldots \mathfrak{N}(\mathfrak{a}_r)^{\nu_r}.$$

Proof. By the Chinese remainder theorem we have

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \ldots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}$$

and thus it suffices to assume without loss of generality $\mathfrak{a} = \mathfrak{p}^\nu$. We consider the chain

$$\mathfrak{p} \supset \mathfrak{p}^2 \supset \ldots \supset \mathfrak{p}^\nu$$

and note that $\mathfrak{p}^i \supsetneq \mathfrak{p}^{i+1}$ since the decomposition into prime ideals is unique. Next note that the quotient $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ can be given the structure of an vector space over $\mathcal{O}_K/\mathfrak{p}$ by defining the scalar multiplication for $a + \mathfrak{p}^{i+1} \in \mathfrak{p}^i/\mathfrak{p}^{i+1}$ and for $k + \mathfrak{p} \in \mathcal{O}_K/\mathfrak{p}$ by

$$(a + \mathfrak{p}^{i+1})(k + \mathfrak{p}) = ak + \mathfrak{p}^{i+1}.$$

We furthermore claim that $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ has dimension 1 over $\mathcal{O}_K/\mathfrak{p}$. To see this choose some element $a \in \mathfrak{p}^i \backslash \mathfrak{p}^{i+1}$ and consider the ideal $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$. The chain $\mathfrak{p}^{i+1} \subsetneq \mathfrak{b} \subset \mathfrak{p}^i$ implies that $\mathfrak{p} = \mathfrak{p}^{-i}\mathfrak{p}^{i+1} \subsetneq \mathfrak{p}^{-i}\mathfrak{b}$. Since the ideal $\mathfrak{p}$ is prime and hence maximal since $\mathcal{O}_K$ is a Dedekind ring we conclude that $\mathfrak{p}^{-i}\mathfrak{b} = \mathcal{O}_K$. This implies that $\mathfrak{p}^i = \mathfrak{b}$ because the inverse of elements in a group is unique and all these ideals form elements of the ideal calls group J_K.

Hence we have an isomorphism of vector spaces $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{a}$. This shows

$$\mathfrak{N}(\mathfrak{p}^\nu) = (\mathcal{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \ldots (\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu) = \mathfrak{N}(\mathfrak{p})^\nu.$$

□

Proof. (of Theorem 4.5) The proof comprises two steps. We first show that there are only finitely many integral ideals $\mathfrak{a}$ with

$$\mathfrak{N}(\mathfrak{a}) \leq M,$$

for any fixed constant M. To see this consider a prime ideal $\mathfrak{p}$ and note that $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$ for a prime number p. As the field $\mathcal{O}_K/\mathfrak{p}$ is finite, we have that $\mathcal{O}_K/\mathfrak{p}$ is a finite field extension, let us say of degree f, of $\mathbb{Z}/p\mathbb{Z}$. Hence

$$\mathfrak{N}(\mathfrak{p}) = p^f.$$

Since $(p) \subset \mathfrak{p}$, there are only finitely many prime ideals with norm of the form p^f for f some integer. This implies there are only finitely many prime ideals with norm less than M. By using the unique decomposition into prime ideals of any integral ideal $\mathfrak{a}$ and Proposition 4.7 we conclude that there are only finitely many ideals in $\mathcal{O}_K$ of norm less that M.

Second we show that for any ideal class $[\mathfrak{a}] \in \mathrm{Cl}_K$ there is an integral ideal $\mathfrak{a}_1 \in [\mathfrak{a}]$ with

$$\mathfrak{N}(\mathfrak{a}_1) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

implying the theorem by the first step. To see this, choose some γ such that $\mathfrak{b} := \gamma\mathfrak{a} \subset \mathcal{O}_K$ is an ideal in $\mathcal{O}_K$. By Corollary 4.4 there is some element $\beta \in \mathfrak{b}$ such that

$$|N_{(K:\mathbb{Q})}(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{b}).$$

Hence by Lemma

$$|N_{(K:\mathbb{Q})}(\beta)|\mathfrak{N}(\mathfrak{b}^{-1}) = \mathfrak{N}(\beta\mathfrak{b}^{-1}) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

□

It in general difficult to determine the class number of number fields and many open questions are there yet to be answered. For example it is an open question whether there is an infinite number of quadratic number fields of class number 1. We give here a list of positive integers d such that $\mathbb{Q}(d)$ has class number 1, which can be found in [Neu07]:

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53,$$
$$57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97, \ldots$$

At first glance, one might guess that for every prime number p the class number of $\mathbb{Q}(\sqrt{p})$ is 1. However, for example the prime number 79 does not satisfy this property.

4.3 Dirichlet's Unit Theorem

As before we denote by K a number field of degree n and by $\mathcal{O}_K$ the ring of integers of K. Furthermore, as in section 2.1, the group of field homomorphisms $H = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ decomposes into r real field homomorphisms and $2s$ complex field homomorphisms.

The object of investigation in this subsection is the subgroup of units $\mathcal{O}_K^*$ of the ring of integers $\mathcal{O}_K$. We first observe the following.

Lemma 4.8. *The units $\mathcal{O}_K^*$ are precisely the elements of $\mathcal{O}_K$ of norm ± 1.*

Proof. Assume $x \in \mathcal{O}_K^*$ is a unit. Then we have that

$$1 = N_{(K,\mathbb{Q})}(1) = N_{(K,\mathbb{Q})}(xx^{-1}) = N_{(K,\mathbb{Q})}(x)N_{(K,\mathbb{Q})}(x^{-1}).$$

Since $N_{(K,\mathbb{Q})}(x), N_{(K,\mathbb{Q})}(x^{-1}) \in \mathbb{Z}$ we conclude that $N(x) = \pm 1$.

Conversely if $N_{(K,\mathbb{Q})}(x) = \pm 1$ for $x \in \mathcal{O}_K$, then the minimal polynomial of x is of the form

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x \pm 1 = 0$$

for $a_1, \ldots, a_{n-1} \in \mathbb{Z}$. Thus we have that

$$x(x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-1}) = \mp 1$$

and hence $x \in \mathcal{O}_K^*$. □

Throughout this subsection we denote

$$\mu(K) := \{\text{roots of unity in } K\} \subset \mathcal{O}_K^*.$$

We aim at proving *Dirichlet's Unit Theorem.*

Theorem 4.9. *(Dirichlet's Unit Theorem) The subgroup of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$ is the direct product of the subgroup $\mu(K)$ consisting of the roots of unity and a free abelian group of rank $(r + s - 1)$.*

To prove the theorem, we study a similar setting as in section 3.1. However, we are interested in K^* instead of K. So we consider

$$K_{\mathbb{C}}^* = \prod_{\tau \in H} \mathbb{C}^*$$

together with the two maps

$$j : K^* \longrightarrow K_{\mathbb{C}}^*, \qquad x \longmapsto (\tau x)_{\tau \in H}$$

and the product of the coordinates

$$P : K_{\mathbb{C}}^* \longrightarrow \mathbb{C}^*, \qquad (x_\tau)_{\tau \in H} \longmapsto \prod_{\tau \in H} x_\tau.$$

We then have the following commutative diagram:

$$\begin{array}{ccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* \\ \downarrow{\scriptstyle N_{(K,\mathbb{Q})}} & & \downarrow{\scriptstyle P} \\ \mathbb{Q}^* & \hookrightarrow & \mathbb{C}^* \end{array}$$

We furthermore consider the logarithm

$$\log : \mathbb{C}^* \longrightarrow \mathbb{R}, \qquad x \longmapsto \log |x|$$

and the map

$$l : K_{\mathbb{C}}^* \longrightarrow \prod_{\tau \in H} \mathbb{R}, \qquad (x_\tau)_{\tau \in H} \longmapsto (\log |x_\tau|)_{\tau \in H}$$

By defining the sum of the coordinates

$$S : \prod_{\tau \in H} \mathbb{R} \longrightarrow \mathbb{R}, \qquad (x_\tau)_{\tau \in H} \longmapsto \sum_{\tau \in H} x_\tau$$

we arrive at the commutative diagram:

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{l} & \prod_{\tau \in H} \mathbb{R} \\ \downarrow{\scriptstyle N_{(K,\mathbb{Q})}} & & \downarrow{\scriptstyle P} & & \downarrow{\scriptstyle S} \\ \mathbb{Q}^* & \hookrightarrow & \mathbb{C}^* & \xrightarrow{\log} & \mathbb{R} \end{array}$$

As in section 3.1, we define

$$F : K_{\mathbb{C}}^* \longrightarrow K_{\mathbb{C}}^*, \qquad (x_\tau) \mapsto (\overline{x}_{\overline{\tau}}).$$

We write by $K_{\mathbb{R}}^*$ the set of F-invariant elements of $K_{\mathbb{C}}^*$ and by $\left[\prod_{\tau \in H} \mathbb{R}\right]^+$ the set of F-invariant elements of $\prod_{\tau \in H} \mathbb{R}$. We then arrive at the following commutative diagram:

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{R}}^* & \xrightarrow{l} & \left[\prod_{\tau \in H} \mathbb{R}\right]^+ \\ \downarrow{\scriptstyle N_{(K,\mathbb{Q})}} & & \downarrow{\scriptstyle P} & & \downarrow{\scriptstyle S} \\ \mathbb{Q}^* & \hookrightarrow & \mathbb{R}^* & \xrightarrow{\log} & \mathbb{R} \end{array}$$

Lastly denote

$$S := \{y \in K_{\mathbb{R}}^* \,:\, P(y) = \pm 1\}, \qquad H = \left\{ x \in \left[\prod_{\tau \in H} \mathbb{R}\right]^+ \,:\, S(x) = 0 \right\}$$

and write

$$\lambda = l \circ j : \mathcal{O}_K^* \to H, \qquad \Gamma = \lambda(\mathcal{O}_K^*).$$

The heart of Theorem 4.9 is the next proposition.

Proposition 4.10. *The subgroup Γ is a lattice in the $(r+s-1)$-dimensional vector space H. Hence Γ is a free abelian group of rank $(r+s-1)$.*

We the help of Proposition 4.10 we deduce Theorem 4.9.

Proof. (of Theorem 4.9) We first claim that we have a short exact sequence

$$1 \longrightarrow \mu(K) \xrightarrow{i} \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0,$$

where we denote by $i : \mu(K) \to \mathcal{O}_K^*$ the inclusion. It is clear that i is injective and λ is surjective. So it remains to show that $\mathrm{Im}(i) = \ker(\lambda)$.

If $\zeta \in \mathrm{Im}(i)$, then we have that $\tau\zeta$ is again a root of unity and hence $\lambda(\zeta) = (\log(|\tau\zeta|))_{\tau\in H} = (0)_{\tau\in H}$. This shows $\zeta \in \ker(\lambda)$. Conversely, if $\zeta \in \ker(\lambda)$, then $|\tau\zeta| = 1$ for all $\tau \in H$. Note that by Proposition 4.3 the subgroup $j\mathcal{O}_K$ is a lattice in $K_{\mathbb{R}}$. For this reason, the set $j(\ker(\lambda))$ is a bounded and hence finite subset of $j\mathcal{O}_K$. As j is injective, this implies that $\ker(\lambda)$ is a finite subgroup of $\mathcal{O}_K^*$ and hence consists of roots of unity.

To conclude the proof we use Proposition 4.10 to see that Γ is a finitely generated abelian group. So let $\gamma_1, \dots, \gamma_{r+s-1} \in \Gamma$ be a set of generators and denote by $v_1, \dots, v_{r+s-1}$ a set of preimages under λ of $\gamma_1, \dots, \gamma_{r+s-1}$ in $\mathcal{O}_K^*$. By mapping $\gamma_i \to v_i$, we see that the above sequence splits and hence

$$\mathcal{O}_K^* = \mu(K) \times \Gamma.$$

□

It remains to prove Proposition 4.10. Recall that elements a and b of a ring are called associated if $a|b$ and $b|a$.

Lemma 4.11. *Up to associating elements, there are only finitely many elements $a \in \mathcal{O}_K$ with fixed norm $N_{(K,\mathbb{Q})} = a$.*

Proof. Let $a \in \mathbb{Z}$ with $a > 1$. We claim that in any of the finitely many cosets of $\mathcal{O}_K/a\mathcal{O}_K$ there is up to associating elements at most one element α such that $|\mathrm{N}_{(K:\mathbb{Q})}(\alpha)| = a$. If in fact $\beta = \alpha + a\gamma \in \mathcal{O}_K$ another such element recall that $N_{(K:\mathbb{Q})}(\beta) \in \mathcal{O}_K$ as it is a product of integral elements and

$$N_{(K:\mathbb{Q})}(\beta) = \prod_{\tau\in\mathrm{Hom}(K,\overline{\mathbb{Q}})} \tau(\beta) \in \beta\mathcal{O}_K$$

as the embedding $K \to \overline{\mathbb{Q}}$ is one possibility. This shows

$$\frac{\mathrm{N}_{(K:\mathbb{Q})}(\beta)}{\beta} \in \mathcal{O}_K$$

$$\frac{\alpha}{\beta} = 1 - \frac{a}{\beta}\gamma = 1 \pm \frac{\mathrm{N}_{(K:\mathbb{Q})}(\beta)}{\beta}\gamma \in \mathcal{O}_K$$

and analogously

$$\frac{\beta}{\alpha} = 1 \pm \frac{\mathrm{N}_{(K:\mathbb{Q})}(\alpha)}{\alpha}\gamma \in \mathcal{O}_K.$$

So α and β are associated. □

Proof. (of Proposition 4.10) We first show that Γ is discrete in H. To see this, it suffices to show that for any $c > 0$ the bounded domain

$$\left\{(x_\tau) \in \prod_\tau \mathbb{R} \,:\, |x_\tau| \leq c\right\}$$

only contains finitely many points of $\Gamma = l(j(\mathcal{O}_K^*)$. Note that the preimage under l of this bounded domain is

$$\left\{(z_\tau) \in \prod_\tau \mathbb{C}^* \,:\, e^{-c} \leq |z_\tau| \leq e^c\right\}.$$

Note that this set only contains finitely many elements of $j(\mathcal{O}_K^*)$ as $j(\mathcal{O}_K^*)$ is a lattice in $\prod_\tau \mathbb{C}^*$.

We next show that Γ generates to whole vector space H. To see this, it suffices to find some bounded set $M \subset H$ such that

$$H = \bigcup_{\gamma\in\Gamma} (M + \gamma).$$

In order to construct such a set, we will consider its preimage under the surjective homomorphism $j : S \to H$. More explicitly we will construct a bounded set $T \subset S$ such that

$$S = \bigcup_{\varepsilon\in\mathcal{O}_K^*} Tj\varepsilon.$$

We then note that as T is bounded and for any $x = x_\tau \in T$ we have $\prod_\tau |x_\tau| = 1$ we have that the absolute values of $|x_\tau|$ are bounded from above and below. This then shows that the set $M = l(T)$ is bounded.

We choose real numbers $c_\tau > 0$, $\tau \in \mathrm{Hom}(K, \mathbb{C})$ with $c_\tau = c_{\overline{tau}}$ and with

$$C = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^2 \sqrt{|d_K|}$$

and consider the set

$$X = \{(z_\tau) \in K_\mathbb{R} \,:\, |z_\tau| < c_\tau\}.$$

Then we have for a general point $y = (y_\tau) \in S$, that

$$Xy = \{(z_\tau) \in K_\mathbb{R} \,:\, |z_\tau| < c'_\tau\}$$

with $c'_\tau = c_\tau|y_\tau|$ and $c'_\tau = c'_\tau$ and $\prod_\tau c'_\tau = \prod_\tau c_\tau = C$ as $\prod_\tau |y_\tau| = |N(y)| = 1$. By Theorem 4.1 we hence have a non-zero element $a \in \mathcal{O}_K$ such that

$$ja = (\tau a) \in Xy.$$

Using Lemma 4.11 we can find a system $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K$ with $\alpha_i \neq 0$ such that every $a \in \mathcal{O}_K$ with $a \neq 0$ and $|N_{(K:\mathbb{Q})}(a)| \leq C$ is associated to one of those elements. Then we consider the set

$$T = S \cap \bigcup_{i=1}^{N} X(ja_i)^{-1}$$

and claim that the properties we aimed at. To see this first note that as X is bounded we also have that $X(j\alpha_i)^{-1}$ is also bounded and hence also T.

It remains to show

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} Tj\varepsilon.$$

Let $y \in S$. Then there is by the above some $a \in \mathcal{O}_K$ with $a \neq 0$ and $ja \in Xy^{-1}$ so $ja = xy^{-1}$, $x \in X$. Furthermore, as

$$|N_{(K:\mathbb{Q})}(a)| = |N(xy^{-1})| = |N(x)| < \prod_\tau c_\tau = C$$

we have that a is associated to some α_i. So there is $\varepsilon \in \mathcal{O}_K^*$ with $a_i = \varepsilon a$. It follows

$$y = xja^{-1} = xj(\alpha_i^{-1}\varepsilon).$$

Then as $y, j\varepsilon \in S$ we have $xj\alpha_i^{-1} \in S \cap Xj\alpha_i^{-1} \subset T$ we also have $y \in Tj\varepsilon$. □

We next want to determine the volume of the lattice $\Gamma = \lambda(\mathcal{O}_K^*)$ of H. In order to achieve this we associate $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$ and hence H becomes by this identification a subspace of $\mathbb{R}^{r+s}$. Furthermore let $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$ be *fundamental* units of $\mathcal{O}_K$, i.e. units that generate the free part of $\mathcal{O}_K$. Then the lattice Γ is spanned by $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t) \in H$. Note that the vector

$$\lambda_0 = \frac{1}{\sqrt{r+s}}(1, 1, \ldots, 1) \in \mathbb{R}^{r+s}$$

is obviously orthogonal to H and has length 1. Thus the volume of the lattice Γ is equal to the parallelepiped spanned by $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ in $\mathbb{R}^{t+1}$ and hence given by the absolute value of the determinant spanned by the matrix given by those vectors. In formulas,

$$\mathrm{vol}(\lambda(\mathcal{O}_K^*)) = \pm \det \begin{pmatrix} \lambda_{0,1} & \lambda_1(\varepsilon_1) & \ldots & \lambda_1(\varepsilon_{r+s-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{0,r+s} & \lambda_{r+s}(\varepsilon_1) & \ldots & \lambda_{r+s}(\varepsilon_{r+s-1}) \end{pmatrix}.$$

In this setting, we define the *regulator* of the number field K as

$$\mathrm{Reg}(K) = \frac{1}{\sqrt{r+s}}\mathrm{vol}(\lambda(\mathcal{O}_K^*)).$$

4.4 Orders and the Picard Group

Throughout this subsection we denote by K a number field of order n and $\mathcal{O}_K$ its ring of integers.

Definition 4.12. A *order* of K is a subring $\mathcal{O}$ of $\mathcal{O}_K$ that has an integral basis of length n. The ring $\mathcal{O}_K$ is called the maximal order of K.

Example 4.13. For example

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{5} \subset \mathbb{Q}(\sqrt{5})$$

is an order. More generally if $\alpha_1, \ldots, \alpha_n$ are integral numbers with $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ then $\mathcal{O} = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is an order and any order is of this from.

Another later useful example of an order is given by the next proposition.

Proposition 4.14. *Let $\alpha_1, \ldots, \alpha_n$ be a basis of K over $\mathbb{Q}$ and let $\mathfrak{a} = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Then*

$$\mathcal{O}_\mathfrak{a} = \{\lambda \in K \,:\, \lambda\mathfrak{a} \subset \mathfrak{a}\}$$

is an order.

Proof. It is clear that $\mathcal{O}_\mathfrak{a}$ forms a ring. Let $\lambda \in \mathcal{O}_\mathfrak{a}$ we want to show that $\lambda \in \mathcal{O}_K$. To see this, denote by A the representation matrix of the λ-multiplication map on K with respect to the basis $\alpha_1, \ldots, \alpha_n$ and note that A has integer entries. Thus the characteristic polynomial φ of A is a monic polynomial with integer coefficients and by Cayley-Hamilton $\varphi(A) = 0$. Thus $\varphi(\lambda) = 0$. Furthermore as $\mathcal{O}_\mathfrak{a}$ is a submodule of the free module $\mathcal{O}_K$ and as the $\mathbb{Q}$-span of $\mathcal{O}_\mathfrak{a}$ is K we conclude that $\mathcal{O}_\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n. □

Theorem 4.15. *An order $\mathcal{O}$ of K is a one-dimensional noetherian integral domain.*

Proof. As $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, we have that every ideal $\mathfrak{a}$ is a finitely generated $\mathbb{Z}$-module and hence also a finitely generated $\mathcal{O}$-module. Thus $\mathcal{O}$ is noetherian. If $\mathfrak{p} \neq 0$ is a prime ideal and $a \in \mathfrak{p} \cap \mathbb{Z}$ with $a \neq 0$, then $a\mathcal{O} \subset \mathfrak{p} \subset \mathcal{O}$ and so $\mathfrak{p}$ and $\mathcal{O}$ have the same rank as a $\mathbb{Z}$-module. Thus $\mathcal{O}/\mathfrak{p}$ is a finite integral domain and thus it is a field and so $\mathfrak{p}$ is a maximal ideal. □

Note that an order $\mathcal{O}$ does not have to be a Dedekind ring as it might not be normal. Hence the set of fractional ideals might not be a group. Hence we restrict to invertible fractional ideal: For an order $\mathcal{O}$ we denote by $J(\mathcal{O})$ the set of invertible fractional ideals, i.e. the non-zero finitely generated $\mathcal{O}$-submodules of K such that there is a fractional ideal $\mathfrak{b}$ with

$$\mathfrak{a}\mathfrak{b} = \mathcal{O}.$$

The set $J(\mathcal{O})$ obviously forms an abelian group and for any element $\mathfrak{a} \subset \mathcal{O}$ the inverse is given by

$$\mathfrak{a}^{-1} = \{x \in K \,:\, x\mathfrak{a} \subset \mathcal{O}\}.$$

We furthermore denote by $P(\mathcal{O})$ the set of principal fractional ideals. Then the factor group

$$\mathrm{Pic}(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$$

is called the *Picard group* of $\mathcal{O}$.

Recall that for an integral domain R and a multiplicative subset $S \subset R\backslash\{0\}$ we define the *localization* of S as

$$S^{-1}R = \left\{ \frac{r}{s} \in \mathrm{Quot}(K) \,:\, r \in R \text{ and } s \in S \right\}.$$

We furthermore write for $\mathfrak{p}$ a prime ideal of R the localization at $R\backslash\mathfrak{p}$ as

$$R_\mathfrak{p} = (R\backslash\mathfrak{p})^{-1}R.$$

We can moreover prove an analogue of Dirichlet's Unit Theorem for the order $\mathcal{O}$.

Theorem 4.16. *(Dirichlet's Unit Theorem of Orders) Let $\mathcal{O}$ be an order in an algebraic number field K. The group $\mathcal{O}^*$ of units is the direct product of the subgroup $\mu(K)$ consisting of roots of unity and a free abelian group of rank $(r+s-1)$.*

Proof. For a proof see [Neu07] Theorem 12.12 of section 1. We furthermore give in section 8 a proof based on algebraic groups for the case $K = \mathbb{Q}(\zeta)$ for ζ an algebraic number. □

4.5 Orders and Periodic Orbits

The aim of this subsection is to relate to algebraic information in totally real number fields to interesting *periodic orbits* for the diagonal subgroup in the space of lattices up to scaling

$$X_d = \mathrm{PGL}_d(\mathbb{Z})\backslash\mathrm{PGL}_d(\mathbb{R}).$$

We first discuss the term *periodic orbit*. Denote

$$A = \left\{ \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_d \end{pmatrix} \in \mathrm{PGL}_d(\mathbb{R}) \right\} < \mathrm{PGL}_d(\mathbb{R})$$

the diagonal subgroup. A point $x \in X_d$ is called *periodic* for the diagonal action on X_d if there exists a finite A-invariant measure on

$$x.A \subset X_d.$$

If x is an A-periodic point, then the set $x.A$ is called the a *periodic orbit*.

It will turn out to be useful to decompose A into a part with a positive determinant representative and a part with a negative representative. So denote by A^+ the subgroup diagonal matrices in A which have a representative of positive determinant and by A^- diagonal matrices in A which have a representative of negative determinant. Note that if d is odd, then $A^+ = A^-$. If d is even then $A^+ = A^- M$ for $M = \mathrm{diag}(-1, 1, \ldots, 1)$[1].

Let K be a totally real number field of degree d and denote by $\tau_1, \ldots, \tau_d$ the real embeddings $K \to \mathbb{R}$ and by τ the $\mathbb{Q}-$linear map

$$\tau : K \to \mathbb{R}^d, \qquad k \mapsto (\tau_1(k), \ldots, \tau_d(k)).$$

First, we want to associate to each fractional ideal $\mathfrak{a}$ a periodic orbit. Consider the lattice

$$L_{\mathfrak{a}} = \{\tau(a) \,:\, a \in \mathfrak{a}\}$$

and let $x_{\mathfrak{a}} \in X_d$ be the element of X_d that corresponds to $L_{\mathfrak{a}}$.

Recall that by Theorem 1.43 the fractional ideal $\mathfrak{a}$ is a free $\mathbb{Z}$ module of rank d that satisfies

$$\mathcal{O}_K \subset \{\lambda \in K \,:\, \lambda\mathfrak{a} \subset \mathfrak{a}\}.$$

[1] In dimension 2, multiplication of a lattice by M corresponds to mirroring the lattice at the y-axis. This obviously generalizes to higher dimensions.

By Proposition 4.14 the latter set is an order in K, hence

$$\mathcal{O}_K = \{\lambda \in K \,:\, \lambda\mathfrak{a} \subset \mathfrak{a}\}. \tag{4.1}$$

If $a_1, \ldots, a_d$ is an integral basis of $\mathfrak{a}$ then $L_\mathfrak{a}$ can we written in terms of the integral basis as follows:

$$L_\mathfrak{a} = \mathbb{Z}^d \begin{pmatrix} \tau(a_1) \\ \tau(a_2) \\ \vdots \\ \tau(a_d) \end{pmatrix} = \mathbb{Z}^d \begin{pmatrix} \tau_1(a_1) & \tau_2(a_1) & \ldots & \tau_d(a_1) \\ \tau_1(a_2) & \tau_2(a_2) & \ldots & \tau_d(a_2) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_1(a_d) & \tau_2(a_d) & \ldots & \tau_d(a_d) \end{pmatrix}.$$

Recall

$$d(\mathfrak{a}) = \det \begin{pmatrix} \tau_1(a_1) & \tau_2(a_1) & \ldots & \tau_d(a_1) \\ \tau_1(a_2) & \tau_2(a_2) & \ldots & \tau_d(a_2) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_1(a_d) & \tau_2(a_d) & \ldots & \tau_d(a_d) \end{pmatrix}^2$$

and hence $L_\mathfrak{a}$ is indeed a lattice as the discriminant is non-zero.

Lemma 4.17. *The point $x_\mathfrak{a} \in X_d$ is A-periodic.*

Before proving the lemma, we proceed with a short digression. Fix an integral basis $a_1, \ldots, a_d$ of $\mathfrak{a}$. Then $a_1, \ldots, a_d$ is a basis of K over $\mathbb{Q}$. Let $\lambda \in K$ and consider the multiplication map

$$m_\lambda : K \to K, \qquad k \mapsto k\lambda.$$

We denote by $M_\lambda \in \mathrm{M}_d(\mathbb{Q})$ the representation matrix m_λ with respect to the basis $a_1, \ldots, a_d$. Then by (4.1) we have

$$M_\lambda \in \mathrm{M}_d(\mathbb{Z}) \quad \Longleftrightarrow \quad \lambda \in \mathcal{O}_K$$

and

$$M_\lambda \in \mathrm{GL}_d(\mathbb{Z}) \quad \Longleftrightarrow \quad \lambda \in \mathcal{O}_K^*.$$

Proof. (of Lemma 4.17) Let $\varepsilon \in \mathcal{O}_K^*$ be a unit. As multiplication by ε is represented by an element of $\mathrm{GL}_d(\mathbb{Z})$ we conclude

$$x_\mathfrak{a} = x_\mathfrak{a} \cdot \begin{pmatrix} \tau_1(\varepsilon) & & & \\ & \tau_2(\varepsilon) & & \\ & & \ddots & \\ & & & \tau_d(\varepsilon) \end{pmatrix}$$

as an equation in X_d.

Denote by $\varepsilon_1, \ldots, \varepsilon_{d-1} \in \mathcal{O}_K^*$ a system of fundamental units of $\mathcal{O}_K^*$. If necessary, we replace ε_i by ε_i^2 in order to arrive at a unit of norm 1. Write $t_i = \mathrm{diag}(\tau_1(\varepsilon_i), \ldots, \tau_d(\varepsilon_i)) \in A^+$ and so $x_\mathfrak{a} = x_\mathfrak{a}.t_i$ for $i = 1, \ldots, d-1$. By Dirichlet's Unit Theorem the $\tau(\varepsilon_1), \ldots \tau(\varepsilon_{d-1})$ span a lattice and are thus linearly independent.

This allows us to endow the A^+-orbit $x_\mathfrak{a}.A^+ \subset X_d$ with an A^+-invariant probability measure as follows: Note that the canonical surjection

$$A^+ \to x.A^+, \qquad a \mapsto x.a$$

has a kernel that contains the $\mathbb{Z}^{d-1}$-span of $t_1, \ldots, t_{d-1}$. Denote by Λ this $\mathbb{Z}^{d-1}$-span and note that this is a lattice in A. Thus the map factors through a surjection

$$A^+/\Lambda \to x.A^+.$$

By pushing forward the finite A^+-invariant measure on A^+/Λ we arrive at a A^+-invariant measure on $x.A^+$. In order to get an A invariant measure on the entire orbit $x_{\mathfrak{a}}.A$ just use the matrix M with $A^- = A^+M$ and the above A^+-invariant measure on $x.A^+$ to define such a measure. □

In fact, the surjection

$$A^+/\Lambda \to x.A^+$$

from the above proof is indeed a bijection. To see this assume without loss of generality that $\tau_1 = \mathrm{id}$. Assume that $a = \mathrm{diag}(\lambda_1, \ldots, \lambda_d) \in A^+$ has determinant 1 and satisfies $x_{\mathfrak{a}} = x_{\mathfrak{a}}.a$. Then multiplication by λ_1 is represented by an integer matrix and so $\lambda_1 \in \mathcal{O}_K$. Moreover, $\tau_i(\lambda_1) = \lambda_i$ for $i = 1, \ldots, d$ and so $\mathrm{N}(\lambda_1) = 1$. So $\lambda_1 \in \mathcal{O}_K^*$ and hence it is contained in Λ.

Lemma 4.18. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals. Then $[\mathfrak{a}] = [\mathfrak{b}]$ if and only if $x_{\mathfrak{a}}.A = x_{\mathfrak{b}}.A$.*

Proof. Assume that $\mathfrak{b} = \lambda\mathfrak{a}$ for $\lambda \in K^\times$. If $a_1, \ldots, a_n$ is an integral basis of $\mathfrak{a}$, then $\lambda a_1, \ldots, \lambda a_n$ is one of $\mathfrak{b}$. Thus

$$\begin{pmatrix} \tau(\lambda a_1) \\ \tau(\lambda a_2) \\ \vdots \\ \tau(\lambda a_n) \end{pmatrix} = \begin{pmatrix} \tau(a_1) \\ \tau(a_2) \\ \vdots \\ \tau(a_n) \end{pmatrix} \begin{pmatrix} \tau_1(\lambda) & & & \\ & \tau_2(\lambda) & & \\ & & \ddots & \\ & & & \tau_d(\lambda) \end{pmatrix}$$

and hence for $a = \mathrm{diag}(\tau_1(\lambda), \ldots, \tau_d(\lambda)) \in A$ we have

$$x_{\mathfrak{b}} = x_{\mathfrak{a}}.a,$$

or equivalently $x_{\mathfrak{a}}.A = x_{\mathfrak{b}}.A$.

For the converse assume there is $a = (\lambda_1, \ldots, \lambda_d) \in A$ so that $x_{\mathfrak{b}} = x_{\mathfrak{a}}.a$. We furthermore assume without loss of generality that $\tau_1 = \mathrm{id}$. For the rest of this proof, in order to arrive at actual equalities of matrices and not just equalities up to homothety, we normalize all matrices to have determinant ± 1. In particular, the matrix a has determinant 1. Let $a_1, \ldots, a_d$ be an integral basis of $\mathfrak{a}$ and $b_1, \ldots, b_d$ one of $\mathfrak{b}$. Then we have that

$$\frac{1}{d(\mathfrak{b})^{\frac{1}{2d}}} \begin{pmatrix} \tau(b_1) \\ \tau(b_2) \\ \vdots \\ \tau(b_n) \end{pmatrix} = \frac{1}{d(\mathfrak{a})^{\frac{1}{2d}}} \begin{pmatrix} \tau(a_1) \\ \tau(a_2) \\ \vdots \\ \tau(a_n) \end{pmatrix} \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_d \end{pmatrix}$$

and so

$$\begin{pmatrix} \tau(b_1) \\ \tau(b_2) \\ \vdots \\ \tau(b_n) \end{pmatrix} = \begin{pmatrix} \tau(a_1) \\ \tau(a_2) \\ \vdots \\ \tau(a_n) \end{pmatrix} \frac{d(\mathfrak{b})^{\frac{1}{2d}}}{d(\mathfrak{a})^{\frac{1}{2d}}} \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_d \end{pmatrix}.$$

Set

$$\lambda = \frac{\sqrt{d(\mathfrak{b})}}{\sqrt{d(\mathfrak{a})}}\lambda_1$$

and so as $\tau_1 = \mathrm{id}$ we conclude that $b_i = \lambda a_i$ for all $i = 1, \dots, d$ or equivalently

$$\lambda = \frac{b_i}{a_i} \in K^\times$$

and so $\mathfrak{b} = \lambda\mathfrak{a}$ and $[\mathfrak{b}] = [\mathfrak{a}]$. □

We next discuss generalizations to all of the above in two directions. First, we can consider not only totally real number fields, but more generally any number field of degree d. However, showing analogous results to before will rely upon using the theory of algebraic groups as will be done in section 10.3. Second, we can consider a much wider class of ideals. Fix an order $\mathcal{O}$ in K. The ideals we are interested in are so called *proper $\mathcal{O}$-ideals* $\mathfrak{a}$, i.e. free $\mathbb{Z}$-modules of rank d that satisfy

$$\mathcal{O} = \{\lambda \in K \,:\, \lambda\mathfrak{a} \subset \mathfrak{a}\}.$$

In fact, if $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal, by definition we have a normalized integral basis $a_1, \dots, a_d$ of $\mathfrak{a}$. Then the same construction as before leads to an element $x_\mathfrak{a} \in X$. Analogously to Lemma 4.17, $x_\mathfrak{a}$ is periodic and the only difference in the proof is that one uses the fundamental units of $\mathcal{O}$ instead of the ones of $\mathcal{O}_K$.

We furthermore, want to generalize Lemma 4.18. Using the same proof we can show for a given proper $\mathcal{O}$-ideal $\mathfrak{a}$ and a proper $\mathcal{O}'$-ideal $\mathfrak{b}$ that the periodic orbits $x_\mathfrak{a}.A$ and $x_\mathfrak{b}.A$ are the same if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, i.e. there exists some $\lambda \in K^\times$ so that

$$\mathfrak{b} = \lambda\mathfrak{a}. \tag{4.2}$$

Note that if (4.2) holds then

$$\mathcal{O}' = \{\mu \in K \,:\, \mu\mathfrak{b} = \mathfrak{b}\} = \{\mu \in K \,:\, \mu\lambda\mathfrak{a} = \lambda\mathfrak{a}\} = \{\mu \in K \,:\, \mu\mathfrak{a} = \mathfrak{a}\} = \mathcal{O}.$$

So we arrive at a generalization of Lemma 4.18, which forms the next proposition.

Proposition 4.19. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders in K and consider $\mathfrak{a}$ a proper $\mathcal{O}$-ideal and $\mathfrak{b}$ be a proper $\mathcal{O}'$-ideal. Then $x_\mathfrak{a}.A = x_\mathfrak{b}.A$ if and only if there is $\lambda \in K^\times$ so that $\mathfrak{b} = \lambda\mathfrak{a}$ and hence $\mathcal{O} = \mathcal{O}'$.*

Proof. The proof together with the discussion above is almost verbatim to the one of Lemma 4.18. □

4.6 Duke's Theorem and the Height of Lattices

This subsection is a continuation of the last one in special case $d = 2$ and so

$$X := X_2 = \mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R}) = \mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})$$

and $K = \mathbb{Q}(\sqrt{d})$ for d a positive non-square integer. This setting allows a particularly beautiful interpretation of the periodic orbit $x_\mathfrak{a}.A$, which is based on hyperbolic geometry. Denote by $\mathbb{H}$ the upper half plane together with the hyperbolic metric. Recall that we can view $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm\mathrm{Id}_2\}$ as the unit tangent bundle of $\mathbb{H}$. This property is preserved by considering quotients

of the upper half plane by discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$. Thus we can view $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PSL}_2(\mathbb{R})$ as the unit tangent bundle of the modular surface $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}$.

Even more remarkable is that the action of the one-dimensional diagonal group A (now viewed as a subgroup of $\mathrm{PSL}_2(\mathbb{R})$) on $\mathbb{H}$ is the geodesic flow. Thus an A-periodic orbit on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})$ is a closed geodesic on the modular surface.

We denote

$$\mathcal{O}_d := \mathbb{Z}\left[\frac{d+\sqrt{d}}{2}\right]$$

and throughout this subsection we assume that $d \equiv 0, 1 \mod 4$. Then $\mathcal{O}_d \subset \mathcal{O}_K$ is an order in K.

To picture a concrete example, consider simply $\mathfrak{a} = \mathcal{O}_d$ and then

$$x_{\mathcal{O}_d} = \begin{pmatrix} 1 & 1 \\ \frac{d+\sqrt{d}}{2} & \frac{d-\sqrt{d}}{2} \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R}).$$

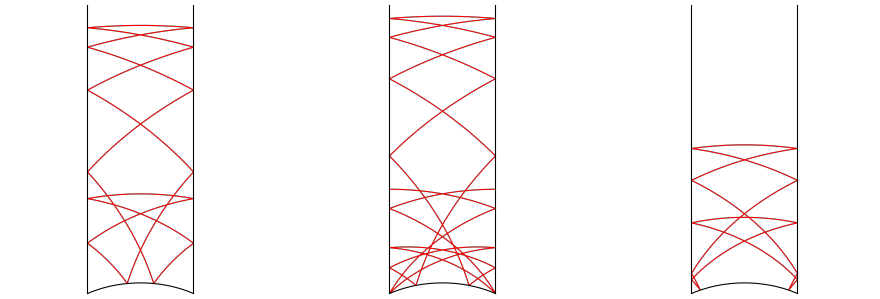


Figure 1: Closed geodesics associated to $\mathcal{O}_d$ in the cases $d = 18, 19, 30$

We want to consider all orbits associated to all possible proper $\mathcal{O}_d$-ideals. In this concrete setting it turns out that the notion of proper $\mathcal{O}_d$-ideal and invertible fractional $\mathcal{O}_d$-ideal coincide.

Proposition 4.20. *Let $\mathfrak{a} \subset K$ be a fractional $\mathcal{O}_d$-ideal. Then $\mathfrak{a}$ is invertible if and only if $\mathfrak{a}$ is a proper $\mathcal{O}_d$-ideal, i.e. $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2 which satisfies*

$$\mathcal{O}_d = \{\lambda \in \mathfrak{a} \,:\, \lambda\mathfrak{a} \subset \mathfrak{a}\}.$$

Proof. See [ELMV12] Section 2.2. □

Thus

$$\{\mathfrak{a} \subset K \text{ proper } \mathcal{O}_d\text{-ideal}\}/K^\times = \mathrm{Pic}(\mathcal{O}_d).$$

Let $\mathcal{G}_d$ be the collection of all periodic orbits associated to all proper $\mathcal{O}_d$-ideals, i.e.

$$\mathcal{G}_d = \bigcup_{\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}_d)} x_{\mathfrak{a}}.A = \bigcup_{\mathfrak{a} \text{ proper } \mathcal{O}_K\text{-ideal}} x_{\mathfrak{a}}.A.$$

This is collection is finite, as the Picard group is finite. By averaging all the periodic orbit probability measures, the collection $\mathcal{G}_d$ posses the A-invariant probability measure

$$\mu_d = \frac{1}{|\mathrm{Pic}(\mathcal{O}_d)|} \sum_{\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}_d)} \mu_{x_{\mathfrak{a}}.A}$$

which is supported on $\mathcal{G}_d \subset X$.

Denote by μ_X the Haar measure on X. In this setting it is natural to ask, whether the set $\mathcal{G}_d$ *equidistributes*, i.e. whether for any $f \in C_c(X)$ it holds that

$$\int f(x)\, d\mu_d(x) \to \int f(x)\, d\mu_X(x)$$

as $d \to \infty$. The affirmative answer is given by Duke's Theorem.

Theorem 4.21. *(Duke's Theorem, Theorem 1.3 of [ELMV12]) As $d \to \infty$ among the non-square discriminants, the set $\mathcal{G}_d$ equidistributes.*

The proof of Duke's Theorem [ELMV12] combines methods from number theory and ergodic theory. As a first step towards the proof of Duke's Theorem, one needs to show that not too much of the collection $\mathcal{G}_d$ is high up in the cusp, picturing the collection of orbits on the modular surface as in Figure 1. To capture this, we introduce the height of lattices.

We define the **height** of a lattice $L = \mathbb{Z}^2 g$ for $g \in \mathrm{GL}_2(\mathbb{R})$ as

$$\mathrm{ht}(L) = \left(\frac{\min_{x \in L \setminus \{0\}} ||x||}{\mathrm{vol}(L)^{\frac{1}{2}}} \right)^{-1} = \left(\frac{\min_{x \in \mathbb{Z}^2 \setminus \{0\}} ||xg||}{\mathrm{vol}(L)^{\frac{1}{2}}} \right)^{-1}.$$

Observe that $\mathrm{ht}(L)$ only depends on the homothety class of L.

We can relate the height of a unimodular lattice to a geometric quantity on the modular surface, as stated in the next lemma. Let

$$S = \{z \in \mathbb{H} : -\tfrac{1}{2} \leq \mathrm{Im}(z) \leq \tfrac{1}{2} \text{ and } |z| \geq 1\}$$

be the fundamental domain (see Section 11 of [EW11]) for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

Lemma 4.22. *Let $x \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})$ and assume $x \cong (z, v) \in T^1(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H})$ for $z \in S$. Then*

$$\mathrm{Im}(z) = \mathrm{ht}(x)^2.$$

Proof. We can choose $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ with $x = \Gamma g$ such that $g.i \in S$, i.e. $|\mathrm{Re}(g.i)| \leq \frac{1}{2}$ and $|g.i| \geq 1$. As

$$g.i = \frac{ai + b}{ci + d} = \frac{ai + b}{ci + d} \frac{d - ci}{d - ci} = \frac{ac + bd}{c^2 + d^2} + i \frac{1}{c^2 + d^2}$$

the assumption $|\mathrm{Re}(g.i)| \leq \frac{1}{2}$ translates to

$$|\mathrm{Re}(z)| = \left| \frac{ac + bd}{c^2 + d^2} \right| \leq \frac{1}{2}.$$

Moreover we can assume upon multiplying g by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and thus replacing $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ by $g = \left(\begin{smallmatrix} -c & -d \\ a & d \end{smallmatrix}\right)$ that

$$c^2 + d^2 \leq a^2 + b^2.$$

Set $L = \mathbb{Z}^2 g$. Then

$$\begin{aligned} \mathrm{ht}(x)^{-2} = \mathrm{ht}(L)^{-2} &= \min_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} ||(m,n)g||^2 \\ &= \min_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \big((ma+nc)^2 + (mb+nd)^2\big) \\ &= \min_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \big(m^2(a^2+b^2) + n^2(c^2+d^2) + 2mn(ac+bd)\big) \end{aligned}$$

Thus we have that

$$\frac{\mathrm{Im}(g.i)}{\mathrm{ht}(x)^2} = \min_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \left(m^2 \frac{a^2+b^2}{c^2+d^2} + n^2 + 2mn\frac{ac+bd}{c^2+d^2} \right) = 1$$

□

Let $H > 1$ and denote

$$X_{\geq H} = \{x \in X \,:\, \mathrm{ht}(x) \geq H\}.$$

Proposition 4.23. *Let $\mathfrak{a} \subset \mathcal{O}_d$ be a proper $\mathcal{O}_d$-ideal. Then $x_{\mathfrak{a}}.A \cap X_{\geq H}$ is nonempty if and only if $\mathfrak{a}^{-1}$ is in the same ideal class as an ideal $\mathfrak{b} \subset \mathcal{O}_d$ of norm $\leq \frac{1}{2}H^{-2}d^{1/2}$.*

Proof. We first observe the following. If we identify $x \in X$ with the unimodular lattice L, we claim that $x.A \cap X_{\geq H}$ is nonempty if and only if there is some nonzero vector

$$(u,v) \in L \quad \text{with} \quad |uv| \leq \frac{1}{2}H^{-2}. \tag{4.3}$$

This observation follows from calculating the minimal norm achieved under the A-action for an element $0 \neq (u,v) \in L$. So consider the continuously on t dependent function

$$\left|\left|(u,v)\cdot a_t\right|\right|^2 = \left|\left|(u,v)\cdot \begin{pmatrix} e^{t/2} & 0 \\ 0 & e^{-t/2} \end{pmatrix}\right|\right|^2 = u^2e^t + v^2e^{-t},$$

which has derivative

$$u^2e^t - v^2e^{-t}.$$

The derivative is zero if and only if (assuming w.l.o.g. $u \neq 0$) $t = \log\left(|\frac{v}{u}|\right)$. Hence the minimum of the function $||(u,v)\cdot a_t||^2$ is $|2uv|$.

Using this, assume we have $(u,v) \in L = \mathbb{Z}^2 x$ with $|uv| \leq \frac{1}{2}H^{-2}$. Then, as above, there is some t_0 so that

$$\left|\left|(u,v)\cdot a_{t_0}\right|\right| = \sqrt{|2uv|} \leq H^{-1}$$

implying $\mathrm{ht}(L.a_{t_0})^{-1} \leq H^{-1}$ and so $\mathrm{ht}(L.a_{t_0}) \geq H$.

For the converse assume that for some t_0, $\mathrm{ht}(L.a_{t_0}) \geq H$ or equivalently $\mathrm{ht}(L.a_{t_0})^{-1} \leq H^{-1}$. Then there is $(u,v) \in L$ such that

$$\sqrt{|2uv|} \leq \left|\left|(u,v) \cdot a_{t_0}\right|\right| \leq H^{-1},$$

implying the claim.

Now let $\mathfrak{a}$ be a proper $\mathcal{O}_d$-ideal with integral basis a_1, a_2. Then

$$\det \begin{pmatrix} a_1 & \tau(a_1) \\ a_2 & \tau(a_2) \end{pmatrix} = \sqrt{d(\mathfrak{a})} = (\mathcal{O}_d : \mathfrak{a})\sqrt{d(\mathcal{O}_d)} = \mathrm{N}(\mathfrak{a}) d^{\frac{1}{2}}.$$

In the following we want to normalize $x_{\mathfrak{a}}$ to arrive at an element with determinant ± 1. So we get

$$x_{\mathfrak{a}} = \frac{1}{\sqrt{\mathrm{N}(\mathfrak{a}) d^{\frac{1}{2}}}} \begin{pmatrix} a_1 & \tau(a_1) \\ a_2 & \tau(a_2) \end{pmatrix}$$

and the lattice $L = \mathbb{Z}^2 x_{\mathfrak{a}}$ given by $x_{\mathfrak{a}}$ is

$$L = \left\{ \frac{1}{\sqrt{\mathrm{N}(\mathfrak{a}) d^{\frac{1}{2}}}} (na_1 + ma_2, \tau(na_1 + ma_1)) \,:\, n, m \in \mathbb{Z} \right\}.$$

So the above condition translates to the following conclusion: $x_{\mathfrak{a}}.A$ intersects $X_{\geq H}$ if and only if $\mathfrak{a}$ contains an element λ so that

$$|\mathrm{N}(\lambda)| \leq \frac{1}{2} H^{-2} \mathrm{N}(\mathfrak{a}) d^{1/2}.$$

Furthermore $\mathrm{N}(\mathfrak{a}^{-1}) = \mathrm{N}(\mathfrak{a})^{-1}$. So $x_{\mathfrak{a}}.A$ intersects $X_{\geq H}$ if and only if $N(\lambda \mathfrak{a}^{-1}) \leq \frac{1}{2} H^{-2} d^{1/2}$ for some $\lambda \in \mathfrak{a}$ so that $\lambda \mathfrak{a}^{-1} \subset \mathcal{O}_d$. □

Corollary 4.24. *There is an bijection*[2] *between connected components of* $\mathcal{G}_d \cap X_{\geq H}$ *and ideal classes of proper* $\mathcal{O}_d$*-ideals* $[\mathfrak{a}]$ *with a representative* $\mathfrak{a} \subset \mathcal{O}_d$ *of norm* $\leq \frac{1}{2} H^{-2} d^{1/2}$.

Proof. The maps are given as follows. If $x_{\mathfrak{a}}.A \cap X_{\geq H} \neq \emptyset$, then by the last proposition the ideal class $[\mathfrak{a}^{-1}]$ has a representative of norm $\leq \frac{1}{2} d^{1/2} H^{-2}$. So the map $x_{\mathfrak{a}}.A \mapsto [\mathfrak{a}^{-1}]$ is well defined. For the same reason the map $[\mathfrak{b}]$ with such a representative mapping to $x_{\mathfrak{b}^{-1}}.A$ is well defined. These two maps are inverse to each other as $\mathrm{Pic}(\mathcal{O}_d)$ is a group and so in particular $(\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$. □

Towards the proof of Duke's Theorem [**?**], we will need to show that for all $\varepsilon > 0$,

$$\mu_d(X_{\geq d^\varepsilon}) \to 0$$

as $d \to \infty$. In fact, a special case of the next proposition (in the case $H = d^\varepsilon$) shows that

$$\mu_d(X_{\geq d^\varepsilon}) \ll_\varepsilon d^\varepsilon.$$

Proposition 4.25. *For all* $\varepsilon > 0$ *and* $H \geq 1$ *we have*

$$\mu_d(X_{\geq H}) \ll_\varepsilon d^\varepsilon H^{-2}.$$

[2] In fact we consider the set of connected components of $\mathcal{G}_d \cap X_{\geq H}$ up to identifying the A^+ and the A^- part.

Proof. For any orbit in $\mathcal{G}_d$ the maximal height achieved is $\leq d^{\frac{1}{4}}$ as there is no ideal of norm less than 1. We show next that for $H > 1$ any connected component of $\mathcal{G}_d \cap X_{\geq H}$ has length $3\log(d)$. Indeed, such a connected component corresponds to the segment of some oriented geodesic circle whose points have imaginary part between H^2 and $d^{\frac{1}{2}}$. More precisely, we want to bound the length of the geodesic segment between two points $z_1 = (x_1, H^2)$ and $z_2 = (x_2, H^2)$ in $\mathbb{H}$, where we choose x_1 and x_2 such that the geodesic arc connecting z_1 and z_2 stays below $d^{\frac{1}{2}}$. This then shows that $|x_1 - x_2| \leq 2d^{1/2}$ by Pythagoras. Thus, using the hyperbolic distance formula

$$\begin{aligned} d_{\mathbb{H}}(z_1, z_2) &= 2\log\left(\frac{\sqrt{(x_2-x_1)^2} + \sqrt{(x_2-x_1)^2 + 4H^4}}{2H^2}\right) \\ &\leq 2\log\left(\frac{2d^{1/2} + 2\sqrt{2}d^{1/2}}{2H^2}\right) \\ &\leq 2\log\left(\frac{(1+\sqrt{2})d^{\frac{1}{2}}}{H^2}\right) \\ &\leq 2\log\Big(1+\sqrt{2}\Big) + 2\log\Big(d^{1/2}\Big) - \ln\big(H^2\big) \\ &\leq 2\log\Big(1+\sqrt{2}\Big) + 2\log\Big(d^{1/2}\Big) \\ &\leq 3\log(d) \end{aligned}$$

for $d \geq 3$ and hence for all d as we only consider non-square discriminants. Together with Corollary 4.24,

$$\text{length}(\mathcal{G}_d \cap X_{\geq H}) \leq 3\log(d) N_{\leq H}(d)$$

for $N_{\leq H}(d)$ being the number of proper ideals $\mathfrak{a} \subset \mathcal{O}_d$ of norm $N(\mathfrak{a}) \leq \frac{1}{2}H^{-2}d^{\frac{1}{2}}$. Recall that for any $n \in \mathbb{N}$ the number of proper ideals in $\mathcal{O}_d$ of norm equal to n can be bounded by the squaring number of divisors of n and so by $\ll_\varepsilon n^\varepsilon$. By summing over all $1 \leq n \leq \frac{1}{2}H^{-2}d^{1/2}$ we conclude

$$N_{\leq H}(d) \ll_\varepsilon \sum_{1 \leq n \leq \frac{1}{2}H^{-2}d^{1/2}} n^\varepsilon \ll_\varepsilon \frac{1}{2}H^{-2}d^{1/2}(\frac{1}{2}H^{-2}d^{1/2})^\varepsilon \ll_\varepsilon (H^{-2}d^{1/2})^{1+\varepsilon}.$$

So we see that

$$\text{length}(\mathcal{G}_d \cap X_{\geq H}) \ll_\varepsilon \log(d)(H^{-2}d^{\frac{1}{2}})^{1+\varepsilon}.$$

As $\log(d)$ is dominated by $d^{\frac{1}{2}}$ and as $H^{-2(1+\varepsilon)} \leq H^{-2}$ we get

$$\text{length}(\mathcal{G}_d \cap X_{\geq H}) \ll_\varepsilon H^{-2}d^{\frac{1}{2}(1+\varepsilon)}.$$

Moreover, a straightforward consequence of Dirichlet's Class Number formula is

$$\text{length}(\mathcal{G}_d) = |d|^{\frac{1}{2}+o(1)}.$$

This implies

$$\mu_d(X_{\geq H}) = \frac{\text{length}(\mathcal{G}_d \cap X_{\geq H})}{\text{length}(\mathcal{G}_d)} \ll_\varepsilon H^{-2}d^\varepsilon.$$

□

5 Binary Quadratic Forms

5.1 The Narrow Class Group

Let K be a number field. Recall that the ideal class group I_K is given by the abelian group of fractional ideals. We denote as usual by P_K the subgroup of principal fractional ideals and the quotient group

$$Cl_K = I_K/P_K$$

is the class group of K and its cardinality the class number. We then define the *positive* subgroup of P_K, given by

$$P_K^+ = \{\text{principal fractional ideals } (\alpha) \text{ with } \sigma(\alpha) > 0 \text{ for all embeddings } \sigma : K \to \mathbb{R}\}.$$

The *narrow class group* is subsequently defined as the quotient

$$Cl_K^+ = J_K/P_K^+.$$

Moreover, we refer by the term *narrow class number* the cardinality of Cl_K^+.

For example, if K is a totally imaginary number field then there are no real embeddings $K \to \mathbb{R}$ and so $P_K^+ = P_K$ and the narrow class group coincides with the standard class group. We won't calculate the narrow class numbers for real quadratic fields here, instead we just give a list of positive integers d such that the narrow class number is 1:

$$2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, \ldots$$

5.2 Binary Quadratic Forms and Number Fields

Definition 5.1. A *binary (integral) quadratic form* is a polynomial

$$Q(X, Y) = aX^2 + bXY + cY^2$$

with $a, b, c \in \mathbb{Z}$. Moreover, we say that the quadratic form Q *represents* the integer $r \in \mathbb{Z}$ if there are integers m, n such that

$$r = Q(m, n).$$

Be setting

$$B_Q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}, \quad \text{and } \underline{X} = \begin{pmatrix} X \\ Y \end{pmatrix}$$

we note that Q is can be written with the help of B_Q as

$$Q(X, Y) = \underline{X}^T B_Q \underline{X}.$$

The number

$$d_Q = b^2 - 4ac = -4 \det(B_Q)$$

is called the *discriminant* of Q. We furthermore call the quadratic form Q *non-degenerate* if $d_Q \neq 0$.

Lemma 5.2. *An integer d is the discriminant of a quadratic form Q if and only if*

$$d \equiv 0, 1 \mod 4$$

Proof. Assume d is the discriminant of a quadratic form $Q(X,Y) = aX^2 + bXY + cY^2$. If $2|b$, then we have that $4|d = b^2 - 4ac$. If $2 \nmid b$, then

$$b \equiv 1, 3 \mod 4$$

and so

$$b^2 = 1 \mod 4$$

implying that

$$d = b^2 - 4ac \equiv 1 \mod 4.$$

Conversely assume that $4|d$. The the quadratic form $Q(X,Y) = X^2 - \frac{d}{4}Y^2$ has discriminant d. If $d = 4n+1$ then the quadratic form $Q(X,Y) = X^2 + XY - nY^2$ provides an example of a quadratic form with discriminant d. □

We are interested to know which integers are represented by the quadratic from Q. If

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z})$$

is an integer matrix, we note that if understand the quadratic form Q then we also understand the quadratic form

$$Q'(X,Y) = Q(\alpha X + \beta Y, \gamma X + \delta Y) = \underline{X}^T A^T B_Q A \underline{X}.$$

More precisely, an integer r is represented by Q' only if it is represented by Q. We can reverse this process if A is an invertible integer matrix with inverse again an integer matrix, which is equivalent to $\det(A) = \pm 1$. All this motivates the following definition.

Definition 5.3. Two quadratic forms Q and Q' are said to be *equivalent* if there is some matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that

$$Q'(X,Y) = Q(\alpha X + \beta Y, \gamma X + \delta Y).$$

Lemma 5.4. *Equivalence of quadratic forms is and equivalence relation. Moreover, if Q and Q' are equivalent binary quadratic forms, then they represent the same integers and have the same discriminant.*

Proof. Let A be as in Definition 5.3. Then we have that

$$B_{Q'} = A^T B_Q A$$

and so the equivalence of quadratic forms is an equivalence relation. Moreover

$$d_{Q'} = -4 \det\left(B'_Q\right) = -4 \det\left(A^T B_Q A\right) = -4 \det(B_Q) \det(A)^2 = d_Q,$$

as $\det(A) = 1$. It remains, to show that if Q and Q' are equivalent binary quadratic forms, then they represent the same integers. So let r be an integer such that $r = Q(m,n)$ with $m, n \in \mathbb{Z}$. Then we have

$$r = \underline{m}^T B_Q \underline{m} = \underline{m}'^T A^T B_Q A \underline{m}' = \underline{m}'^T B_{Q'} \underline{m}',$$

where

$$\underline{m} = \begin{pmatrix} m \\ n \end{pmatrix}, \underline{m}' = A^{-1}\underline{m}.$$

So r is also represented by Q'. The converse follows by symmetry of the equivalence relation. □

It is not the case that any two quadratic forms with the same discriminant are equivalent. However the main aim of this subsection is to show that there are only finitely many equivalence classes of quadratic form for a fixed discriminant.

Denote by d a square-free integer write $K = \mathbb{Q}(\sqrt{d})$ and as usual denote by $\mathcal{O}_K$ the ring of integers and by d_K the discriminant of K. We want to relate to this setting a quadratic form with discriminant d_K. This is possible by considering the so-called *norm form* q_K defined by

$$q_K(X,Y) = N_{(K:\mathbb{Q})}(X + Y\sqrt{d}) = (X + Y\sqrt{d})(X - Y\sqrt{d}) = X^2 - dY^2$$

if $d \not\equiv 1 \mod 4$ and by

$$q_K(X,Y) = N_{(K:\mathbb{Q})}\left(X + Y\left(\frac{1+\sqrt{d}}{2}\right)\right) = X^2 + XY + \left(\frac{1-d}{4}\right)Y^2$$

if $d \equiv 1 \mod 4$. We note that in both cases the quadratic from q_K has discriminant d_K.

We first prove the following interesting relation.

Proposition 5.5. *Let Q be a binary quadratic form with square-free discriminant d_Q. If there is a number field $K = \mathbb{Q}(\sqrt{d})$ for d a square-free integer such that*

$$d_Q = d_K,$$

then Q is primitive, i.e. $\gcd(a,b,c) = 1$.

Proof. First assume that $d_K = d_Q \equiv 1 \mod 4$. If $\gcd(a,b,c) \neq 1$, then note that $d_K = d_Q = b^2 - 4ac$ is not square-free, a contradiction to the assumption.

If $d_K = d_Q \not\equiv 1 \mod 4$, then we have that $d_Q \equiv 0 \mod 4$. This shows $d_Q = d_K = 4d$ and $d \equiv 2, 3 \mod 4$. So we see that $\gcd(a,b,c)$ must divide 2 since otherwise we again have that d is not square-free (the case $\gcd(a,b,c)|2$ is possible as $d_Q = b^2 - 4ac = 4d$ and d is assumed to be square free). Assume next for a contradiction $\gcd(a,b,c) = 2$. So we have that

$$d = \frac{d_K}{4} = \left(\frac{b}{2}\right)^2 - 4\left(\frac{a}{2}\right)\left(\frac{c}{2}\right) \equiv \left(\frac{b}{2}\right)^2 \mod 4.$$

But then $d \not\equiv 2, 3 \mod 4$ as it a square $\mod 4$, which can't be. Thus $\gcd(a,b,c) = 1$. □

An integer d which satisfies $d \equiv 0, 1 \mod 4$ is called *fundamental* if d is either square-free, in which case $d \equiv 1 \mod 4$, or $\frac{d}{4}$ is a square-free integer congruent to $2, 3 \mod 4$. By the proof of the last proposition we see that a discriminant d_Q is fundamental if and only if it is the discriminant of a quadratic field. Moreover, any quadratic form with fundamental discriminant is primitive.

In the following discussion we always assume that d is a fundamental integer. Denote by

$$\begin{aligned} R_{\text{disc}}(d) &= \{Q(X,Y) = aX^2 + bXY + cY^2 \,:\, a,b,c \in \mathbb{Z} \text{ and } d_Q = d\} \\ &= \{Q(X,Y) = aX^2 + bXY + cY^2 \,:\, a,b,c \in \mathbb{Z}, d_Q = d \text{ and } \gcd(a,b,c) = 1\} \\ &\cong \{(a,b,c) \in \mathbb{Z}^3 \,:\, b^2 - 4ac = d \text{ and } \gcd(a,b,c) = 1\}. \end{aligned}$$

We denote by

$$\mathcal{Q}_d = \mathrm{SL}_2(\mathbb{Z}) \backslash R_{\text{disc}}(d)$$

the set of equivalence classes of quadratic forms. We next state and prove the main theorem of this section.

Theorem 5.6. *Let d be a fundamental integer and denote $K = \mathbb{Q}(\sqrt{d})$. Then there is a bijection between the narrow class group Cl_K^+ of K and the set of equivalence classes $\mathcal{Q}_d$ of quadratic forms with discriminant d.*

In the following we are going to construct the bijection, whose existence is claimed in Theorem 5.6. In order to achieve this we will need a few preliminarily recollections and remarks.

Denote by σ the non-trivial automorphism of K and let $\mathfrak{a} \subset \mathcal{O}_K$ be a fractional integral ideal with integral basis a_1, a_2. By Proposition 1.46 we have that

$$\det\left(\begin{pmatrix} a_1 & a_2 \\ \sigma a_1 & \sigma a_2 \end{pmatrix}\right)^2 = \mathfrak{N}(\mathfrak{a})^2 d_K.$$

We understand $\sqrt{d_K}$ always as the positive square root if $d_K > 0$ and as the square root with positive imaginary part if $d_K < 0$. We call the ordered basis (a_1, a_2) of $\mathfrak{a}$ *normalized* when

$$\det\left(\begin{pmatrix} a_1 & a_2 \\ \sigma a_1 & \sigma a_2 \end{pmatrix}\right) = \mathfrak{N}(\mathfrak{a})\sqrt{d_K}.$$

Note that given a basis $\{a_1, a_2\}$ of $\mathfrak{a}$, exactly one of the ordered bases (a_1, a_2) or (a_2, a_1) will be normalized.

Given a normalized basis (a_1, a_2) of $\mathfrak{a}$ we define the quadratic form

$$\begin{aligned} Q_{(a_1,a_2)}(X,Y) &= \mathfrak{N}(\mathfrak{a})^{-1} \mathrm{N}_{(K:\mathbb{Q})}(a_1 X + a_2 Y) \\ &= \mathfrak{N}(\mathfrak{a})^{-1}(a_1\sigma a_1 X^2 + (a_1\sigma a_2 + \sigma a_1 a_2)XY + a_2 \sigma a_2 Y^2). \end{aligned}$$

To see that this quadratic form is indeed well-defined, first observe that for any $x, y \in \mathbb{Z}$ we have $a_1 x + a_2 y \in \mathfrak{a}$. Furthermore, we note that if $b \in \mathfrak{a}$, then $(b) \subset \mathfrak{a}$ and so by Lemma 4.6

$$|\mathrm{N}_{(K:\mathbb{Q})}(b)| = \mathfrak{N}((b)) = (\mathcal{O}_K : \mathfrak{a})(\mathfrak{a} : (b)) = \mathfrak{N}(\mathfrak{a})$$

implying

$$\mathfrak{N}(\mathfrak{a}) \,|\, \mathrm{N}_{(K:\mathbb{Q})}(b)$$

and so the quadratic form is well-defined. Furthermore we have that

$$\begin{aligned} d_{Q_{(a_1,a_2)}} &= \frac{1}{\mathfrak{N}(\mathfrak{a})^2}((a_1\sigma a_2 + \sigma a_1 a_2)^2 - 4a_1\sigma a_1 \sigma a_1 a_2) \\ &= \frac{1}{\mathfrak{N}(\mathfrak{a})^2}(a_1\sigma a_2 - \sigma a_1 a_2)^2 \\ &= \frac{1}{\mathfrak{N}(\mathfrak{a})^2}\det\left(\begin{pmatrix} a_1 & a_2 \\ \sigma a_1 & \sigma a_2 \end{pmatrix}\right)^2 = d_K \end{aligned}$$

Next note the following. If we choose an alternative normalized basis (b_1, b_2) of $\mathfrak{a}$ we note that there is an invertible integral matrix $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with

$$\begin{pmatrix} b_1 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

As σ leaves integers invariant

$$\begin{pmatrix} b_1 & b_2 \\ \sigma b_1 & \sigma b_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ \sigma a_1 & \sigma a_2 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

Since both bases are normalized we have that $A \in \mathrm{SL}_2(\mathbb{Z})$. Note next that

$$\begin{aligned} Q_{(b_1,b_2)}(X,Y) &= \mathfrak{N}(\mathfrak{a})^{-1}(\mathrm{N}_{(K:\mathbb{Q})}(b_1X + b_2Y)) \\ &= \mathfrak{N}(\mathfrak{a})^{-1}(\mathrm{N}_{(K:\mathbb{Q})}((a_1\alpha + a_2\gamma)X + (a_1\beta + a_2\delta)Y)) \\ &= \mathfrak{N}(\mathfrak{a})^{-1}(\mathrm{N}_{(K:\mathbb{Q})}(((\alpha X + \beta Y)a_1 + (\gamma X + \delta Y)a_2)) \\ &= Q_{(a_1,a_2)}(\alpha X + \beta Y, \gamma X + \delta Y). \end{aligned}$$

So we see that $Q_{(b_1,b_2)}$ and $Q_{(a_1,a_2)}$ are equivalent.

Next consider the case where we replace $\mathfrak{a}$ be some element of the narrow class of $\mathfrak{a}$. So we consider $\mathfrak{b} = \alpha\mathfrak{a}$ for α totally positive. Then we have that αa_1 and αa_2 is an integral basis for $\mathfrak{b}$. Next note that as λ is totally positive

$$\begin{aligned} \det\left(\begin{pmatrix} \alpha a_1 & \alpha a_2 \\ \sigma\alpha\sigma a_1 & \sigma\alpha\sigma a_2 \end{pmatrix}\right) &= \alpha\sigma\alpha\det\left(\begin{pmatrix} a_1 & \sigma a_2 \\ a_1 & \sigma a_2 \end{pmatrix}\right) \\ &= N_{(K:\mathbb{Q})}(\alpha)\sqrt{d_K}\mathfrak{N}(\mathfrak{a}) = \sqrt{d_K}\mathfrak{N}(\alpha\mathfrak{a}). \end{aligned}$$

So $(\alpha a_1, \alpha a_2)$ is normalized and so $Q_{\alpha a_1, \alpha a_2}$ is a well-defined quadratic form. Again as $\mathrm{N}_{(K:\mathbb{Q})}(\alpha) = \mathfrak{N}((\alpha))$ as α is totally positive,

$$Q_{(\alpha a_1,\alpha a_2)}(X,Y) = \frac{N_{K:\mathbb{Q}}(\alpha a_1 X + \alpha a_2 Y)}{\mathfrak{N}(\alpha\mathfrak{a})} \tag{5.1}$$

$$= \frac{N_{K:\mathbb{Q}}(a_1 X + a_2 Y)}{\mathfrak{N}(\mathfrak{a})} = Q_{(a_1,a_2)}(X,Y) \tag{5.2}$$

and so the two forms are indeed equivalent.

We thus have constructed a map

$$\kappa : C_K^+ \to \mathcal{Q}_d.$$

Proof. (of Theorem 5.6) We prove that κ is bijective. We start with showing that κ is surjective. To see this let

$$Q(X,Y) = aX^2 + bXY + cY^2$$

be a quadratic form with discriminant d_K. Denote by $\mathfrak{a}$ the fractional ideal generated by a and $\frac{b-\sqrt{d_K}}{2}$.

Observe that

$$a\left(\frac{d_K+\sqrt{d_K}}{2}\right) = -a\left(\frac{(b-\sqrt{d_K})}{2}\right) + a\left(\frac{b+d_K}{2}\right).$$

As $d_K \equiv 2 \mod 4$ we have that

$$a\left(\frac{d_K+\sqrt{d_K}}{2}\right) \in \mathbb{Z}a \oplus \mathbb{Z}\left(\frac{b-\sqrt{d_K}}{2}\right).$$

Second we note

$$\begin{aligned}\left(\frac{d_K+\sqrt{d_K}}{2}\right)\left(\frac{b-\sqrt{d_K}}{2}\right) &= \frac{d_K}{2}\left(\frac{b-\sqrt{d_K}}{2}\right) + \frac{b\sqrt{d_K}-d_K}{4}\\ &= \frac{d_K}{2}\left(\frac{b-\sqrt{d_K}}{2}\right) + \frac{b\sqrt{d_K}-b^2+4ac}{4}\\ &= \left(\frac{d_K-b}{2}\right)\left(\frac{b-\sqrt{d_K}}{2}\right) + ac.\end{aligned}$$

So we have

$$\left(\frac{d_K+\sqrt{d_K}}{2}\right)\left(\frac{b-\sqrt{d_K}}{2}\right) \in \mathbb{Z}a \oplus \mathbb{Z}\left(\frac{b-\sqrt{d_K}}{2}\right).$$

Together this shows that

$$\left\{a, \frac{b-\sqrt{d_K}}{2}\right\}$$

is an integral basis of $\mathfrak{a}$ as $\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right]$.

If a is positive then we set $\alpha = 1$ and if a is negative we set $\alpha = \sqrt{d_K}$. To show that κ is surjective we consider the fractional ideal $\alpha\mathfrak{a}$ which has as explained above the integral basis $a_1 = \alpha a$ and $a_2 = \alpha\left(\frac{b-\sqrt{d_K}}{2}\right)$. We observe that this is a normalized basis as

$$\det\left(\begin{pmatrix} a_1 & a_2 \\ \sigma a_1 & \sigma a_2\end{pmatrix}\right) = \mathrm{N}_{(K:\mathbb{Q})}(\alpha)\det\left(\begin{pmatrix} a & \frac{b-\sqrt{d_K}}{2} \\ a & \frac{b+\sqrt{d_K}}{2}\end{pmatrix}\right) = \mathrm{N}_{(K:\mathbb{Q})}(\alpha)a\sqrt{d_K},$$

which shows that

$$\mathfrak{N}(\alpha\mathfrak{a}) = \mathrm{N}_{(K:\mathbb{Q})}(\alpha)a. \tag{5.3}$$

Finally we consider the quadratic form

$$\begin{aligned}Q_{(a_1,a_2)}(X,Y) &= \frac{\mathrm{N}_{(a_1,a_2)}(\alpha)}{\mathfrak{N}(\alpha\mathfrak{a})}\mathrm{N}_{(K:\mathbb{Q})}\left(aX + Y\left(\frac{b-\sqrt{d_K}}{2}\right)\right)\\ &= \frac{1}{a}\left(a^2X + abXY + Y^2\left(\frac{b^2-d_K}{4}\right)\right)\\ &= aX^2 + bXY + cY^2,\end{aligned}$$

where the second equal sign follows by (5.3) and the last equation follows as $d_K = b^2 - 4ac$. So we have showed that $\kappa([\mathfrak{a}]) = Q(X,Y)$.

It remains to prove that κ is injective. To see this let $\mathfrak{a}$ and $\mathfrak{b}$ be two fractional ideals with normalized bases (a_1, a_2) and (b_1, b_2) such that $Q_{(a_1,a_2)}(X,Y)$ is equivalent to $Q_{(b_1,b_2)}(X,Y)$. By a change of basis we may assume

$$Q_{(a_1,a_2)}(X,Y) = Q_{(b_1,b_2)}(X,Y).$$

We want to show that these is some $\alpha \in K$ totally positive, in this case $\mathrm{N}_{(K:\mathbb{Q})}(\alpha) > 0$, such that $\mathfrak{a} = \alpha\mathfrak{b}$.

Note that the form

$$Q_{(a_1,a_2)}(1,Y) = a_1\sigma a_1 + (a_1\sigma a_2 + a_2\sigma a_1)Y + a_2\sigma a_2 Y^2$$

is zero if

$$0 = \frac{a_1\sigma a_1}{a_2\sigma a_2} + (\frac{a_1}{a_2} + \frac{\sigma a_1}{\sigma a_2})Y + Y^2.$$

So it has the roots $-\frac{a_1}{a_2}$ and $-\frac{\sigma a_1}{\sigma a_2}$. We we conclude that as $Q_{(a_1,a_2)}(X,Y) = Q_{(b_1,b_2)}(X,Y)$ that either

$$\frac{a_1}{a_2} = \frac{b_1}{b_2} \quad \text{or} \quad \frac{a_1}{a_2} = \frac{\sigma b_1}{\sigma b_2}.$$

We shall see that only the first case is possible.

In the first case where $\frac{a_1}{a_2} = \frac{b_1}{b_2}$. We set

$$\alpha = \frac{a_1}{b_1} = \frac{a_2}{b_2}.$$

So $a_1 = \alpha b_1$ and $a_2 = \alpha b_2$ and hence $\mathfrak{a} = \alpha\mathfrak{b}$. Furthermore $\mathrm{N}_{(K:\mathbb{Q})}(\alpha) > 0$ as

$$\begin{aligned}\sqrt{d_K}\mathfrak{N}(\mathfrak{a}) = \det\left(\begin{pmatrix} a_1 & a_2 \\ \sigma a_1 & \sigma a_2 \end{pmatrix}\right) &= \mathrm{N}_{(K:\mathbb{Q})}(\alpha)\det\left(\begin{pmatrix} b_1 & b_2 \\ \sigma b_1 & \sigma b_2 \end{pmatrix}\right) \\ &= \mathrm{N}_{(K:\mathbb{Q})}(\alpha)\sqrt{d_K}\mathfrak{N}(\mathfrak{b}).\end{aligned}$$

For the second case where $\frac{a_1}{a_2} = \frac{\sigma b_1}{\sigma b_2}$ we set

$$\alpha = \frac{a_1}{\sigma b_1} = \frac{a_2}{\sigma b_2}$$

and so

$$\det\left(\begin{pmatrix} a_1 & a_2 \\ \sigma a_1 & \sigma a_2 \end{pmatrix}\right) = \mathrm{N}_{(K:\mathbb{Q})}(\alpha)\det\left(\begin{pmatrix} \sigma b_1 & \sigma b_2 \\ b_1 & b_2 \end{pmatrix}\right)$$

and again since both bases are normalized we deduce $N_{(K:\mathbb{Q})}(\alpha) < 0$. However we also have that

$$\begin{aligned}\frac{1}{\mathfrak{N}(\mathfrak{b})}(b_1X + b_2Y)(\sigma b_1 X + \sigma b_2 Y) &= Q_{(b_1,b_2)}(X,Y) \\ &= Q_{(a_1,a_2)}(X,Y) \\ &= \frac{1}{\mathfrak{N}(\mathfrak{a})}(a_1X + a_2Y)(\sigma a_1 X + \sigma a_2 Y) \\ &= \frac{1}{\mathfrak{N}(\mathfrak{a})}\alpha\sigma\alpha(\sigma b_1 X + \sigma b_2 Y)(b_1X + b_2Y).\end{aligned}$$

This shows that

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})\mathrm{N}_{(K:\mathbb{Q})}(\alpha)$$

which contradicts $N_{(K:\mathbb{Q})}(\alpha) < 0$ and hence the second case is impossible. □

5.3 Binary Quadratic Forms and Proper Ideals

In this section we generalize the main result of the last section to the case where d is a positive non-necessarily fundamental discriminant. More precisely we relate quadratic forms to proper ideals, a notion we already encountered in Sections 4.5 and 4.6. In contrast to the last section, we consider in this section the quaadratic forms up to $\mathrm{GL}_2(\mathbb{Z})$ equivalence, i.e. we say that two quadratic forms Q_1 and Q_2 are equivalent if there is a matrix $g \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$Q_1(X,Y) = \frac{1}{\det(g)} Q_2((X,Y)g).$$

Let $d > 0$ be a non-square discriminant, i.e. $\equiv 0, 1 \mod 4$ and denote as in Section 4.6 by $K = \mathbb{Q}(\sqrt{d})$ and $\mathcal{O}_d = \mathbb{Z}[\frac{d+\sqrt{d}}{2}]$. Furthermore, as before write

$$\begin{aligned} \mathrm{R}_{\mathrm{disc}}(d) &= \{Q(X,Y) = aX^2 + bXY + cY^2 \,:\, a,b,c \in \mathbb{Z}, d_Q = d \text{ and } \gcd(a,b,c) = 1\} \\ &\cong \{(a,b,c) \in \mathbb{Z}^3 \,:\, b^2 - 4ac = d, \text{ and } \gcd(a,b,c) = 1\}. \end{aligned}$$

Denote by $[R_{\mathrm{disc}}(d)]$ the set of $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of elements in $R_{\mathrm{disc}}(d)$. The central result of this section is the following.

Theorem 5.7. *The cardinality of* $[\mathrm{R}_{\mathrm{disc}}(d)]$ *is equal to the cardinality of* $\mathrm{Pic}(\mathcal{O}_d)$.

Instead of directly constructing a bijection between $\mathrm{Pic}(\mathcal{O}_d)$ and $[\mathrm{R}_{\mathrm{disc}}(d)]$, we first construct a bijection between $[\mathrm{R}_{\mathrm{disc}}(d)]$ and $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of so-called *optimal ring embeddings* $\mathcal{O}_d \to M_2(\mathbb{Z})$ and then a bijection between the latter set and $\mathrm{Pic}(\mathcal{O}_d)$. In order to proceed, we first discuss ring embeddings $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$ and then introduce the notion of an *optimal ring embedding*.

Denote by $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$ a ring embedding. By extending ι $\mathbb{Q}$-linearly, we arrive at a ring embedding $\iota : K \to M_2(\mathbb{Q})$ (by a slight abuse of notation we do not distinguish ι defined on $\mathcal{O}_d$ and ι defined on K). The ring embedding $\iota : K \to M_2(\mathbb{Q})$ is determined by the image of $\sqrt{d}$. More precisely, if

$$Z := \iota(\sqrt{d}) \in M_2(\mathbb{Q})$$

then

$$\iota(a + b\sqrt{d}) = a \cdot \mathrm{Id}_2 + b \cdot Z \tag{5.4}$$

for $a, b \in \mathbb{Q}$.

Moreover, we want to determine which further conditions the matrix

$$Z = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(\mathbb{Q})$$

has to satisfy such that $\iota(\mathcal{O}_K) \subset M_2(\mathbb{Z})$ and so that ι is a ring homomorphism. First ι is a ring homomorphism if and only if

$$d \cdot \mathrm{Id}_2 = \iota(d) = \iota(\sqrt{d})^2 = Z^2 = \begin{pmatrix} x^2 + yz & y(x+w) \\ z(x+w) & w^2 + yz \end{pmatrix}.$$

This shows that if $y, z \neq 0$ then $x = -w$ and so $\mathrm{tr}(Z) = 0$. Note that neither y nor z can be zero, as if for example $y = 0$ then

$$Z^2 = \begin{pmatrix} x^2 & 0 \\ z(x+w) & w^2 \end{pmatrix} = d \cdot \mathrm{Id}_2$$

and so $d = x^2$ for $x, w \in \mathbb{Q}$ contradicting the assumption that d is not a perfect square. So we see that $\iota : K \to M_2(\mathbb{Q})$ is a ring homomorphism if and only if $\mathrm{tr}(Z) = 0$ so that Z is of the form

$$Z = \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \in M_2(\mathbb{Q}).$$

We next determine for which such Z the map ι defined by (5.4) satisfies $\iota(\mathcal{O}_K) \subset M_2(\mathbb{Z})$. This is equivalent to

$$\begin{aligned} \iota\left(m + n(\tfrac{d+\sqrt{d}}{2})\right) &= \left(m + \frac{nd}{2}\right) \cdot \mathrm{Id}_2 + \frac{n}{2} Z \\ &= \begin{pmatrix} m + \frac{nd+nx}{2} & \frac{ny}{2} \\ \frac{nz}{z} & m + \frac{nd-nx}{2} \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) \end{aligned}$$

for all $m, n \in \mathbb{Z}$. This is equivalent to $y, z \in 2\mathbb{Z}$ and d and x having the same parity.

To summarize we have proved the following: The ring embeddings $\iota : K \to M_2(\mathbb{Q})$ are precisely given by the maps $\iota_Z : K \to M_2(\mathbb{Q})$ defined by

$$a + b\sqrt{d} \mapsto \iota_Z(a + b\sqrt{d}) = a \cdot \mathrm{Id}_2 + b \cdot Z \tag{5.5}$$

where $Z \in M_2(\mathbb{Q})$ of the form

$$Z = \begin{pmatrix} x & 2y \\ 2z & -x \end{pmatrix} \tag{5.6}$$

for $x, y, z \in \mathbb{Z}$ with $y, z \neq 0$ and where x has the same parity as d. We next define, what we mean by an *optimal embedding*.

Definition 5.8. Let $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$ be a ring embedding with extension $\iota_Z : K \to M_2(\mathbb{Q})$ (given by (5.5) and (5.6)). Then we say that the ring embedding ι is *optimal* if and only if

$$\iota_Z^{-1}(M_2(\mathbb{Z})) = \mathcal{O}_d \subset K.$$

In order to characterize optimal ring embeddings more easily we are going to calculate $\iota_Z^{-1}(M_2(\mathbb{Z}))$.

Proposition 5.9. *Let $\iota_Z : K \to M_2(\mathbb{Q})$ be a ring embedding given by* (5.5) *and* (5.6). *Then*

$$\iota_Z^{-1}(M_2(\mathbb{Z})) = \left\{ m + n\sqrt{d} \,:\, m \in \frac{1}{2}\mathbb{Z}, n \in \frac{1}{\gcd(2x, 2y, 2z)}\mathbb{Z} \text{ and } m + 2nx \in 2\mathbb{Z} \right\}.$$

Proof. The proof is simply a calculation: Let $a, b \in \mathbb{Q}$ with

$$\iota_Z(a + b\sqrt{d}) = a \cdot \mathrm{Id}_2 + bZ = \begin{pmatrix} a + bx & 2yb \\ 2zb & a - bx \end{pmatrix} \in M_2(\mathbb{Z}).$$

Adding the diagonal entries, we get

$$2a = (a + bx) + (a - bx) \in \mathbb{Z}$$

and so $a \in \frac{1}{2}\mathbb{Z}$. Moreover, considering the non-diagonal entries and using that y, z are both not zero we conclude $b \in \frac{1}{2y}\mathbb{Z}$ and $b \in \frac{1}{2z}\mathbb{Z}$. Write $a = \frac{m}{2}$ for $m \in \mathbb{Z}$. Then

$$a + bx = \frac{m}{2} + bx \in \mathbb{Z}$$

if any only if $m + 2bx \in 2\mathbb{Z}$, in particular $b \in \frac{1}{2x}\mathbb{Z}$. Thus $b \in \frac{1}{\gcd(2x,2y,2z)}\mathbb{Z}$. Hence

$$\iota_Z^{-1}(M_2(\mathbb{Z})) \subset \left\{ m + n\sqrt{d} \,:\, m \in \frac{1}{2}\mathbb{Z}, n \in \frac{1}{\gcd(2x, 2y, 2z)}\mathbb{Z} \text{ and } m + 2nx \in 2\mathbb{Z} \right\}$$

and the converse is obvious. □

Corollary 5.10. *Let $\iota_Z : K \to M_2(\mathbb{Q})$ be a ring embedding given by* (5.5) *and* (5.6)*. Then ι_Z is optimal if any only if* $\gcd(x, y, z) = 1$.

Proof. Note that

$$\begin{aligned} \mathbb{Z}\left[\frac{d + \sqrt{d}}{2}\right] &= \left\{ \frac{1}{2}m + \frac{1}{2}n\sqrt{d} \,:\, m, n \in \mathbb{Z} \text{ and } m + nd \in 2\mathbb{Z} \right\} \\ &= \left\{ \frac{1}{2}m + \frac{1}{2}n\sqrt{d} \,:\, m, n \in \mathbb{Z} \text{ and } m + nx \in 2\mathbb{Z} \right\} \end{aligned}$$

as x and d have the same parity as $Z^2 = d \cdot \mathrm{Id}_2$ and so $d = x^2 + 4yz$. □

For $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$ a ring embedding we can consider for each $g \in \mathrm{GL}_2(\mathbb{Z})$ then conjugate element

$$\iota^g : \mathcal{O}_d \to M_2(\mathbb{Z}), \qquad x \mapsto g\iota(x)g^{-1}.$$

We note that if $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$ is optimal, then so is every element from its $\mathrm{GL}_2(\mathbb{Z})$-conjugacy class. Using Corollary 5.10 we arrive at the aforementioned bijection between $[\mathrm{R}_{\mathrm{disc}}(d)]$ and the $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of optimal embeddings.

Proposition 5.11. *Let d be a non-square positive integer. Then there is a bijection between $[\mathrm{R}_{\mathrm{disc}}(d)]$ and the $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of optimal embeddings $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$.*

Proof. Note first that

$$Q(X, Y) : aX^2 + bXY + cY^2 \mapsto \begin{pmatrix} b & -2a \\ 2c & -b \end{pmatrix}$$

gives a bijection between the set of binary quadratic forms with discriminant d and trace-zero matrices. Moreover

$$d_Q = b^2 - 4ac = -\det \begin{pmatrix} b & -2a \\ 2c & -b \end{pmatrix}.$$

Via (5.5) and (5.6) this yields a bijection between quadratic forms with discriminant d, where d is not a perfect square, and ring embeddings $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$. Moreover by Corollary 5.10 we arrive at bijection between $\mathrm{R}_{\mathrm{disc}}(d)$ and optimal embeddings $\iota : \mathcal{O}_d \to M_2(\mathbb{Z})$.

Finally, the statement follows by noticing that if $g \in \mathrm{GL}_2(\mathbb{Z})$ we have that

$$g.(aX^2 + bXY + cY^2) \longleftrightarrow g \begin{pmatrix} b & -2a \\ 2c & -b \end{pmatrix} g^{-1}.$$

□

Next we show that the set of $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of optimal embeddings is in bijection with $\mathrm{Pic}(\mathcal{O}_d)$. The next proposition together with last proposition implies Theorem 5.7.

Proposition 5.12. *Let d be a non-square positive discriminant. Then there exists a bijection between $\mathrm{Pic}(\mathcal{O}_d)$ and the set of $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of optimal embeddings.*

Proof. Given a proper $\mathcal{O}_d$-ideal $\mathfrak{a} \subset K$ we choose an integral basis a_1, a_2 of $\mathfrak{a}$. This yields a bijection

$$\theta : \mathfrak{a} \to \mathbb{Z}^2, \qquad ma_1 + na_2 \mapsto (m, n).$$

The bijection θ induces the embedding

$$\iota : K \to M_2(\mathbb{Q}),$$

where we define for $\lambda \in K$ the matrix $\iota(\lambda) \in M_2(\mathbb{Q})$ implicitly by viewing $\iota(\lambda)$ by

$$\iota(\lambda)(p, q) = \theta(\lambda(pa_1 + qa_2))$$

for $p, q \in \mathbb{Q}$ or equivalently so that $\theta(\lambda \cdot x) = \iota(\lambda)\theta(x)$.

Note that

$$\begin{aligned} \iota^{-1}(M_2(\mathbb{Z})) &= \{\lambda \in K \,:\, \iota(\lambda)(m, n) \in \mathbb{Z}^2 \text{ for all } m, n \in \mathbb{Z}\} \\ &= \{\lambda \in K \,:\, \theta(\lambda(ma_1 + na_2)) \in \mathbb{Z}^2 \text{ for all } m, n \in \mathbb{Z}\} \\ &= \{\lambda \in K \,:\, \lambda\mathfrak{a} \subset \mathfrak{a}\}. \end{aligned}$$

So we see that $\iota^{-1}(M_2(\mathbb{Z})) = \mathcal{O}_d$ if and only if $\mathfrak{a}$ is a proper $\mathcal{O}_d$-ideal.

Next, we observe that if we replace the integral basis a_1, a_2 of $\mathfrak{a}$ by another integral basis a_1', a_2', then let $g = (z_{ij}) \in \mathrm{GL}_2(\mathbb{Z})$ be the change of basis matrix such that

$$a_i' = z_{i1}a_1 + z_{2i}a_2$$

for $i = 1, 2$. Write θ' and ι' for the analogously to θ and ι defined map with respect to the basis a_1', a_2'. Then if $m, n \in \mathbb{Z}$ we have that

$$\begin{aligned} \theta(ma_1' + na_2') &= \theta((mz_{11} + nz_{21})a_1 + (mz_{21} + nz_{22})a_1) \\ &= (mz_{11} + nz_{21}, mz_{21} + nz_{22})a_1) = g(m, n) = g\theta'(ma_1' + na_2'). \end{aligned}$$

Hence for $\lambda, x \in K$ we conclude

$$g^{-1}\iota(\lambda)g\theta'(x) = g^{-1}\iota(\lambda)\theta(x) = g^{-1}\theta(\lambda.x) = \theta'(\lambda.x)$$

and so $\iota'(\lambda) = g^{-1}\iota(\lambda)g$ showing that ι' and ι are in the same $\mathrm{GL}_2(\mathbb{Z})$-conjugacy class. Thus we arrive at a map

$$\begin{aligned} \{\text{proper } \mathcal{O}_d\text{-ideals}\} &\longrightarrow \{\text{optimal ring embeddings } \mathcal{O}_d \to M_2(\mathbb{Z})\}/\mathrm{GL}_2(\mathbb{Z}) \\ \mathfrak{a} &\longmapsto \iota_{\mathfrak{a}} \end{aligned}$$

If we replace $\mathfrak{a}$ by an element of the same ideal class $\mathfrak{a}' = \mu\mathfrak{a}$ for $\mu \in K^\times$. Then $\theta'(\mu x) = \theta(x)$ for $x \in \mathfrak{a}$ and so

$$\iota(\lambda)\theta(x) = \theta(\lambda x) = \theta'(\lambda\mu x) = \iota'(\lambda)\theta'(\mu x) = \iota'(\lambda)\theta(x)$$

showing that $\iota(\lambda) = \iota'(\lambda)$ and that the above map $\mathfrak{a} \mapsto \iota_{\mathfrak{a}}$ gives a well defined map $[\mathfrak{a}] \mapsto [\iota_{\mathfrak{a}}]$ defined on

$$\{\text{proper } \mathcal{O}_K\text{-ideals}\}/K^\times \longrightarrow \{\text{optimal ring embeddings } \mathcal{O}_K \to M_2(\mathbb{Z})\}/\mathrm{GL}_2(\mathbb{Z}).$$

We now give an inverse to the above map, showing that it is bijective. Let $\iota : K \to M_2(\mathbb{Q})$ be an optimal embedding of $\mathcal{O}_d$. Denote $e_1 = (1, 0) \in \mathbb{Z}^2$. The map

$$\psi : K \to \mathbb{Q}^2, \qquad \lambda \mapsto \iota(\lambda)e_1$$

is an isomorphism of $\mathbb{Q}$-vector spaces, as it is clearly linear and also injective by the characterization of optimal embeddings (5.5) and (5.6). Now set

$$\mathfrak{a}_\psi = \psi^{-1}(\mathbb{Z}^2) = \{\mu \in K \,:\, \iota(\mu)e_1 \in \mathbb{Z}^2\}$$

and we claim that $\mathfrak{a}_\psi$ is a proper $\mathcal{O}_d$-ideal. To see this first note that $\mathfrak{a}_\psi$ is a free $\mathbb{Z}$-module of rank 2 as ψ is an isomorphism of $\mathbb{Q}$-vector spaces. Now we show $\{\lambda \in K \,:\, \lambda\mathfrak{a}_\psi \subset \mathfrak{a}_\psi\} = \mathcal{O}_d$. So let $\lambda \in \mathcal{O}_d$. This follows as $\lambda \in \mathcal{O}_d$ if and only if multiplication by λ is represented by an integer matrix and so the claim follows.

It remains to check that the two maps are inverse to each other. First consider $\mathfrak{a}$ a proper $\mathcal{O}_d$-ideal and denote as above $i_{\mathfrak{a}} : K \to M_2(\mathbb{Q})$ the associated optimal ring embedding and by $\psi_{\mathfrak{a}} : K \to \mathbb{Q}^2, \lambda \mapsto \iota(\lambda)e_1$. We need to show that $\psi_{\mathfrak{a}}^{-1}(\mathbb{Z}^2)$ is in the same ideal class as $\mathfrak{a}$. We calculate

$$\begin{aligned}
\psi_{\mathfrak{a}}^{-1}(\mathbb{Z}^2) &= \{\lambda \in K \,:\, \theta(\lambda a_1) = \iota_{\mathfrak{a}}(\lambda)e_1 \in \mathbb{Z}^2\} \\
&= \{\lambda \in K \,:\, \lambda a_1 = ma_1 + na_2 \text{ for } m, n \in \mathbb{Z}\} \\
&= \{\lambda = \frac{ma_1 + na_2}{a_1} \text{ for } m, n \in \mathbb{Z}\} = \frac{\mathfrak{a}}{a_1}
\end{aligned}$$

and so $[\mathfrak{a}] = [\psi_{\mathfrak{a}}^{-1}(\mathbb{Z}^2)]$.

For the other direction let $\iota : K \to M_2(\mathbb{Q})$ be an optimal ring embedding with ψ defined as above. Let $\mathfrak{a} = \psi^{-1}(\mathbb{Z})$ and write $a_1 = \psi^{-1}((1, 0))$, $a_2 = \psi^{-1}((0, 1))$ so that a_1 and a_2 form an integral basis of $\mathfrak{a}$. Observe that

$$\theta : \mathfrak{a} \to \mathbb{Z}^2, \qquad ma_1 + na_2 = \psi^{-1}((m, n)) \mapsto (m, n).$$

So $\theta \circ \psi^{-1} = \mathrm{id}$ so $\theta = \psi$ as both maps are bijective. Thus, in this case $\iota_{\mathfrak{a}}$ is given as

$$\iota_{\mathfrak{a}}(\lambda)(m, n) = \theta(\lambda(ma_1 + na_2)) = \psi(\lambda(ma_1 + na_2)).$$

Thus, viewing $\iota_{\mathfrak{a}}(\lambda)$ as a matrix we conclude

$$\begin{aligned}
\iota_{\mathfrak{a}}(\lambda) = (\iota_{\mathfrak{a}}(\lambda)(1, 0) \quad \iota_{\mathfrak{a}}(\lambda)(0, 1)) &= (\psi(\lambda a_1) \quad \psi(\lambda a_2)) \\
&= (\iota(\lambda a_1)e_1 \quad \iota(\lambda a_1)e_1) \\
&= (\iota(\lambda)\iota(a_1)e_1 \quad \iota(\lambda)\iota(a_2)e_1) \\
&= \iota(\lambda)(\iota(a_1)e_1 \quad \iota(a_2)e_1) \\
&= \iota(\lambda)
\end{aligned}$$

as $\iota(a_1)e_1 = \psi(a_1) = \psi(\psi^{-1}(1, 0)) = (1, 0)$ and analogously $\iota(a_2)e_1 == (0, 1)$. Thus $\iota_{\mathfrak{a}} = \iota$. Thus we have showed that the maps are inverse to each other. □

5.4 Binary Quadratic Forms and Duke's Theorem

Let $X = \mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})$. In this section we first give a different viewpoint on the collection of geodesics

$$\mathcal{G}_d = \bigcup_{\mathfrak{a}\in \mathrm{Pic}(\mathcal{O}_d)} x_{\mathfrak{a}}.A \tag{5.7}$$

constructed in Section 4.6 based on quadratic forms.

We use the same notation as in the previous section for $\mathcal{Q}_d$ and $\mathrm{R}_{\mathrm{disc}}(d)$ for d a positive discriminant. The group $\mathrm{GL}_2(\mathbb{R})$ acts on $\mathcal{Q}_d$ or $\mathrm{R}_{\mathrm{disc}}(d)$ for $g \in \mathrm{GL}_2(\mathbb{R})$ by

$$(g.Q)(X,Y) = \frac{1}{\det(g)} Q((X,Y)g)$$

for $Q \in \mathrm{Q}_d$. The above action factors through an action of $\mathrm{PGL}_2(\mathbb{R})$. Viewing the space of quadratic forms as part of the space of symmetric matrices, where each quadratic form $Q(X,Y) = aX^2 + bXY + cY^2$ is represented as

$$B_Q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

the above action intertwines with the action

$$g.Q \quad \longleftrightarrow \quad \frac{1}{\det(g)} g \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} g^T.$$

Let $d \geq 0$ be a non-square discriminant. Then for $(a,b,c) \in \mathrm{R}_{disc}(d)$ we consider the points on the real line

$$x_{a,b,c,\pm} = \frac{-b \pm \sqrt{d}}{2a},$$

which only depend on the $\mathrm{GL}_2(\mathbb{Z})$-orbit of (a,b,c). Viewing $x_{a,b,c,\pm}$ as elements of the boundary of $\mathbb{H}$ there exists a uniquely determined geodesic on $\mathbb{H}$ with endpoints $x_{a,b,c,\pm}$. We denote by $\gamma_{(a,b,c)}$ the lifting of the geodesic to the unit tangent bundle of $\mathbb{H}$. Moreover, we can view the geodesic $\gamma_{(a,b,c)}$ as an A-orbit in $X \cong T^1(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H})$, which we denote by $\gamma^X_{(a,b,c)}$. So we can consider the finite collection of curves

$$\bigcup_{(a,b,c)\in[\mathrm{R}_{\mathrm{disc}}(d)]} \gamma^X_{(a,b,c)}. \tag{5.8}$$

The first goal of this section is to show that this latter collection of curves equals the collection of periodic A-orbits $\mathcal{G}_d$.

For $(a,b,c) \in \mathrm{R}_{disc}(d)$ we denote

$$h_{a,b,c} = \begin{pmatrix} b+\sqrt{d} & b-\sqrt{d} \\ 2c & 2c \end{pmatrix} \quad \text{and} \quad w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Then $wh_{a,b,c} = \left(\begin{smallmatrix} -2c & -2c \\ b+\sqrt{d} & b-\sqrt{d} \end{smallmatrix}\right)$ and so

$$wh_{a,b,c}.0 = -\frac{2c}{b-\sqrt{d}} = -\frac{2c}{b-\sqrt{d}}\frac{b+\sqrt{d}}{b+\sqrt{d}} = \frac{-2cb-2c\sqrt{d}}{-4ac} = \frac{b+\sqrt{d}}{2a}$$

and

$$wh_{a,b,c}.\infty = -\frac{2c}{b+\sqrt{d}} = -\frac{2c}{b+\sqrt{d}}\frac{b-\sqrt{d}}{b-\sqrt{d}} = \frac{-2cb+2c\sqrt{d}}{-4ac} = \frac{b-\sqrt{d}}{2a}.$$

This shows that $h_{a,b,c}.A$ corresponds to $\gamma_{(a,b,c)}$. Furthermore we calculate

$$\frac{1}{\det(h_{a,b,c})}h_{a,b,c}\begin{pmatrix}0 & \frac{1}{2}\\ \frac{1}{2} & 0\end{pmatrix}h_{a,b,c}^T = \frac{1}{4c\sqrt{d}}\begin{pmatrix}b^2-d & 2cb\\ 2cb & 4c^2\end{pmatrix} = \frac{1}{\sqrt{d}}\begin{pmatrix}a & \frac{b}{2}\\ \frac{b}{2} & c\end{pmatrix}.$$

Denote the quadratic from $Q_0(X,Y) = XY$. Then the above calculation shows that

$$\sqrt{d}(h_{a,b,c}.Q_0)(X,Y) = aX^2 + bXY + cY^2$$

As A is the stabilizer subgroup of Q_0 this shows that $\gamma_{(a,b,c)}$ corresponds to the elements $h \in \mathrm{SL}_2(\mathbb{R})$ such that

$$\sqrt{d}(h.Q_0)(X,Y) = aX^2 + bXY + cY^2.$$

Furthermore, $\gamma^X_{(a,b,c)}$ consists of all elements $x = \Gamma g \in X$ such that $\sqrt{d}(h.Q_0)(X,Y)$ is in the same $\mathrm{GL}_2(\mathbb{Z})$-equivalence class as $aX^2 + bXY + cY^2$.

Now consider the proper $\mathcal{O}_d$-ideal $\mathfrak{a}$ and denote by $(a_\mathfrak{a}, b_\mathfrak{a}, c_\mathfrak{a})$ the element of $\mathrm{R}_{\mathrm{disc}}(d)$ given by the bijection of Theorem 5.7. In Section **??** we used the norm form $Q_\mathfrak{a}$ defined for any integral basis a_1, a_2 by

$$Q_\mathfrak{a}(X,Y) = \frac{\mathrm{N}_{(K:\mathbb{Q})}(a_1X + a_2Y)}{\mathrm{N}(\mathfrak{a})}$$

which neither depends on the choice of integral basis nor on the ideal class of $\mathfrak{a}$.

In order to show that the collections 5.7 and 5.8 are the same it suffices to show $x_\mathfrak{a}.A = \gamma_{(a_\mathfrak{a},b_\mathfrak{a},c_\mathfrak{a})}$, which follows as above by showing that $\sqrt{d}(x_\mathfrak{a}.Q_0)(X,Y)$ is in the same $\mathrm{GL}_2(\mathbb{Z})$-equivalence class as

$$a_\mathfrak{a}X^2 + b_\mathfrak{a}XY + c_\mathfrak{a}Y^2.$$

Fix a_1 and a_2 an integral basis of $\mathfrak{a}$ such that

$$x_\mathfrak{a} = \begin{pmatrix}a_1 & \sigma(a_1)\\ a_2 & \sigma(a_2)\end{pmatrix}$$

has positive determinant, i.e. such that $\det(x_\mathfrak{a}) = \sqrt{d(\mathfrak{a})}$. Then as

$$\begin{aligned}\sqrt{d}(x_\mathfrak{a}.Q_0)(X,Y) &= \frac{\sqrt{d}}{d(\mathfrak{a})}Q_0(a_1X + a_2Y, \sigma(a_1X + a_2Y))\\ &= \frac{\sqrt{d}}{\sqrt{d(\mathfrak{a})}}\mathrm{N}_{(K:\mathbb{Q})}(a_1X + a_2Y)\\ &= \frac{\mathrm{N}_{(K:\mathbb{Q})}(a_1X + a_2Y)}{\mathfrak{N}(\mathfrak{a})} = Q_\mathfrak{a}(X,Y)\end{aligned}$$

we have that $\sqrt{d}(x_\mathfrak{a}.Q_0)(X,Y)$ is the norm form $Q_\mathfrak{a}(X,Y)$ we already encountered in the previous subsections. So we need to show that the norm form $Q_\mathfrak{a}(X,Y)$ is in the same $\mathrm{GL}_2(\mathbb{Z})$-equivalence class as $a_\mathfrak{a}X^2 + b_\mathfrak{a}XY + c_\mathfrak{a}Y^2$.

Explicitly considering the bijection from section 5.3, observe (using the same notation as in section 5.3) that

$$\iota_{\mathfrak{a}}(\sqrt{d}) = \begin{pmatrix} b_{\mathfrak{a}} & -2a_{\mathfrak{a}} \\ 2c_{\mathfrak{a}} & -b_{\mathfrak{a}} \end{pmatrix},$$

where $\iota_{\mathfrak{a}}(\sqrt{d})$ is the uniquely determined matrix in $\mathrm{GL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \sqrt{d}a_1 \\ \sqrt{d}a_2 \end{pmatrix} = \iota_{\mathfrak{a}}(\sqrt{d}) \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} b_{\mathfrak{a}}a_1 - 2a_{\mathfrak{a}}a_2 \\ 2c_{\mathfrak{a}}a_1 - b_{\mathfrak{a}}a_2 \end{pmatrix}$$

We note that

$$Q_{\mathfrak{a}}(X,Y) = \frac{a_1\sigma(a_1)X^2 + (a_1\sigma(a_2) + a_2\sigma(a_1))XY + a_2\sigma(a_2)Y^2}{\mathfrak{N}(\mathfrak{a})}.$$

We calculate

$$\frac{(a_1\sigma(a_2) + a_2\sigma(a_1))a_1 - 2a_1\sigma(a_1)a_2}{\mathfrak{N}(\mathfrak{a})} = \frac{d(\mathfrak{a})a_1}{\mathfrak{N}(\mathfrak{a})} = \sqrt{d}a_1$$

and

$$\frac{(2a_2\sigma(a_2)a_1 - (a_1\sigma(a_2) + a_2\sigma(a_1))a_2}{\mathfrak{N}(\mathfrak{a})} = \frac{d(\mathfrak{a})a_2}{\mathfrak{N}(\mathfrak{a})} = \sqrt{d}a_2$$

and thus

$$Q_{\mathfrak{a}}(X,Y) = a_{\mathfrak{a}}X^2 + b_{\mathfrak{a}}XY + c_{\mathfrak{a}}Y^2,$$

implying the claim.

Recall from Section 4.6 the height of a lattice $L = \mathbb{Z}^2 g$ with $g \in \mathrm{GL}_2(\mathbb{R})$ to be

$$\mathrm{ht}(L) = \left(\frac{\min_{v \in L\setminus\{0\}} ||v||}{\mathrm{vol}(L)^{1/2}}\right)^{-1} = \left(\frac{\min_{x \in \mathbb{Z}^2\setminus\{0\}} ||xg||}{|\det(g)|^{1/2}}\right)^{-1}$$

and denote

$$X_{\geq H} = \{x \in X \,:\, \mathrm{ht}(x) \leq H\}.$$

The aim of the remainder of this subsection is to prove the following proposition.

Proposition 5.13. *For any $\varepsilon > 0$,*

$$(\mu_d \times \mu_d)\left(\{(x,y) \in X^2_{\leq H} \,:\, d_X(x,y) < \delta\}\right) \ll_\varepsilon H^4 d^3 d^\varepsilon$$

for $d^{-\frac{1}{4}} \leq \delta \leq \frac{1}{3}H^{-2}$ and $H \geq 1$ large.

Before proving Proposition 5.13 we make short digression on the representation of quadratic from. Let q be an integral quadratic form in n-variables and let Q one in m-variables, where we assume $n \leq m$. We call $\mathbb{Z}-$linear map $\iota : \mathbb{Z}^n \to \mathbb{Z}^m$ a *representation* of q by Q if for all $x \in \mathbb{Z}^n$ we have

$$Q(\iota(x)) = q(x).$$

Denote by $R_Q(q)$ the set of such representations. We write

$$\mathrm{SO}_Q(\mathbb{Z}) = \{A \in M_m(\mathbb{Z}) \,:\, Q(Ax) = Q(x) \text{ for all } x \in \mathbb{Z}^m\}$$

for the special orthogonal group with respect to Q. Then $\mathrm{SO}_{\mathbb{Q}}$ naturally acts on the set $R_Q(q)$ and the quotient $\mathrm{SO}_Q(\mathbb{Z})\backslash R_Q(q)$ is finite.

For a more extended discussion concerning the representation of integral quadratic forms we refer to section 3.2 of [ELMV12]. We will be only interested in the representation of the quadratic form $q(X,Y) = dX^2 + \ell XY + dY^2$ for d as above and ℓ some integer by the ternary from given by the discriminant $\mathrm{disc}(X,Y,Z) = Y^2 - 4XZ$. In this situation the following result holds.

Corollary 5.14. *(Corollary 3.5 of [ELMV12]) Assume that $\ell \neq \pm 2d$, then*

$$|\mathrm{SO}_{\mathrm{disc}}(\mathbb{Z})\backslash\{(\mathbb{Z}^2, dX^2 + \ell XY + dY^2) \hookrightarrow (\mathbb{Z}^3, \mathrm{disc})\}| \ll_\varepsilon f \max(|d|,|\ell|)^\varepsilon$$

where f^2 is the largest square divisor of $\gcd(d,\ell)$.

Moreover, we next explain how we can embed $\mathrm{PGL}_2(\mathbb{Z})$ into $\mathrm{SO}_{\mathrm{disc}}(\mathbb{Z})$. We note that $\mathbb{Z}^3$ can be viewed as the space of binary integral quadratic forms. As the action of $\mathrm{PGL}_2(\mathbb{Z})$ on this latter space preserves the discriminant, each element of $\mathrm{PGL}_2(\mathbb{Z})$ corresponds to a uniquely determined element of $\mathrm{SO}_{\mathrm{disc}}(\mathbb{Z})$. As $\mathrm{SO}_{\mathrm{disc}}$ is rationally equivalent to PGL_2 it follows that we can replace in the statement of 5.14 the group $\mathrm{SO}_{\mathrm{disc}}(\mathbb{Z})$ by the image of $\mathrm{SL}_2(\mathbb{Z})$ under this injection. Thus

$$|\mathrm{SL}_2(\mathbb{Z})\backslash\{(\mathbb{Z}^2, dX^2 + \ell XY + dY^2) \hookrightarrow (\mathbb{Z}^3, \mathrm{disc})\}| \ll_\varepsilon f \max(|d|,|\ell|)^\varepsilon \qquad (5.9)$$

We now turn towards proving Proposition 5.13. Denote by $\mathscr{F}$ the fundamental domain of X given by

$$\mathscr{F} = \{(z,v) \in \mathbb{H} \times S^1 \text{ such that } |\mathrm{Re}(z)| \leq \tfrac{1}{2} \text{ and } |z| \geq 1\}$$

and by $\mathscr{F}'$ a slight extension of $\mathscr{F}'$ given by

$$\mathscr{F}' = \{(z,v) \in \mathbb{H} \times S^1 \text{ such that } |\mathrm{Re}(z)| \leq 1 \text{ and } |z| \geq \tfrac{1}{2}\}.$$

We progress by a few preliminary observations. Let $x_1, x_2 \in X_{\leq H}$ such that $d_X(x_1,x_2) < \delta$. Write $x_i = \Gamma g_i$ for $i = 1,2$ and $g_i \in \mathrm{PGL}_2(\mathbb{R})$. In order to bound coefficients of g_i, we always assume that the matrix g_i has determinant ± 1.

We choose g_1 such that $g_1 \in \mathscr{F}$ and $g_2 \in \mathrm{PGL}_2(\mathbb{R})$ such that $d_G(g_1,g_2) < \delta$ and so for δ sufficiently small, $g_2 \in \mathscr{F}'$. We claim that $||g_i|| \ll H$. We assume without loss of generality that g_1 has determinant 1. We use the NAK decomposition of $\mathrm{SL}_2(\mathbb{R})$ in order to write

$$g_1 = \begin{pmatrix} a & t \\ 0 & a^{-1} \end{pmatrix} k$$

$a, t \in \mathbb{R}$ with $a \neq 0$ and for $k \in \mathrm{SO}_2(\mathbb{R})$. As $g_1 \in \mathscr{F} \cap X_{\leq H}$ we conclude that $\mathrm{Re}(g_1.i) \leq 1$ and $\frac{1}{2} \leq \mathrm{Im}(g_1.i) \leq H^2$. We note that

$$g_1.i = a^2 i + at$$

and so $\frac{1}{2} \leq |a| \leq H$ and $|t| \leq \frac{1}{|a|} \leq 2$. Thus all the coefficients of g_1 are $\ll H$. As g_2 is close to g_1 we conclude that $||g_i|| \ll H$.

We now associate to g_i the primitive integral quadratic form

$$q_i(X,Y) = \sqrt{d}[g_i.q_0](X,Y) = a_iX^2 + b_iXY + c_iY^2$$

with $d = b_i^2 - 4a_ic_i$ and $\gcd(a_i, b_i, c_i) = 1$. Towards the estimate of Proposition 5.13 the case where $q_1 = q_2$ will be easier, so we focus on the case $q_1 \neq q_2$. We want to count the number of such possible tuples g_1, g_2 such that $q_1 \neq q_2$. By compactness of $\mathcal{G}_d$ the number of distinct such quadratic form is finite and we write

$$\Gamma(q_1^{(1)}, q_2^{(1)}), \dots, \Gamma(q_1^{(k)}, q_2^{(k)})$$

for a complete list of such quadratic forms. Our first aim is to count k effectively.

Lemma 5.15. *In the above setting,*

$$k \ll_\varepsilon d^{1+2\varepsilon} H^4 \delta^2.$$

Proof. As $||g_i|| \ll H$, it follows that

$$\max(|a_i|, |b_i|, |c_i|) \ll d^{1/2} H^2$$

and as by assumption $g_2 = g_1 h$ for $d(h, \mathrm{id}) < \delta$ we conclude that $q_2 = \sqrt{d} g_1(h.q_0)$ with $||h.q_0 - q_0|| \ll \delta$ and so

$$\max(|a_1 - a_2|, |b_1 - b_2|, |c_1 - c_2|) \ll d^{1/2} H^2 \delta. \tag{5.10}$$

We now define the quadratic form

$$q(X,Y) = \mathrm{disc}(X(a_1, b_1, c_1) + Y(a_2, b_2, c_2)) = dX^2 + \ell XY + dY^2$$

for $\ell \in \mathbb{Z}$. Thus the map

$$\iota : \mathbb{Z}^2 \to \mathbb{Z}^3, \quad \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \\ c_1 & c_2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

defines a representation of $dX^2 + \ell XY + dY^2$ by disc.

Note that

$$|2d - \ell| = |q(1, -1)| = \mathrm{disc}(a_1 - a_2, b_1 - b_2, c_1 - c_2) \ll dH^4\delta^2$$

and so there is only a finite number of possible values for ℓ. Furthermore, assuming that $q_1 \neq q_2$ we show that $\ell \neq \pm 2d$. Indeed, if $\ell = \pm 2d$, then

$$\begin{aligned} d(a_2 \mp a_1)^2 &= da_2^2 \mp 2da_2a_1 + da_1^2 = q(a_2, -a_1) \\ &= \mathrm{disc}(a_2(a_1b_1c_1) - a_1(a_2, b_2, c_2)) = (a_2b_1 - a_1b_2)^2 \end{aligned}$$

which contradicts the assumption that d is not a perfect square. So by (5.9),

$$N_{\ell,d} = |\mathrm{SL}_2(\mathbb{Z}) \backslash \{(\mathbb{Z}^2, dX^2 + \ell XY + dY^2) \hookrightarrow (\mathbb{Z}^3, \mathrm{disc})\}| \ll_\varepsilon f \max(|d|, |\ell|)^\varepsilon$$

and so $N_{\ell,d} \ll f d^\varepsilon$ as $d \geq 0$ and as by (5.10)

$$|\ell| \ll |\ell - 2d| + 2d \ll 2d + dH^4\delta^2 \ll d$$

as $d^{-1/4} \leq \delta \leq H^{-2}$.

If $\Gamma(q_1^{(i)}, q_2^{(i)})$ and $\Gamma(q_1^{(j)}, q_2^{(j)})$ are different then they define different embeddings up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence, where we view $\mathrm{SL}_2(\mathbb{Z}) \hookrightarrow \mathrm{SO}_{\mathrm{disc}}(\mathbb{Z})$. Thus

$$\begin{aligned} k &\leq \sum_{\text{all possible } \ell} N_{\ell,d} \\ &\leq \sum_{f^2|d} \sum_{\text{all possible } \ell} f d^{\varepsilon} \\ &\ll \sum_{f^2|d} f d^{\varepsilon} \frac{dH^4\delta^2}{f^2} \\ &\ll \sum_{f^2|d} d^{1+\varepsilon} H^4 \delta^2 \\ &\ll_{\varepsilon} d^{1+2\varepsilon} H^4 \delta^2, \end{aligned}$$

where in the third line we used that ℓ has to satisfy $|2d - \ell| \ll dH^4\delta^2$ and $f^2|\ell$ so that $\frac{\gcd(\ell,\delta)}{f^2}$ is square-free. In the last line we used that the number of divisors of d can be bounded by $\ll_{\varepsilon} d^{\varepsilon}$ for any $\varepsilon > 0$. □

Lemma 5.16. *Let $(x_1, x_2) = (\Gamma g_1, \Gamma g_2) \in (\mathcal{G}_d \cap X_{\leq H})^2$ be as above such that $d_X(x_1, x_2) < \delta$ and $q_1 \neq q_2$. Then there some j so that $x_1 = \Gamma g_1^{(j)} a_t$ where $t \in I_j$ for I_j some interval of length $\ll \log(d)$.*

Proof. Choose j so that $(\sqrt{d}(g_1.q.0), \sqrt{d}(g_2.q.0)) = (q_1^{(j)}, q_2^{(j)})$. We note that $\mathcal{G}_d \subset X_{<d^{1/4}}$ and so using (5.10) there is a constant c so that

$$\max(|a_1 - a_2|, |b_1 - b_2|, |c_1 - c_2|) \leq cd^{1/2}(d^{1/4})^2\delta \leq cd\delta.$$

Thus $d(g_1 a_t, g_2 a_t') \geq \frac{1}{2c} d^{-1}$. In particular, $d(g_1 a_t, g_2 A) \geq \frac{1}{2c} d^{-1}$. So it follows that for any j the inequality $d(g_1 a_t, g_2 A) < 1$ can only hold in an interval of length $\ll \log(d)$. □

Proof. (of Proposition 5.13) Let $(x_1, x_2) = (\Gamma g_1, \Gamma g_2) \in (\mathcal{G}_d \cap X_{\leq H})^2$ be such that $d_X(x_1, x_2) < \delta$ for g_1, g_2 as above. Then as before we associate to x_i the quadratic form $q_i = \sqrt{d}(g_i.q_0)(X, Y)$. Recall that $\mathrm{lenght}(\mathcal{G}_d^2) = d^{1+o(1)}$. So it suffices to show that

$$\mathrm{length}(\{(x, y) \in (\mathcal{G}_d \cap X_{\leq H})^2 \,:\, d_X(x, y) < \delta\}) \ll_{\varepsilon} H^4\delta^3 d^{1+\varepsilon}$$

If $q_1 = q_2$ then x_1 and x_2 lie on the same geodesic and so in this case we have that all these points can be described by

$$\{(x, xa_t) \in (\mathcal{G}_d \cap X_{\leq H})^2 \,:\, |t| \ll \delta\} \subset \{(x, xa_t) \in (\mathcal{G}_d)^2 \,:\, |t| \ll \delta\}.$$

Thus we have $\mathrm{length}(\{(x, xa_t) \in (\mathcal{G}_d \cap X_{\leq H})^2 \,:\, |t| \ll \delta\}) \ll \delta \cdot \mathrm{length}(\mathcal{G}_d) \ll_{\varepsilon} \delta d^{\frac{1}{2}+\varepsilon}$ so as $d^{-1/4} \leq \delta$,

$$(\mu_d \times \mu_d)(\{(x, xa_t) \in (\mathcal{G}_d \cap X_{\leq H})^2 \,:\, |t| \ll \delta\}) \ll_{\varepsilon} \delta d^{-1/2} d^{\varepsilon} \ll_{\varepsilon} \delta^3 d^{\varepsilon}.$$

In the case $q_1 \neq q_2$ Lemma 5.15 and Lemma 5.16 apply and so the length of the set

$$\{(x_1, x_2) \in (\mathcal{G}_d \cap X_{\leq H})^2 \,:\, d_X(x_1, x_2) < \delta \text{ and } q_1 \neq q_2\}$$

can be bounded by $\sum_{j=1}^{k} |I_j|\delta \ll \log(d) k\delta \ll_{\varepsilon} H^4\delta^3 d^{1+2\varepsilon}$. □

6 p-adic Numbers

6.1 Definition of the p-adic Numbers

Definition 6.1. A *valuation* on a field K is a map

$$|\cdot| : K \to \mathbb{R}_{\geq 0}$$

such that the following three conditions hold:

1. $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x|\,|y|$ for all $x, y \in K$.
3. $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

We furthermore call the valuation $|\cdot|$ *non-Archimedean* if it satisfies the additional condition

$$|x + y| \leq \max(|x|, |y|)$$

for all $x, y \in K$.

Let p be a prime number. We consider the field of rational numbers $\mathbb{Q}$ together with the *p-adic valuation*

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

where we define the *p-adic order* of x as

$$\mathrm{ord}_p(x) = \begin{cases} \text{the highest power of } p \text{ that divides } x & \text{if } x \in \mathbb{Z}, \\ \mathrm{ord}_p a - \mathrm{ord}_p b & \text{if } x = \frac{a}{b} \text{ with } a, b \in \mathbb{Z} \text{ and } b \neq 0. \end{cases}$$

Example 6.2. If $p = 2$, then we have that

$$\mathrm{ord}_2(1) = 0, \quad \mathrm{ord}_2(2) = 1, \quad \mathrm{ord}_2(3) = 0, \quad \mathrm{ord}_2(4) = 2, \quad \mathrm{ord}_2(5) = 0$$

and hence

$$|2|_2 = 2^{-1}, \qquad |1|_2 = |3|_2 = |5|_2 = 1, \qquad |\tfrac{1}{2}|_2 = 2, \quad \text{and} \quad |\tfrac{3}{4}|_2 = |\tfrac{1}{4}|_2 = 4.$$

The next theorem states that $|\cdot|_p$ indeed defines a valuation on $\mathbb{Q}$.

Theorem 6.3. *For any prime number p, the function $|\cdot|_p$ defines non-Archimedean valuation on the field $\mathbb{Q}$.*

Proof. It is clear that $|x|_p = 0$ whenever $x = 0$. For the proof of the remaining properties the case when $x = 0$ or $y = 0$ is clear. Next note that

$$\mathrm{ord}_p(x \cdot y) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$$

for all $x, y \in \mathbb{Q}\backslash\{0\}$ and hence

$$||x \cdot y|| = p^{-\mathrm{ord}_p(x \cdot y)} = p^{-(\mathrm{ord}_p(x) + \mathrm{ord}_p(y))} = ||x||\,||y||.$$

To prove that the norm is non-Archimedean, it suffices to prove for all $x, y \in \mathbb{Q}\backslash\{0\}$ that

$$\mathrm{ord}_p(x+y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}.$$

This property also implies the triangle inequality.

The prove the above equation it suffices to consider

$$x = \frac{p^{n_x}}{p^{m_x}} \qquad \text{and} \qquad y = \frac{p^{n_y}}{p^{m_y}}$$

for positive integers n_x, m_x, n_y and m_y. Then

$$\begin{aligned}\mathrm{ord}_p(x+y) &= \mathrm{ord}_p\left(\frac{p^{n_x+m_y}+p^{n_y+m_x}}{p^{m_x+m_y}}\right)\\ &= \min\{n_x+m_y, n_y+m_x\} - (m_x+m_y)\\ &= \min\{n_x-m_x, n_y-m_y\}\\ &= \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}.\end{aligned}$$

□

Definition 6.4. The *p-adic numbers* $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ with respect to the valuation $|\cdot|_p$.

We give an explicit construction of the p-adic numbers, which will show that the p-adic numbers form a field.

Denote by R the set of Cauchy sequences of $\mathbb{Q}$ with respect to $|\cdot|_p$. Note that R can be considered as a ring if we define addition and multiplication of two Cauchy sequences $x = (x_1, x_2, x_3, \ldots)$ and $y = (y_1, y_2, y_3, \ldots)$ as

$$x+y = (x_1+y_1, x_2+y_2, x_3+y_3, \ldots) \quad \text{and} \quad x\cdot y = (x_1\cdot y_1, x_2\cdot y_2, x_3\cdot y_3, \ldots).$$

These operations are well-defined as $x+y$ and $x\cdot y$ are again Cauchy sequences, as a straightforward verification proves. Furthermore $0_R = (0,0,0,\ldots)$ forms a neutral element for the addition and $1_R = (1,1,1\ldots)$ makes R into a commutative unital ring. Inside R we consider the ideal $\mathfrak{m}$ consisting of sequences that converge to $0 \in \mathbb{Q}$. We claim that $\mathfrak{m}$ is a maximal ideal. To see this, let $\mathfrak{a} \subset R$ be an ideal with

$$\mathfrak{m} \subsetneq \mathfrak{a} \subset R.$$

Then there is a Cauchy sequence $x = (x_1, x_2, x_3, \ldots) \in \mathfrak{a}$ such that the sequence $|x_n|_p$ does not converge to 0, hence $|x_n|_p$ converges to p^{n_x} with $n_x \in \mathbb{Z}$. As $\mathfrak{a}$ contains all sequences that converge to $0 \in \mathbb{Q}$, we have that every sequence whose p-adic norm converges to p^{n_x} is contained in $\mathfrak{a}$. By multiplying the sequence x with p^{n_x-n} for $n \in \mathbb{Z}$ we arrive at a sequence whose p-adic norm converges to p^n. Hence $\mathfrak{a} = R$.

For an element $x = (x_1, x_2, x_3, \ldots) \in R/\mathfrak{m}$ we define

$$|x|_p = \lim_{n\to\infty} |x_n|_p \in \{p^n : n \in \mathbb{Z}\} \cup \{0\},$$

where we note that $|x_n|_p$ converges as $|x_n|_p$ is a Cauchy sequence in $\mathbb{R}$ with values in the set $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$. We can embed $\mathbb{Q}$ into $\mathbb{Q}_p$ by the map

$$\mathbb{Q} \hookrightarrow R/\mathfrak{m}, \qquad q \mapsto (q, q, q, \ldots).$$

With all this we one shows, as in the case of the completion of a normed vector space, that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ and that $R/\mathfrak{m}$ is a complete normed field. So we set

$$\mathbb{Q}_p := R/\mathfrak{m}.$$

Every p-adic number has a so called *p-adic expansion*, as we show in the next theorem.

Theorem 6.5. *Let x be a non-zero p-adic number with $|x|_p = p^m$ for $m \in \mathbb{Z}$. Then we can write x uniquely as a converging sum*

$$x = \sum_{i=-m}^{\infty} d_i p^i \tag{6.1}$$

for $0 \leq d_i < p$ and $d_{-m} \neq 0$.

We start with the following lemma.

Lemma 6.6. *Let x be a rational number with $|x|_p \leq 1$. Then for any $i \in \mathbb{N}$ there is a unique $\alpha_i \in \{0, 1, \ldots, p^i - 1\}$ such that*

$$|x - \alpha_i|_p \leq p^{-i}.$$

Proof. Write $x = \frac{ap^m}{b}$ for $m \in \mathbb{Z}_{\geq 0}$ and $a, b \in \mathbb{Z}$ with p not dividing a or b. We want to find an $\alpha_i \in \{0, 1, \ldots, p^i - 1\}$ such that

$$b\alpha_i - ap^n \equiv 0 \mod p^i.$$

As b does not divide p, there is a multiplicative inverse b^{-1} of b in $\mathbb{Z}/p^i\mathbb{Z}$. Thus α_i is the unique element in $\{0, 1, \ldots, p^i - 1\}$ such that

$$\alpha_i + p^i\mathbb{Z} = ap^n b^{-1} + p^i\mathbb{Z}$$

in $\mathbb{Z}/p^i\mathbb{Z}$. □

Theorem 6.5 can easily be proved by using the next proposition.

Proposition 6.7. *Let x be a p-adic number with $|x|_p \leq 1$. Then there is a unique Cauchy sequence $a = (a_1, a_2, a_3, \ldots)$ that represents x such that $0 \leq a_i < p^i$ and $a^i \equiv a^{i+1} \mod p^i$.*

Proof. Let $x = (x_1, x_2, x_3, \ldots)$ be a representative of x as a Cauchy sequence. As $\lim_{i\to\infty} |x_i|_p = |x|_p$, we have that $|x_i|_p \leq 1$ for almost all i. Thus we can assume without loss of generality that $|x_i|_p \leq 1$ for all $i \in \mathbb{N}$.

Since $(x_1, x_2, x_3, \ldots)$ is a Cauchy sequence for all $j \in \mathbb{N}$ there is some $N(j)$ with

$$|x_k - x_l|_p \leq p^{-j}$$

for $k, l \geq N(j)$. By Lemma 6.6 there is a unique $0 \leq a_j < p^j$ with

$$|x_{N(j)} - a_j|_p \leq p^{-j}.$$

We note that $a := (a_1, a_2, a_3, \ldots)$ is a Cauchy sequence as for any $\varepsilon > 0$ we have

$$|a_k - a_l|_p = |a_k - x_{N(k)} + x_{N(k)} - x_{N(l)} + x_{N(l)} - x_l| \leq \varepsilon$$

for k and l large enough. Furthermore a represents the same element as x since

$$|a_j - x_j|_p \leq |a_j - x_{N(j)} + x_{N(j)} - x_j| \leq \varepsilon$$

for j large enough.

Next, we prove that $a_j \equiv a_{j+1} \mod p^j$. To see it suffices to note

$$\begin{aligned} |a_j - a_{j+i}|_p &\leq |a_i - x_{N(j)} + x_{N(j)} - x_{N(j+1)} + x_{N(j+1)} - a_{j+1}|_p \\ &\leq \max\{|a_i - x_{N(j)}|_p, |x_{N(j)} - x_{N(j+1)}|_p, |x_{N(j+1)} - a_{j+1}|_p\} \\ &\leq p^{-j}. \end{aligned}$$

Finally we show that x can be uniquely represented in such a way. To see this let $a = (a_1, a_2, a_3, \ldots)$ and $a' = (a'_1, a'_2, a'_3, \ldots)$ be a two such representation with $a_{i_0} \neq a'_{i_0}$ for some i_0. Then we have for all $i \geq i_0$ that

$$a_i \equiv a_{i_0} \neq a'_{i_0} \equiv a'_i \mod p^i$$

and hence

$$|a_i - a'_i|_p \geq p^{-i_0}$$

for all $i \geq i_0$. This is a contradiction as this shows that a and a' do not represent the same element. □

Proof. (of Theorem 6.5) We first note that for any choice of $0 \leq d_i < p$ the sequence

$$x_l = \sum_{i=-m}^{l} d_i p^i$$

forms a Cauchy sequence as

$$|x_l - x_k|_p = \left| \sum_{i=-m}^{l} d_i p^i - \sum_{i=-m}^{k} d_i p^i \right|_p = \left| \sum_{i=\min\{l,k\}}^{\max\{l,k\}} d_i p^i \right|_p \leq p^{-\min\{l,k\}}.$$

By multiplying by x with p^{-m} we can assume without loss of generality that $|x|_p = 1$. The last proposition gives a unique representation $x = (a_1, a_2, a_3, \ldots)$ with $0 \leq a_i < p^i$ and $a_i = a_{i+1} \mod p^i$. Hence there are unique $0 \leq d_i < p$ with

$$a_i = d_0 + d_1 p + \ldots + d_{i-1} p^{i-1}$$

for $i \geq 0$. So we have a unique decomposition

$$x = \sum_{i=0}^{\infty} d_i p^i.$$

□

Definition 6.8. A p-adic number $a \in \mathbb{Q}_p$ is said to be a p-adic integer if and only if its p-adic expansion contains only nonnegative powers of p. The set of p-adic intergers is usually denoted by $\mathbb{Z}_p$.

Corollary 6.9. *We have that*

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p \,:\, a = \sum_{i=0}^{\infty} d_i p^i \text{ with } 0 \leq d_i < p \right\} = \{a \in \mathbb{Q}_p \,:\, |a|_p \leq 1\}$$

Proof. This follows immediately from Theorem 6.5. □

For two p-adic numbers

$$a = \sum_{i=-m}^{\infty} a_i p^i \quad \text{and} \quad b = \sum_{i=-m}^{\infty} b_i p^i$$

we have that

$$a + b = \sum_{i=-m}^{\infty} (a_i + b_i) p^i,$$

where we note that with this definition $a + b$ might not be in the standard form (6.1) but can easily be modified to attain the standard form. We also have

$$a \cdot b = \sum_{i=-2m}^{\infty} c_i p^i$$

where

$$c_{-2m} = a_{-m} b_{-m}, \qquad c_{-2m+1} = a_{-m} b_{-m+1} + a_{-m+1} b_{-m}$$

and so on.

6.2 Algebraic Properties of the p-adic Integers

In this subsection, we state and prove some algebraic properties about the p-adic integers.

Proposition 6.10. *The p-adic integers $\mathbb{Z}_p$ form an integral domain and the the units of $\mathbb{Z}_p$ are*

$$\mathbb{Z}_p^{\times} = \left\{ \sum_{i=0}^{\infty} a_i p^i \,:\, a_0 \neq 0 \right\} = \{x \in \mathbb{Q}_p \,:\, |x|_p = 1\}.$$

Proof. The second equality is clear. To prove the first let $a = \sum_{i=0}^{\infty} a_i p^i$ be a unit in $\mathbb{Z}_p$. If a_0, was zero. Then for any p-adic number $b = \sum_{i=0}^{\infty} b_i p^i$ we had

$$a \cdot b = 0 + b_0 a_1 p + \ldots \neq 1.$$

Conversely if $a = \sum_{i=0}^{\infty} a_i p^i$ satisfies $a_0 \neq 0$. We want to find a p-adic number $b = \sum_{i=0}^{\infty} b_i p^i$ with $0 \leq b_i < p$ such that $a \cdot b = 1$. We can find b_0 such that

$$a_0 b_0 = 1 + n \cdot p$$

for some $n \geq 1$. Next we need to choose b_1 such that

$$n \cdot p + a_0 b_1 + b_0 a_1 \equiv 0 \mod p.$$

Such a b_1 exists as a_0 is invertible in $\mathbb{Z}/p\mathbb{Z}$. Continuing this process, always using the fact that a_0 is invertible in $\mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 1$, we arrive at a p-adic number $b = \sum_{i=0}^{\infty} b_i p^i$ with $a \cdot b = 1$. □

The next proposition shows that $\mathbb{Z}_p$ is a principle ideal domain and the only prime ideal in $\mathbb{Z}_p$ is $p\mathbb{Z}_p$.

Proposition 6.11. *Let $\mathfrak{a}$ be a non-zero ideal in $\mathbb{Z}_p$. Then there is a an integer $n \geq 0$ such that*

$$\mathfrak{a} = p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \,:\, |x|_p \leq \tfrac{1}{p^n}\}.$$

Furthermore

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}_p/p^n\mathbb{Z}.$$

Proof. Let $\mathfrak{a}$ be a non-zero ideal in $\mathbb{Z}_p$. Then choose a non-zero element $x \in \mathfrak{a}$ of minimal norm. By Proposition 6.10 we can write $x = p^n u$ for $n \geq 0$ and $u \in \mathbb{Z}_p^\times$. Hence $\mathfrak{a} = p^n\mathbb{Z}_p$.

Finally consider the homomorphism

$$\rho : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p, \qquad x \mapsto x + p^n\mathbb{Z}_p.$$

Note that ρ is surjective as we can find for any $x \in \mathbb{Z}_p$ some number $\alpha \in \mathbb{Z}$ such that

$$|x - \alpha|_p \leq \frac{1}{p^n}$$

and hence $x - \alpha \in p^n\mathbb{Z}_p$. Furthermore the kernel of ρ is $p^n\mathbb{Z}$ implying the last statement. □

Finally, we give an equivalent characterization of the p-adic integers. We consider the projective limit

$$\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} := \left\{ (a_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \,:\, a_{n+1} = a_n \mod p^n \text{ for all } n \geq 1 \right\}.$$

By Proposition 6.7, for any p-adic integer $a \in \mathbb{Z}_p$, there is a unique representation of a as a Cauchy sequence $a = (a_1, a_2, a_3 \ldots)$ with $0 \leq a_n < p^n$ and $a_{n+1} \equiv a_n \mod p^n$. By viewing a_n as an element in $\mathbb{Z}/p^i\mathbb{Z}$ we get a ring homomorphism

$$\mathbb{Z}_p \longrightarrow \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

This ring homomorphism is injective as the above representation of a as a Cauchy sequence is unique and surjective as any such sequence $(a_1, a_2, a_3, \ldots)$ is Cauchy and hence defines an element in $\mathbb{Z}_p$. This all is summarized in the next proposition.

Theorem 6.12. *There exists a ring isomorphism*

$$\mathbb{Z}_p \longrightarrow \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

6.3 Topological Properties

We consider $\mathbb{Q}_p$ together with the topology induced by the norm $|\cdot|_p$. The aim of this subsection is to discuss a few interesting topological properties of the p-adic numbers and p-adic integers. For instance, the p-adic numbers are totally disconnected and hence differ dramatically form the real numbers.

We first discuss topological properties of $\mathbb{Q}_p$. For $a \in \mathbb{Q}_p$ and $r > 0$ we define the ball of radius r around a as

$$B(a,r) := \{x \in \mathbb{Q}_p \,:\, |x-a|_p < r\}$$

and the sphere

$$S(a,r) := \{x \in \mathbb{Q}_p \,:\, |x-a|_p = r\}.$$

Proposition 6.13. *For any $a \in \mathbb{Q}_p$ and $r > 0$ the sphere $S(a,r)$ and the ball $B(a,r)$ are open and closed.*

Proof. By definition of the topology on $\mathbb{Q}_p$, the ball $B(a,r)$ is open and

$$S(a,r) = \{x \in \mathbb{Q}_p \,:\, |x-a|_p \leq r\} \cap B(a,r)^c$$

is an intersection of closed sets as $|\cdot|_p$ is continuous.

To prove that $S(a,r)$ is open, let $x \in S(a,r)$. We show for any $\varepsilon < r$ that $B(x,\varepsilon) \subset S(a,r)$. To see this let $y \in B(x,\varepsilon)$ and hence

$$|y-x|_p < \varepsilon < r.$$

As the p-adic norm is non-Archimidean

$$|y-a|_p = |y-x+x-a|_p \leq \max\{|y-x|_p, |x-a|_p\} = r$$

so $|y-a| \leq r$ and

$$r = |x-a|_p = |x-y+y-a|_p \leq \max\{|x-y|_p, |y-a|_p\} = |y-a|_p$$

as $|x-y|_p < r$. So $|y-a| = r$ and $B(x,\varepsilon) \subset S(a,r)$.

As $S(a,r)$ is open, it follows that

$$B(a,r)^c = S(a,r) \cup \{x \in \mathbb{Q}_p \,:\, |x-a| > r\}$$

is open and so $B(a,r)$ is closed. □

Proposition 6.14. *Let $a \in \mathbb{Q}_p$ and $r > 0$. If $b \in B(a,r)$ then $B(b,r) = B(a,r)$. Furthermore if the intersection of any two balls is non-empty, then one ball is contained in the other.*

Proof. Let $x \in B(b,r)$. Then

$$|x-a| = |x-b+b-a| < r.$$

Conversely if $x \in B(a,r)$ we have $|x-b| = |x-a+a-b| < r$.

Next let $B(a,r)$ and $B(b,s)$ be two balls for $a, b \in \mathbb{Q}_p$ and $r, s > 0$ with non-empty intersection. We assume without loss of generality that $r \leq s$. We have some element $x \in B(a,r) \cap B(b,s)$. Then by using the first part of the proposition

$$B(a,r) = B(x,r) \subset B(x,s) = B(b,s).$$

□

Theorem 6.15. *The p-adic numbers are a totally disconnected topological space.*

Proof. Let x and y be distinct point, so $|x-y|_p = p^m$ for $m \in \mathbb{Z}$. Then $x \in B(x, p^{m-1})$ and $y \in B(y, p^{m-1})$ are disjoint open and closed sets containing x and y. Hence x and y do not lie in the same connected component. □

We now move over to study properties of $\mathbb{Z}_p$.

Proposition 6.16. *The p-adic integers are a compact and hence complete subset of $\mathbb{Q}_p$.*

Proof. Consider a sequence x^n of p-adic integers given in the standard form

$$x^n = \sum_{i=0}^{\infty} x_i^n p^n.$$

Then we can find a subsequence of x^n such that x_i^n converges for all i and hence is constant for large enough n. We assume without loss of generality that $x_i^n = x_i$ for n large enough and write $x = \sum_{i=0}^{\infty} x_i p^i$. Fix i_0 a number and choose N large enough such that $x_i^n = x_i$ for all $i \leq i_0$ and $N \geq n$. Then we have for all $m \geq N$ that

$$|x^m - x|_p = \left| \sum_{i=i_0+1}^{\infty} (x_i^m - x_i) p^i \right|_p \leq p^{-(i_0+1)}$$

and hence x^n converges to x. Thus $\mathbb{Z}_p$ is compact. □

In the discussion below, we specialize for simplicity to the case $p = 2$. However, one can easily vary the below result for any prime number p.

Consider the Cantor set

$$C = \left\{ \sum_{i=0}^{\infty} \frac{a_i}{3^{i+1}} \text{ with } a_i \in \{0, 2\} \right\} \subset [0, 1]$$

with the induced topology from $[0, 1]$. Note that the Cantor set is Hausdorff.

Theorem 6.17. *The dyadic integers $\mathbb{Z}_2$ are homeomorphic to the Cantor set.*

Proof. Consider the map

$$\psi : \mathbb{Z}_2 \longrightarrow C, \qquad a = \sum_{i=0}^{\infty} a_i 2^i \longmapsto \sum_{i=0}^{\infty} \frac{2a_i}{3^{i+1}},$$

where $a = \sum_{i=0}^{\infty} a_i 2^i$ is written in the standard form with $a_i \in \{0, 1\}$. As any dyadic number can be uniquely written in such a way, it follows that ψ is bijective. We claim that ψ is a homeomorphism. As $\mathbb{Z}_2$ is compact and the Cantor set is Hausdorff, it suffices to prove that ψ is continuous. Let $\varepsilon > 0$ and choose $n \geq 1$ such that $\frac{1}{3^n} < \varepsilon$. If for $a^1, a^2 \in \mathbb{Z}_2$ with the dyadic expansion

$$a^1 = \sum_{i=0}^{\infty} a_i^1 2^i \quad \text{and} \quad a^2 = \sum_{i=0}^{\infty} a_i^2 2^i$$

it holds that

$$|a_1 - a_2| \leq \frac{1}{3^n}$$

we then have $a_i^1 = a_i^2$ for all $i \leq n$. So

$$|\psi(a_1) - \psi(a_2)| < \varepsilon.$$

□

Corollary 6.18. *The Cantor set is totally disconnected.*

Proof. This statement is implied by the last theorem and Proposition 6.15. □

7 Valuations and Local Fields

7.1 Valuations

In the last section we studied the field $\mathbb{Q}$ with the p-adic valuation $|\cdot|_p$. In this section we study valuations more generally.

Theorem 7.1. *A valuation $|\cdot|$ on a field K is non-archimedean if and only if $|n|$ is bounded for $n \in \mathbb{N}$.*

Proof. If the valuation is non-archimedean, then

$$|n| = |1 + \ldots + 1| \leq |1|$$

and hence $|n|$ is bounded by $|1|$ for any $n \in \mathbb{N}$. Conversely assume that $|n| \leq N$ for all $n \in \mathbb{N}$. Then let $x, y \in K$ and assume without loss of generality that $|x| \geq |y|$. Then we have that $|x|^\nu |y|^{n-\nu} \leq |x|^n$ for $\nu \geq 0$. So we have by the triangle inequality

$$|x+y|^n \leq \sum_{\nu=1}^{n} \left| \binom{n}{\nu} \right| |x|^\nu |y|^{n-\nu} \leq N(n+1)|x|^n.$$

So we have that

$$|x+y| \leq N^{1/n}(1+n)^{1/n}|x| = N^{1/n}(1+n)^{1/n} \max\{|x|, |y|\}$$

and so $|x+y| \leq \max\{|x|, |y|\}$ as $N^{1/n}(1+n)^{1/n}$ converges to 1 as $n \to \infty$. □

Definition 7.2. We call two valuations on K equivalent if they induce the same topology on K.

Theorem 7.3. *Two valuations $|\cdot|_1$ and $|\cdot|_2$ on K are equivalent if and only if*

$$|x|_1 = |x|_2^s$$

for all $x \in K$ and some $s > 0$.

Theorem 7.4. *Every valuation on $\mathbb{Q}$ is equivalent to one of the valuations $|\cdot|_p$ for p a prime number or to the euclidean norm $|\cdot|$ on $\mathbb{Q}$.*

7.2 Global and Local Fields

Definition 7.5. A *global field* is a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_p(t)$ for p a prime number.

Definition 7.6. A local field is either $\mathbb{R}, \mathbb{C}$ or a finite extension of either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.

Part II
The Theory of Linear Algebraic Groups

8 Essence of Algebraic Geometry

8.1 Zariski Topology

Let K be an algebraically closed field. We consider the space $K^n = K \times \ldots \times K$ which is called *affine n-space* and is also also sometimes denoted $\mathbb{A}^n$. Furthermore we consider the noetherian polynomial ring in n-variables $K[X_1, \ldots, X_n]$ which we will mostly abbreviate by $K[X]$.

For any ideal $\mathfrak{a} \subset K[X]$ we define the *vanishing locus of* $\mathfrak{a}$ as

$$V(\mathfrak{a}) = \{x \in K^n \,:\, f(x) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

Proposition 8.1. *We have the following properties:*

1. $V(K[X]) = \emptyset$ *and* $V((0)) = K^n$.
2. *If two ideals* $\mathfrak{a}, \mathfrak{b} \subset K[X]$ *satisfy* $\mathfrak{a} \subset \mathfrak{b}$ *then we have* $V(\mathfrak{a}) \supset V(\mathfrak{b})$.
3. *For any ideals* $\mathfrak{a}, \mathfrak{b}$ *of* $K[X]$ *it holds that*
$$V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b}).$$
4. *For a collection of ideals* $\mathfrak{a}_i \subset K[X]$ *with* $i \in I$ *we have that*
$$V\left(\sum_{i \in I} \mathfrak{a}_i\right) = \bigcap_{i \in I} V(\mathfrak{a}_i).$$

Proof. 1. and 2. are clear. For 3. note that $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}$ and $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{b}$ and so $V(\mathfrak{a} \cap \mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b})$. Conversely assume for a contradiction that $x \in V(\mathfrak{a} \cap \mathfrak{b})$ but $x \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$. Then we have there is some $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$ such that $f(x) \neq 0$ and $g(x) \neq 0$. So we have that $f(x)g(x) \neq 0$ as K is a field. Since $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ we hence arrive at the contradiction $x \notin V(\mathfrak{a} \cap \mathfrak{b})$.

For 4. note that $\sum_{i \in I} \mathfrak{a}_i \supset \mathfrak{a}_i$ for all $i \in I$ and hence $V\left(\sum_{i \in I} \mathfrak{a}_i\right) \subset \bigcap_{i \in I} V(\mathfrak{a}_i)$. Conversely if $x \in \bigcap_{i \in I} V(\mathfrak{a}_i)$, then for any finite number of elements $f_j \in \mathfrak{a}_{i_j}$ with $1 \leq j \leq n$ we have

$$f_1(x) + \ldots + f_n(x) = 0$$

and so $x \in V\left(\sum_{i \in I} \mathfrak{a}_i\right)$. □

By this proposition we can define a topology on K^n for which the closed sets are precisely the sets $V(\mathfrak{a})$ for $\mathfrak{a}$ any ideal in $K[X]$. This topology is called the *Zariski topology.*

Example 8.2. We show in the following that the Zariski closed sets in $K = K^1$ are precisely the finite sets.

First note that any finite set $\{x_1, \ldots, x_n\}$ is Zariski closed by considering $V(\mathfrak{a})$ for $\mathfrak{a}$ the ideal generated by the polynomial $(X - x_1) \cdot \ldots \cdot (X - x_n)$. Conversely if $\mathfrak{a}$ is an ideal then, as $K[X]$ is noetherian, there is are finitely many generators $f_1, \ldots, f_n$ such that

$$\mathfrak{a} = (f_1, \ldots, f_n) = \sum_{i=1}^{n} (f_i).$$

So

$$V(\mathfrak{a}) = \bigcap_{i=1}^{n} V((f_i))$$

is finite as the set $V(f_i)$ consists precisely of the finitely many zeros of f_i.

Example 8.3. Consider in this example $K = \mathbb{C}$ and the Zariski closed subsets of $\mathbb{C}^n$. As in the last example we note that for any polynomial $f \in K[X]$ we have

$$V((f)) = \{x \in \mathbb{C}^n \,:\, f(x) = 0\}.$$

As any polynomial is continuous, we note that the set $V((f))$ is closed. Thus as any ideal $\mathfrak{a} \subset K[X]$ is finitely generated we can write

$$V(\mathfrak{a}) = \bigcap_{i=1}^{n} V(f_i)$$

for $\mathfrak{a} = (f_1, \ldots, f_n)$. So any Zariski closed set is closed with respect to the euclidean topology.

We next note that any closed euclidean r-ball $B_r(x) = \{y \in \mathbb{C}^n \,:\, |x-y| \leq r\}$ for any $x \in \mathbb{C}^n$ is not Zariski closed. To see this assume that there was some ideal $\mathfrak{a} \subset K[X]$ such that $V(\mathfrak{a}) = B_r(x)$. So we have that for any $f \in \mathfrak{a}$ that $f(x) = 0$ for all $B_r(x)$. Thus $f \equiv 0$. So $\mathfrak{a} = (0)$ but this is a contradiction as $V((0)) = \mathbb{C}^n \neq B_r(x)$. This also shows that any euclidean ball is Zariski dense.

Next we study the converse operation to V, namely for any subset $Z \subset K^n$ we define the *ideal associated to* X as

$$I(Z) = \{f \in K[X] \,:\, f(z) = 0 \text{ for all } z \in Z\}.$$

Recall that the radical of any ideal $\mathfrak{a}$ is defined as

$$\operatorname{rad}(\mathfrak{a}) = \{f \in K[X] \,:\, f^n \in \mathfrak{a} \text{ for some } n\}.$$

Furthermore an ideal is called *radical* if it is its own radical.

Theorem 8.4. *(Hilbert's Nullstellensatz) Let $\mathfrak{a}$ be any ideal in $K[X]$, then*

$$I(V(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a}).$$

Proof. For a proof see [Hum75] Page 5. □

Corollary 8.5. *The Zariski closure of any set $Z \subset K^n$ is $V(I(Z))$. Moreover, the map I is a bijection between Zariski closed sets in K^n and radical ideals of $K[X]$ with inverse V.*

Proof. As $Z \subset V(I(X))$, it remains to consider a Zariski closed set $C = V(\mathfrak{a})$ that contains Z. Then $\mathfrak{a} \subset I(Z)$ and so $C = V(\mathfrak{a}) \supset V(I(Z))$. So $V(I(Z))$ is indeed the Zariski closure of Z.

Next let $C = V(\mathfrak{a})$ be a Zariski closed subset. Then we have by the Nullstellensatz

$$V(I(C)) = V(I(V(\mathfrak{a}))) = V(\operatorname{rad}(\mathfrak{a})) = V(\mathfrak{a}).$$

Furthermore if $\mathfrak{a} = \operatorname{rad}(\mathfrak{a})$ is a radical ideal, then again by the Nullstellensatz

$$I(V(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a}) = \mathfrak{a}.$$

So I and V are inverse bijections between the set of Zariski closed sets in K^n and radical ideals of $K[X]$. □

We next show discuss some properties of the Zariski topology.

Proposition 8.6. *Let Z be a Zariski closed subset of K^n considered with the induced Zariski topology.*

1. *Points in Z are closed.*
2. *Any open cover of Z has a finite subcover.*

Proof. To see 1., note that for any $Z = (z_1, \ldots, z_n) \in X$ we have that the ideal generated by the monomials $X_1 - z_1, \ldots, X_n - z_n$ just consists of the point x. For 2. we assume that

$$\emptyset = \bigcap_{i \in I} V(\mathfrak{a}_i) = V\left(\sum_{i \in I} \mathfrak{a}_i\right).$$

By the Nullstellensatz we have that

$$K[X] = \operatorname{rad}\left(\sum_{i \in I} \mathfrak{a}_i\right)$$

and so $1 = 1^n \in \sum_{i \in I} \mathfrak{a}_i$. Hence there is a finite sum $f_1 + \ldots + f_n = 1$ with $f_j \in \mathfrak{a}_{i_j}$. This shows that $\sum_{j=1}^{n} \mathfrak{a}_{i_j} = K[X]$ and so

$$\emptyset = \bigcap_{j=1}^{n} V(\mathfrak{a}_{i_j}).$$

□

Definition 8.7. A topological space Z is called *noetherian* if any family of closed sets contains a minimal one or equivalently if any family of open sets contains a maximal one.

Furthermore, note that another equivalent condition for a noetherian topological space is the following: Any descending chain of closed subsets $Z_1 \subset Z_2 \subset \ldots$ becomes stationary. In fact, as $K[X]$ is noetherian, we have that K^n with the Zariski topology is noetherian. As any closed subset of a noetherian topological space is again noetherian with respect to the induced topology, we have that any Zariski closed subset Z of K^n is noetherian with respect to the induced Zariski topology.

Definition 8.8. A topological space Z is called *reducible* if it is the union of two proper closed subsets. Otherwise Z is called *irreducible*. A subset $A \subset Z$ is irreducible if it is irreducible with respect to the induced topology.

Proposition 8.9. *Let Z be a noetherian topological space. Then Z has finitely many maximal irreducible subsets. These are closed and cover Z.*

Proof. See Page 3 of [Spr98]. □

Proposition 8.10. *A Zariski closed subset Z of K^n is irreducible if and only if $I(Z)$ is a prime ideal.*

Proof. Assume that Z is irreducible and let $f, g \in K[X]$ with $fg \in I(Z)$. As $K[X]$ is an integral domain

$$Z = (Z \cap V((f))) \cup (Z \cap V((g)))$$

and so by irreducibility $Z \subset V((f))$ or $Z \subset V((g))$ or equivalently $f \in I(Z)$ or $g \in I(Z)$.

For the converse assume that $I(Z)$ is a prime ideal and that $Z = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$. If $Z \neq V(\mathfrak{a})$, then there is $f \in \mathfrak{a}$ such that $f \notin I(Z)$. Since $fg \in I(Z)$ for all $g \in \mathfrak{b}$ it follows that $\mathfrak{b} \subset I(X)$ and so $X = V(\mathfrak{b})$. Thus X is irreducible. □

Definition 8.11. Let A be an algebra over K. Then A is called *affine* if it is of finite type, i.e. there are finitely many elements $f_1, \ldots, f_n \in A$ such that $A = K[f_1, \ldots, f_n]$, and A is reduced, i.e. 0 is the only nilpotent element of A.

For a Zariski closed subset $Z \subset K^n$ we define the *affine algebra of* Z or the *coordinate ring of* Z as

$$K[Z] = K[X]/I(Z).$$

The ring $K[Z]$ is an affine k-algebra as $K[X]$ is noetherian and $I(Z)$ is a radical ideal. Note that $K[Z]$ is an integral domain if and only if Z is irreducible.

We now describe how to associate to each affine K-algebra A a Zariski closed subset of K^n for some n. Namely choose generators $f_1, \ldots, f_n \in A$ and consider the ideal $\mathfrak{a} = (f_1, \ldots, f_n)$. By sending the variable X_i to f_i we get an isomorphism

$$A \cong K[X_1, \ldots, X_n]/\mathfrak{a}.$$

Furthermore $\mathfrak{a}$ is radical as A is reduced. Thus $\mathfrak{a} = I(Z)$ for a unique Zariski closed subset $Z \subset K^n$.

Proposition 8.12. *The map*

$$Z \mapsto \operatorname{Specmax}(K[Z]), \qquad z \mapsto \mathfrak{m}_z = I_Z(\{z\})$$

is bijective.

Proof. Note that the maximal ideals if $K[Z]$ are the maximal ones of $K[Z]$ that contain $I(Z)$. Thus the map is well defined. Note that $I_Z(\{z\}) = \langle (X_1 - z_1), \ldots, (X_n - z_n) \rangle + I(Z)$ and so the map is injective. To see that the map is surjective, note that the maximal ideals of $K[X]$ are precisely of the form $\langle (X_1 - z_1), \ldots, (X_n - z_n) \rangle$ for some element $z = (z_1, \ldots, z_n) \in K^n$. □

Proposition 8.13. *The map*

$$\operatorname{Specmax}(K[Z]) \to \operatorname{Hom}_K(K[Z], K), \qquad \mathfrak{m}_z = I_Z(\{z\}) \mapsto (X_i \mapsto z_i),$$

where $\operatorname{Hom}_K(K[Z], K)$ *is the set of* K*-algebra homomorphisms from* $K[Z]$ *to* K*, is a bijection.*

Proof. This follows with the last proposition and the fact that a K-algebra homomorphism from $K[X_1, \ldots, X_n]$ to K is completely determined by the image of the elements X_i. □

Definition 8.14. Let Z be a Zariski closed subset and $\mathfrak{a}$ be an ideal in $K[Z]$. Then the vanishing locus of $\mathfrak{a}$ relative to Z is defined as

$$V_Z(\mathfrak{a}) = \{z \in Z \,:\, f(z) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

Furthermore, we define for $Y \subset Z$ a subset

$$I_Z(Y) = \{f \in K[Z] \,:\, f(y) = 0 \text{ for all } y \in Y\}.$$

Corollary 8.15. *The Zariski closure of any set $Y \subset Z$ is $V_Z(I_Z(Y))$. Moreover, the map I_Z is a bijection between Zariski closed subsets in Z and radical ideals of $K[Z]$ with inverse V_Z.*

Proof. Analogously to the Nullstellensatz have that $I_X(V_X(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a})$. The rest of the statement follows analogously to Corollary 8.5. □

If $f \in K[Z]$ denote the Zariski open set

$$D_Z(f) = D(f) = \{x \in X \,:\, f(x) \neq 0\}.$$

These sets are called the *principle open sets* and they form a basis of the Zariski topology. Moreover for any

$$f, g \in K[Z]$$

we have

$$D(fg) = D(f) \cap D(g), \quad \text{and} \quad D(f^n) = D(f)$$

for $n \geq 1$.

8.2 Affine Algebraic Varieties

Throughout this section denote by K an algebraically closed field, by $Z \subset K^n$ a Zariski closed subset and by $K[Z]$ its coordinate ring.

Definition 8.16. A K-valued function f defined in a neighborhood U of z is called *regular at z* if there are $g, h \in K[Z]$ and an open neighborhood $V \subset U \cap D(h)$ of z such that

$$f(y) = g(y)h(y)^{-1}$$

for $y \in V$.

A K-valued function f on U is called *regular* if it is regular at all its points. We denote by

$$\mathcal{O}_Z(U) \text{ or } \mathcal{O}(U)$$

the K-algebra of regular functions on U.

We note that $\mathcal{O}_Z$ defines a sheaf on Z, sometimes called the *structure sheaf on Z*. More precisely, if $V \subset U$ are non-empty open subset, then restriction yields a k-algebra homomorphism

$$\mathcal{O}_Z(U) \to \mathcal{O}_Z(V).$$

Furthermore if $U = \bigcup_{\alpha \in A} U_\alpha$ is an open covering and we are given a collection of regular functions $f_\alpha \in \mathcal{O}_Z(U_\alpha)$ that are compatible on the intersections $U_\alpha \cap U_\beta$, then the functions f_α uniquely glue to a function $f \in O_Z(U)$ that satisfies $f|_{U_\alpha} = f_\alpha$. This all makes $(Z, \mathcal{O}_Z)$ into a *ringed space*, meaning a topological space Z together with a sheaf of functions $\mathcal{O}$.

Definition 8.17. An *affine algebraic variety* $(Z, \mathcal{O}_Z)$ is a Zariski closed set Z in K^n with the above describes sheaf of functions $\mathcal{O}_Z$. We usually drop the $\mathcal{O}_Z$ and just refer to an affine algebraic variety Z.

For an affine algebraic variety $(Z, \mathcal{O}_Z)$ we note that any function $f \in K[Z]$ is regular. Thus we have an injective algebra homomorphism

$$\phi : K[Z] \to \mathcal{O}_Z(Z), \qquad f \mapsto f.$$

Theorem 8.18. *The homomorphism ϕ is an algebra isomorphism.*

Proof. See [Spr98] Page 8. □

Let $(Z_1, \mathcal{O}_{Z_1})$ and $(Z_2, \mathcal{O}_{Z_2})$ be two locally ringed spaces. For a continuous map $\phi : Z_1 \to Z_2$ and any open subset $V \subset Z_2$ we can map any element $f \in \mathcal{O}_{Z_2}(V)$ to

$$\phi^* f = f \circ \phi,$$

which is a function defined on $\phi^{-1}V$.

Definition 8.19. Let $(Z_1, \mathcal{O}_{Z_1})$ and $(Z_2, \mathcal{O}_{Z_2})$ be two locally ringed spaces. A *morphism of locally ringed spaces* from $(Z_1, \mathcal{O}_{Z_1})$ to $(Z_2, \mathcal{O}_{Z_2})$ consists of a continuous function $\phi : Z_1 \to Z_2$ such that for all $V \subset Z_2$ we have a well defined algebra homomorphism

$$\phi^* : \mathcal{O}_{Z_2}(V) \to \mathcal{O}_{Z_1}(\phi^{-1}V), \qquad f \mapsto \phi^* f = f \circ \phi.$$

Definition 8.20. Let $(Z_1, \mathcal{O}_{Z_1})$ and $(Z_2, \mathcal{O}_{Z_2})$ be two affine algebraic varieties. A *morphism of affine algebraic varieties* ϕ from $(Z_1, \mathcal{O}_{Z_1})$ to $(Z_2, \mathcal{O}_{Z_2})$ is a morphism of locally ringed spaces $(Z_1, \mathcal{O}_{Z_1})$ to $(Z_2, \mathcal{O}_{Z_2})$.

We will now discuss the above definition more concretely. Consider two affine algebraic varieties $Z_1 = V(\mathfrak{a}) \subset K^n$ and $Z_2 = V(\mathfrak{b}) \subset K^m$ with two radical ideals $\mathfrak{a}$ and $\mathfrak{b}$ and let $\phi : Z_1 \to Z_2$ be a morphism of affine algebraic varieties. Thus we have an algebra homomorphism

$$\phi^* : \mathcal{O}_{Z_2}(Z_2) \to \mathcal{O}_{Z_1}(Z_1).$$

By Theorem 8.18 we get an induced algebra homomorphism

$$\phi^* : K[Z_2] = K[X_1, \ldots, X_m]/\mathfrak{b} \to K[Z_1] = K[X_1, \ldots, X_m]/\mathfrak{a},$$

where again $\phi^* f \mapsto f \circ \phi$. Denote by ψ_i the image of $X_i + \mathfrak{b}$ in $K[Z_1]$. We note that then ϕ is given by

$$\phi : Z_1 \to Z_2, \qquad x \mapsto (\psi_1(x), \ldots, \psi_m(x)).$$

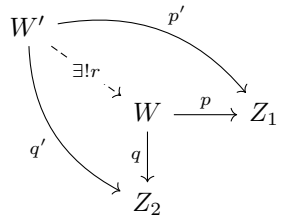
Summarizing all this, we see that a morphism of affine algebraic varieties is given by a well defined map

$$\phi : Z_1 \to Z_2, \qquad x \mapsto (\psi_1(x), \ldots, \psi_m(x))$$

with $\psi_1, \ldots, \psi_m \in K[Z_1]$.

We next want to discuss the *product* of two affine algebraic varieties Z_1 and Z_2 over K. It turns that it is suitable to define the product in a categorical

way. Namely, we characterize the product of X and Y up to isomorphism by the following universal property: The product of Z_1 and Z_2 is a triple (W, p, q) consisting of an affine algebraic variety W over K together with two morphisms $p : W \to Z_1$ and $p : W \to Z_2$ such that for any triple (W', p', q') of an affine variety W' together with morphisms $p' : W' \to Z_1, q' : W' \to Z_2$ there exists a unique morphism $r : W' \to W$ such that $p' = p \circ r$ and $q' = q \circ r$. As a diagram this looks as follows:



Theorem 8.21. *The product of two affine algebraic varieties Z_1 and Z_2 over K exists and is unique up to isomorphism. The coordinate ring is furthermore isomorphic to $K[Z_1] \otimes_K K[Z_2]$, which is again a reduced affine algebra over K.*

Proof. See [Spr98] Page 10. □

We usually denote the product by $Z_1 \times Z_2$ or $Z_1 \times_K Z_2$ to make clear that the varieties are over K.

Proposition 8.22. *Let Z_1 and Z_2 be affine algebraic varieties over K. Then the product variety $Z_1 \times Z_2$ is in bijection with the product of the sets Z_1 and Z_2.*

Proof. Recall that by the universal property of tensor products we have a bijection

$$\mathrm{Hom}_K(K[Z_1] \otimes_K K[Z_2], K) \cong \mathrm{Hom}_K(K[Z_1], K) \times \mathrm{Hom}_K(K[Z_2], K).$$

This implies the statement of the proposition as by 8.12 and 8.13 we have for any affine variety Z a bijection between Z itself and $\mathrm{Hom}_K(K[Z], K)$. □

8.3 Prevarieties and Varieties

Let K be an algebraically closed field. We define in the following the notion of a *variety* which is the analogue of a manifold in the setting of algebraic geometry. We first discuss *prevarieties*.

Definition 8.23. A *prevariety* over K is a quasi-compact ringed space $(X, \mathcal{O}_X)$ such that any point of X has an open neighborhood U with the property that the ringed subspace $(U, \mathcal{O}_X|_U)$ is isomorphic to an affine K-variety. A *morphism of prevarieties* is a morphism of ring spaces.

A *subprevaritey* of a prevaritey is a ringed subspace which is isomorphic to a prevariety.

We again define the product of a prevariety in the catergorical manner as in the affine case.

Proposition 8.24. *The product of two prevarieties exists and is unique up to unique isomorphism.*

Proof. See [Spr98] Page 11. □

Let X be a prevariety and denote by

$$\triangle_X = \{(x, x) : x \in X\} \subset X \times X.$$

We are now ready to define the notion of an algebraic variety.

Definition 8.25. Let X be a prevariety. We call X a *variety* if

$$\triangle_X \subset X \times X$$

is closed. We define a morphism of varieties as a morphism of prevarieties.

Note that a topological space X is Hausdorff if and only if the diagonal $\triangle_X$ is closed in $X \times X$ in the product topology. Thus, a variety is more precisely the analogue of a Hausdorff manifold.

Proposition 8.26. *We have the following properties:*

1. *An affine algebraic variety is a variety.*
2. *The product of two varieties is a variety.*
3. *A subprevaritey of a variety is a variety.*

Proof. The proof is omitted as the statement is not needed later. □

It is thus sensible to call a subprevaritey of a variety a *subvariety*.

8.4 F-structures and affine F-varieties

Throughout this section denote by F a subfield of K, where K is algebraically closed. If Z is a Zariski closed subset of K^n, then we say that F is a *field of definition* of Z. If so we set

$$F[Z] = F[X_1, \ldots, X_n]/(I(Z) \cap F[X_1, \ldots, X_n]).$$

The inclusion

$$F[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$$

induced an isomorphism

$$K \otimes_F F[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$$

which descends to an isomorphism

$$K \otimes_F F[Z] \to K[Z].$$

So $F[X_1, \ldots, X_n]$ is an example of an *F-structure*.

Definition 8.27. Let $A = K[Z]$ be an affine algebra. An *F-structure on Z* is an F-subalgebra A_0 of A which is of finite type over F and which is such that the homomorphism induced by multiplication

$$K \otimes_F A_0 \to K[Z]$$

is an isomorphism. The surjectivity means that A_0 spans V over K and the injectivity translates to the property that elements of A_0 which are linearly independent over F are also linearly independent over K. We then denote $A_0 = F[Z]$.

Definition 8.28. Let $A_0 = F[Z]$ be an F-structure on Z. Then the set

$$Z(F) := \{F\text{-homomorphisms } F[Z] \to F\}$$

is called the set of *F-rational points*.

The next proposition shows that we can view $Z(F)$ as $Z \cap F^n$.

Proposition 8.29. *The map*

$$Z \cap F^n \to Z(F), \qquad z \mapsto (X_i \mapsto z_i)$$

is a bijection.

Proof. This proved as Proposition 8.12 and 8.13. □

We next discuss what is means for a closed subset Y of Z to be closed relative to our F-structure.

Definition 8.30. A F-vector subspace W of $K[Z]$ is called *defined over F* if the K-span of $W \cap F[Z]$ is W.

Definition 8.31. A closed subset Y of Z is *F-closed* if the ideal $I_Z(Y)$ is defined over F. A subset is *F-open* if its complement is F-closed. The F-open sets define a topology as we prove in the next proposition. This is the so called *F-topology*.

Proposition 8.32. *The F-open sets define a topology on Z. A basis for the F-topology is given by the principal open sets $D(f)$ for $f \in F[Z]$.*

Proof. It is clear that Z is F-closed and to see that $\emptyset$ is F-open note that $I_Z(\emptyset) = K[X]$ which is spanned by $F[X]$ over K. Next let $Y_i = V(\mathfrak{a}_i)$ for $i \in I$ be a collection of Zariski closed sets with $\mathfrak{a}_i$ radical ideals in $K[X]$. Then we have by the Nullstellensatz that

$$I_Z\left(\bigcap_{i\in I} Y_i\right) = I_Z\left(\bigcap_{i\in I} V_Z(\mathfrak{a}_i)\right) = I_Z\left(V_Z\left(\sum_{i\in I}\mathfrak{a}_i\right)\right) = \mathrm{Rad}\left(\sum_{i\in I}\mathfrak{a}_i\right).$$

One checks that $\mathrm{Rad}\left(\sum_{i\in I}\mathfrak{a}_i\right)$ is defined over F and so $\bigcap_{i\in I} Y_i$ defines a F-closed set. Furthermore

$$\begin{aligned} I_Z\left(\bigcup_{i=1}^n Y_i\right) = I_Z\left(\bigcup_{i=1}^n V(\mathfrak{a}_i)\right) &= I_Z\left(V_Z\left(\bigcap_{i=1}^n \mathfrak{a}_i\right)\right) \\ = \mathrm{Rad}\left(\bigcap_{i=1}^n \mathfrak{a}_i\right) &= \bigcap_{i=1}^n \mathrm{Rad}(\mathfrak{a}_i) = \bigcap_{i=1}^n \mathfrak{a}_i. \end{aligned}$$

and as $\bigcap_{i=1}^{n} \mathfrak{a}_i$ is clearly defined over F we conclude that $\bigcup_{i=1}^{n} Y_i$ is F-open. So the F-open sets define a topology.

If $f \in F[Z]$ then we have that the coordinate ring of the complement of $D(f)$ is isomorphic to $K[Z]/I_Z((f))$ and so the complement of $D(f)$ is F-closed and this $D(f)$ is F-open. Let Y be an F-closed set. Then we have that $I_Z(Y)$ is defined over F. The rest of the proof is left to the reader. □

Definition 8.33. Let A and B be affine K-algebras with F-structures A_0 and B_0 and let $L : A \to B$ be a K-linear map. We say that L is defined over F if

$$L(A_0) \subset B_0.$$

We next define how to define a F-structure on affine varieties.

Definition 8.34. Let $(Z, \mathcal{O}_Z)$ be an affine variety. An F-structure on the affine variety Z is given by the following data:

1. An F-structure on Z.
2. For each F-open subset U of Z we are given an F-subalgebra $\mathcal{O}_X(U)(F)$ of $\mathcal{O}_Z(U)$ such that the homomorphism induced by multiplication

$$K \otimes_F \mathcal{O}_Z(U)(F) \to \mathcal{O}_X(U)$$

is an isomorphism and these isomorphisms are compatible with the sheaf structure on $\mathcal{O}_Z$.

An affine variety over K with an F-structure will be called an *affine F-variety*

We note that one can also proof in this setting that

$$F[X] \cong \mathcal{O}_Z(Z)(F).$$

For more details see [Spr98] Page 9.

Definition 8.35. Let $(Z, \mathcal{O}_Z)$ and $(W, \mathcal{O}_W)$ be affine varieties. A morphism of affine varieties $a : Z \to W$ is said to be defined over F is a is continuous with respect to the F-topologies and if $U \subset Z$ and $V \subset X$ are F-open such that $a(V) \subset U$ then the induced map

$$\mathcal{O}_Y(U) \to \mathcal{O}_X(U)$$

is defined over F.

Theorem 8.36. *There is an contravariant equivalence of categories between affine varieties over K with F-structures and homomorphisms of K-algebras with k-structures.*

Proof. See [Bor69] Chapter AG and especially subsection 11. □

8.5 Projective Variety

8.6 Complete Varieties

8.7 Smooth Points

Let K be an algebraically closed field and let Z be an irreducible affine variety of dimension k over K.

Definition 8.37. For a point $x \in Z$ we define the *tangent space* at x as

$$T_x Z = \left\{ (u_1, \ldots, u_d) \in K^d \, : \, \sum_{j=1}^{d} u_j \partial_{x_j} f(x) = 0 \text{ for all } f \in I(Z) \right\}.$$

We say that the point $x \in Z$ is smooth if the tangent space is k-dimensional and we furthermore call Z smooth if all of its points are smooth.

We next state some properties about smooth points without proof.

Proposition 8.38. *If K is algebraically closed, then the set of smooth points of Z is nonempty and Zariski open.*

Proof. See [EW] section 3.4. □

Proposition 8.39. *Let $Z \subset \mathbb{C}^d$ be a k-dimensional connected variety defined over $\mathbb{R}$. Let $x \in Z(\mathbb{R})$ be a smooth point. Then there exists an analytic function defined on an open subset in $\mathbb{R}^k$ which is a homeomorphism to a neighborhood of $x \in Z(\mathbb{R})$. The same holds over $\mathbb{C}$ or over $\mathbb{Q}_p$.*

Proof. See [EW] section 3.4. □

8.8 Dimension

Recall that the following terminology.

Definition 8.40. Let (L, K) be a field extension. A *transcendence basis* of L over K is a subset $A \subset L$ such that A is a maximal algebraically independent subset. The *transcendence basis* of L over K is the cardinality of any transcendence basis.

We next define the dimension of an affine variety.

Definition 8.41. Let Z be an irreducible affine variety with coordinate ring $K[Z]$. Note that $K[Z]$ is an integral domain and thus has a quotient field $K(Z)$. The *dimension* of Z, denoted $\dim Z$, is the transcendence degree of $K(Z)$ over K.

If Z is a reducible affine variety with $Z = \bigcup_{i=1}^{m} Z_i$ its irreducible components, we then define the *dimension* of Z as

$$\dim Z = \max_i \dim Z_i.$$

Proposition 8.42. *Let Z be an irreducible affine variety and let Y be a proper irreducible closed subvariety. Then*

$$\dim Y < \dim X.$$

Proof. Let $A = K[Z] = K[z_1, \ldots, z_n]$ and note $K[Y] = A/P$, where P is a non-zero prime ideal of $K[Z]$. Let y_i be the image of z_i in $K[Y]$. Write $d = \dim X$ and $e = \dim Y$. We may assume that $y_1, \ldots, y_e$ are algebraically independent and so also $x_1, \ldots, x_e$ are algebraically independent. So $e \leq d$.

Assume for a contradiction that $e = d$. Let then f be a non-zero element of P. Then as $d = e$ we have a polynomial $H \in K[T_0, \ldots, T_e]$ such that

$$H(f, z_1, \ldots, z_e) = 0.$$

We thus have

$$H(0, y_1, \ldots, y_e) = 0.$$

This is a contradiction. Thus $d < e$. □

Proposition 8.43. *Let X and Y be irreducible affine varieties. Then*

$$\dim X \times Y = \dim X + \dim Y.$$

Proof. This follows from the observation that is $x_1, \ldots, x_d$ and $y_1, \ldots, y_e$ are maximal sets of algebraically independent elements in $K[X]$ respectively $K[X]$ then

$$\{x_1 \otimes 1, \ldots, x_d \otimes 1, 1 \otimes y_1, \ldots, 1 \otimes y_e\}$$

is such a set in $K[X] \otimes K[Y] = K[X \times Y]$. □

Proposition 8.44. *Let $f \in K[T_1, \ldots, T_n]$ be an irreducible polynomial. Then the affine variety*

$$Z = V((f))$$

is an $(n-1)$-dimensional irreducible subvariety of K^n.

Proof. The coordinate ring of Z is $K[T_1, \ldots, T_n]/(f)$. □

9 Linear Algebraic Groups

9.1 Definitions and Examples

Definition 9.1. A algebraic variety G which is also a group is called an *algebraic group* if the maps

$$p : G \times G \to G, \qquad (x, y) \mapsto xy,$$

where we view the set of points in $G \times G$ by 8.22 as a product set, and $i : G \to G, \qquad g \mapsto g^{-1}$ are morphisms of algebraic varieties.

We say that G is a *affine* or *linear algebraic group* if the underlying variety of G is affine.

We next discuss three important examples, where we denote by K always an algebraically closed field.

Example 9.2. Consider $G = K$ with addition as group operation. Then we have the induced homomorphisms

$$m^* : K[G] = K[X] \to K[G] \otimes_K K[G] \cong K[X, Y], \qquad X \mapsto X + Y$$

and

$$i^* : K[G] = K[X] \to K[G] = K[X], \qquad X \mapsto -X$$

are indeed algebra homomorphisms and so G is indeed a linear algebraic group.

Definition 9.3. Let G and G' be algebraic groups. A homomorphism of algebraic groups $\phi : G \to G'$ is a group homomorphism that is also a morphism of varieties.

9.2 Basic Properties

In this subsection we list some basic properties of algebraic groups. Throughout this section we denote by G an algebraic group over K an algebraically closed field.

Proposition 9.4. *Let $g \in G$. Then the maps*

$$L_g : G \to G, \qquad x \mapsto gx$$

and

$$R_g : G \to G, \qquad x \mapsto xg$$

are isomorphisms of varieties.

Proof. By definition L_g and R_g are morphisms of varieties with inverse $L_{g^{-1}}$ and $R_{g^{-1}}$ and hence they are isomorphisms. □

Proposition 9.5. *There is a unique irreducible component G^0 of G that contains the identity element. G^0 is a closed connected normal subgroup of finite index. Furthermore G^0 contains any closed subgroup of G of finite index.*

Proof. Let X and Y be irreducible components of G containing e. Then as multiplication is in particular continuous we conclude that XY and its closure $\overline{XY}$ are irreducible. Since X and Y are contained in $\overline{XY}$ we conclude $X = Y = \overline{XY}$. Since i is a homeomorphism, we see that X^{-1} is an irreducible component of G containing e and so must be equal to X. So X is a closed subgroup. As conjugation defines a homeomorphism we have that $xXx^{-1} = X$, so that X is a normal subgroup. The cosets xX must be the components of G and as a noetherian topological space has only finitely many maximal irreducible subspaces the number of cosets and hence the index of X must be finite. As an irreducible subspace is also connected, we conclude that X is connected.

Finally let H be a closed subgroup of G of finite index. Then H^0 is a closed subgroup of finite index of G^0. As the index of H^0 is finite, we can find a finite sets S of elements in G^0 such that

$$G^0 = \bigsqcup_{s \in S} sH^0.$$

By the last proposition we have that left multiplication is a homeomorphism. Thus each of the sets sH^0 is closed and since we take a finite union, we conclude that the complement of H^0 is closed and hence H^0 is open. Since by the first step we have that G^0 is connected we conclude that $H^0 = G^0$. □

Corollary 9.6. *An algebraic group is connected whenever it is irreducible.*

Proof. If G is irreducible, then it coincides with its unique irreducible component that contains $e \in G$. Thus G is connected by the last proposition. Conversely, if G is connected, then it has only one irreducible component as any irreducible component is connected. □

Lemma 9.7. *Let U and V be dense open subsets of G. Then $UV = G$.*

Proof. Let $x \in G$. Then xV^{-1} and U are both open dense subsets. In the irreducible component of the identity we have that xV^{-1} and U are non-empty open subsets and hence have a nonempty intersection. So $x \in UV$. □

Lemma 9.8. *The closure of any subgroup is again a subgroup.*

Proof. Let H be a subgroup of G. Let $x \in H$. Then $H = xH \subset x\overline{H}$. Since $x\overline{H}$ is closed we have $\overline{H} \subset x\overline{H}$ and $x^{-1}\overline{H} \subset \overline{H}$. So $H\overline{H} \subset \overline{H}$. This argument can be extended for any $x \in \overline{H}$. Lastly since $(\overline{H})^{-1} = \overline{H^{-1}} = \overline{H}$ we have proved that $\overline{H}$ is a subgroup. □

Proposition 9.9. *Let $\phi : G \to G'$ be homomorphism of algebraic groups. Then* $\ker(\phi)$ *is a closed normal subgroup of G and $\phi(G)$ is a closed subgroup of G'.*

Proof. As $\ker(\phi) = \phi^{-1}(e)$ the first statement follows. It is clear that $\phi(G)$ is a subgroups and to see that it is closed we note that

$$\overline{\phi(G)} = \phi(\overline{G}) = \phi(G).$$

□

9.3 Group Actions and Representations

Let G be a algebraic group over K an algebraically closed field. We introduce several important notions and then use them to prove that any linear algebraic group is isomorphic to a closed subgroup of GL_n.

Definition 9.10. We say that G *acts as an algebraic group* on a variety X if there is a morphism of varieties

$$a : G \times X \to X, \qquad (g, x) \mapsto a(g, x) = g.x$$

such that for any $g, h \in G$ and $x \in X$ we have

$$g.(h.x) = (gh).x \quad \text{and} \quad e.x = x.$$

The space X is called a *homogeneous space* if G acts transitively.

The *orbit* of $x \in X$ is the set

$$G.x = \{g.x \,:\, g \in G\}$$

and the *stabilizer* of x, also called the *isotropy group* of x ths the closed subgroup

$$G_x = \{g \in G \,:\, g.x = x\}.$$

Definition 9.11. Let V be a finite dimensional vector space over K. A *rational representation* of G in V is a homomorphism of algebraic groups

$$r : G \to \mathrm{GL}(V).$$

We furthermore say that the rational representation $r : G \to \mathrm{GL}(V)$ of G is defined over a subfield $F \subset K$, if the homomorphism r is defined over F.

With the help of the notion of a rational representations we aim at proving the following theorem.

Theorem 9.12. *Any linear algebraic group G is isomorphic to a closed subgroup of GL_n.*

To prove the theorem we need to investigate the *regular left* and *regular right representation*

$$\lambda : G \to \mathrm{GL}(K[G]), \qquad g \mapsto \lambda(g),$$
$$\rho : G \to \mathrm{GL}(K[G]), \qquad g \mapsto \rho(g),$$

where $\lambda(g)$ and $\rho(g)$ is defined for $f \in K[G]$ as

$$(\lambda(g)f)(x) = f(g^{-1}x), \qquad (\rho(g)f)(x) = f(xg).$$

Note that we view here the affine algebra $K[G]$ as the ring of regular functions on G. In order to study these representations we consider the more general setting of a linear algebraic group G acting $a : G \times X \to X$ on an affine variety X. So a is given by an algebra homomorphism

$$a^* : K[X] \to K[G \times X] = K[G] \otimes_k K[X].$$

Furthermore the action of G on X induces a group representation

$$s : G \to \mathrm{GL}(K[X]), \qquad g \mapsto s(g),$$

where $s(g)$ is defined for $f \in \mathrm{GL}(K[X])$ as

$$s(g)f)(x) = f(g^{-1}.x).$$

Proposition 9.13. *In the above setting, let V be a finite dimensional subspace of $K[X]$. Then there is a finite dimensional subspace W of $K[X]$ which contains V and is stable under all $s(g)$ for $g \in G$. Then V is stable under all $s(g)$ if and only if $a^*V \subset K[G] \otimes V$. If this is so, the group representation defines a rational representation of G.*

Proof. It suffices to prove the first statement for $V = Kf$ a one dimensional subspace. Note that we can write

$$a^* f = \sum_{i=1}^{n} u_i \otimes f_i$$

with $u_1, \ldots, u_n \in K[G]$ and $f_1, \ldots, f_n \in K[X]$. Then we have that

$$(s(g)f))(x) = f(g^{-1}.x) = \sum_{i=1}^{n} u_i(g^{-1}) f_i(x).$$

So we see that all $s(g)f$ lie in the subspace W' of $K[X]$ generated by the f_i. The subspace W of W' spanned by the $s(g)f$ then has the wished properties.

Exactly this argument also shows that if $a^*V \subset K[G] \times V$ then the space V is stable under all $s(g)$. Conversely if V is stable for all $s(g)$, then choose a basis (f_i) of V and extend it to a basis $(f_i) \cup (g_j)$ of $K[X]$. Let $f \in V$. Then write

$$a^* f = \sum u_i \times f_i + \sum v_j \times g_j$$

where $u_i, v_j \in K[G]$. Then we have that

$$s(g)f = \sum u_i(g^{-1}) f_i + \sum v_j(g^{-1}) g_j.$$

By assumption we have that $v_j(g^{-1}) = 0$ for all g, hence all v_j vanish. This implies the second statement. □

We are now ready to prove Theorem 9.12.

Proof. (of Theorem 9.12) Write $K[G] = K[f_1, \ldots, f_n]$ and denote by V the vector space generated by all the f_i. By the proof of the last proposition we see that V is $\rho(g)$ stable for any $g \in G$. Furthermore there exists elements $(m_{ij})_{1 \le i,j \le n}$ in $K[G]$ with

$$\rho(g) f_i = \sum_{j=1}^{m} m_{ij}(g) f_j.$$

We claim next that the map

$$\phi : G \to \mathrm{GL}_n, \qquad g \mapsto (m_{ij}(g))_{1 \le i,j \le n}$$

defines a group homomorphism. To see this note that as ρ is a representation

$$\begin{aligned}\rho(g_1g_2)f_i &= \rho(g_1)\rho(g_2)f_i \\ &= \rho(g_1)\left(\sum_{j=1}^{n} m_{ij}(g)f_j\right) \\ &= \sum_{j=1}^{n} m_{ij}(g)\rho(g_1)f_j \\ &= \sum_{j=1}^{n} m_{ij}(g)\sum_{k=1}^{n} m_{jk}(g)f_k \\ &= \sum_{k=1}^{n}\left(\sum_{j=1}^{n} m_{ij}(g)m_{jk}(g)\right)f_k\end{aligned}$$

So we see that

$$m_{ik}(g_1g_2) = \sum_{j=1}^{n} m_{ij}(g)m_{jk}(g),$$

which shows precisely that ϕ is a group homomorphism. Furthermore, ϕ is a morphism of affine algebraic varieties. Thus $\phi(G)$ is a closed subgroup by Proposition 9.9. We next show that ϕ is injective. For this assume that $\phi(g) = e \in \mathrm{GL}_n$. Then $\rho(g)f_i = f_i$ and so $\rho(g)f = f$. As $\rho(g)$ is a faithful representation we conclude $g = e$. The corresponding algebra homomorphism

$$\phi^* : K[\mathrm{GL}_n] = K[T_{ij}, D^{-1}] \to K[G]$$

is given by $\phi^*T_{ij} = m_{ij}, \phi^*(D^{-1}) = \det(m_{ij})^{-1}$. As $f_i(g) = \sum_j m_{ji}(g)f_j(e)$ it follows that ϕ^* is surjective. So $K[G]$ is isomorphic to $K[\mathrm{GL}_n]/\ker(\phi^*)$. Thus ϕ defines an isomorphism of algebraic groups from G to the closed subgroup $\phi(G)$. □

Corollary 9.14. *Any linear algebraic groups is isomorphic to a closed subgroup of* SL_n.

Proof. To see this consider the well-defined map

$$\phi : \mathrm{GL}_n \to \mathrm{SL}_n, \qquad g \mapsto \begin{pmatrix} g & 0 \\ 0 & \det(g)^{-1} \end{pmatrix}.$$

It is clear that ϕ is an injective group homomorphism and a morphism of affine algebraic varieties. It is also straightforward to see that K-algebra homomorphism

$$\phi : K[\mathrm{SL}_n] \to K[\mathrm{GL}_n]$$

is surjective and hence indeed ϕ is isomorphism of algebraic groups from ϕ to the closed subgroup $\phi(\mathrm{GL}_n)$ of SL_{n+1}. The statement follows from composing the homomorphism from the proof Theorem 9.12 with ϕ. □

9.4 Jordan Decomposition

We begin with the following definitions. As always we denote by K an algebraically closed field.

Definition 9.15. Let V be a vector space over K. An endomorphism a of V is called *semi-simple* of *diagonalizable* if there is a basis of V consisting of eigenvectors of a. We call a *nilpotent* if $a^s = 0$ for some integers $s \geq 1$. Lastly, we say that a is *unipotent* if $a - 1$ is nilpotent.

We aim first at proving the following proposition.

Proposition 9.16. *(Additive Jordan Decomposition) Let $a \in \mathrm{End}(V)$. Then we can decompose the endomorphism a uniquely into commuting elements $a = a_s + a_n$, where $a_s \in \mathrm{End}(V)$ is diagonalizable and $a_n \in \mathrm{End}(V)$ is nilpotent. Moreover, there are polynomials $P, Q \in K[T]$ without constant terms such that $a_s = P(a)$ and $a_n = Q(a)$.*

We start with two Lemmas.

Lemma 9.17. *Let $S \subset M_n$ be a set of pairwise commuting matrices. Then there exists $x \in \mathrm{GL}_n$ such that xSx^{-1} consists of upper triangular matrices. If moreover all S are diagonalizable then they are simultaneously diagonalizable, i.e. there is some $x \in \mathrm{GL}_n$ such that xSx^{-1} consists of diagonal matrices.*

Proof. For the first claim, we proceed by induction on n. If $n = 1$, the assertion is clear. For the inductive step we may assume that not all elements of S are multiples of the identity, since then the statement is again trivial. If so, there is some $s \in S$ with an eigenspace that is a non-trivial subspace W of K^n, since otherwise s was a multiple of the identity. As all the matrices of S commute, we conclude that W is S-stable. By the inductive assumption, we may assume that the statement holds for the endomorphisms induced by S on W and on V/W. This implies the statement.

The second assertion is proved analogously writing V as a direct sum of eigenspaces of s. □

Lemma 9.18. *The product of two commuting semi-simple (nilpotent, unipotent) endomorphisms of V is again semi-simple (nilpotent, unipotent).*

Proof. This follows from the last Lemma in the semi-simple case. The unipotent and nilpotent cases are clear. □

Proof. (of Proposition 9.16) Write the characteristic polynomial as

$$\det(T \cdot 1 - a) = \prod (T - a_i)^{n_i}$$

be the characteristic polynomial of a, the a_i being the distinct eigenvalues of a. Denote

$$V_i = \{x \in V \,:\, (a - a_i)^{n_i} x = 0\}.$$

We claim that V_i is a-stable. To see this, note that if $x \in V_i$ then we have that

$$(a - a_i)^{n_i} ax = a(a - a_i) n_i x = 0$$

and hence V is a-stable. By the Chinese Remainder Theorem there exists $P \in K[T]$ such that

$$P(T) \equiv 0 \mod T$$

and

$$P(T) = a_i \mod (T - a_i)^{n_i}$$

for all i.

Set $a_s = P(a)$. Since $P(a_i) = a_i$ the eigenvalues of a_s are the same as those of a and a_s furthermore stabilizes the spaces V_i. Thus the V_i are the eigenspaces of a_s and V is their direct sum. Thus a_s is diagonalizable and $a - a_s$ is nilpotent. It remains to show uniqueness. To see this assume $a = b_s + b_n$ be a second decomposition as in the claim. Then we have that $a_s - b_s = b_n - a_n$ are both diagonalizable and nilpotent and hence equal to zero. □

Corollary 9.19. *(Multiplicative Jordan Decomposition) Let $a \in \mathrm{GL}(V)$ then we have a unique decomposition*

$$a = a_s a_u = a_u a_s,$$

where a_s is diagonalizable and a_u is unipotent.

Proof. Let $a = a_s + a_n$ be the additive Jordan decomposition. As a is invertible, we note that 0 is not an eigenvalue of a. Thus from the prove of the last proposition we see that a_s is invertible. Hence $a_u = 1 + a_s^{-1} a_n$ has the required properties. Uniqueness follows analogously to the last proposition. □

We call a linear algebraic group *unipotent*

9.5 Commutative Algebraic Groups

Theorem 9.20. *Let G be a commutative linear algebraic group. Then the sets G_s and G_u of semi-simple and unipotent elements are closed subgroups and the product map*

$$\pi : G_s \times G_u \to G$$

is an isomorphism of algebraic groups.

Proof. We assume without loss of generality that G is a closed subgroup of GL_n for some n. By Lemma 9.18 we conclude that G_s and G_u are closed subgroups. By applying Lemma 9.17 we can furthermore assume that G is upper triangular and such that $G_s = G \cap \mathbb{D}_n$. Thus G_s is closed. To see that G_u is closed we proceed analogously. The second assertion is clear. □

Definition 9.21. A linear algebraic group G is called *diagonalizable* if it is isomorphic to a closed subgroup of D_n the group of diagonal matrices for some n. We furthermore call G a *torus* if it is isomorphic to D_n for some n.

9.6 Linear Algebraic Groups defined over $\mathbb{R}$

We start by the the following observation.

Lemma 9.22. *Every point of a linear algebraic G group is smooth.*

Proof. By Proposition 8.38 we see that the set of smooth points is non-empty. So let $g \in G$ be a smooth point. Then $e = g^{-1}g$ is a smooth point of $g^{-1}G = G$ and so e is smooth point. This argument shows that any point in a linear algebraic group is smooth. □

This establishes the following useful corollary.

Corollary 9.23. *Let G be a linear algebraic group defined over $\mathbb{R}$. Then G is a Lie group over $\mathbb{C}$ and $G(\mathbb{R})$ is a Lie group over $\mathbb{R}$.*

Proof. By the last lemma we have that every point of G is smooth and Proposition 8.39 provides G with a chart at every point. This manifold structure on G is compatible with the group structure as the group operation is given by a morphism of algebraic varieties and thus given by polynomials and hence is smooth. □

Proposition 9.24. *Let $G \subset \mathrm{SL}_d$ be a linear algebra group defined over $\mathbb{R}$ with Lie algebra $\mathfrak{g}$. Then*

$$\mathfrak{g} \cap \mathfrak{sl}_d(\mathbb{R})$$

is the Lie algebra of $G(\mathbb{R})$.

Proof. See section 3.4 of [EW]. □

10 Compact Orbits and Orders

10.1 Closed Orbits for Rational Representations

We consider a rational representation $r : \mathrm{SL}_d \to \mathrm{GL}_n$ over $\mathbb{Q}$ and let $v \in \mathbb{Q}^n$. Then we consider the stabilizer

$$T = \mathrm{Stab}_{\mathrm{SL}_d}(v) = \{g \in \mathrm{SL}_d \,:\, r(g)v = v\}.$$

The aim of this subsection is to prove the following proposition. As usual we denote by $T(\mathbb{R})$ the $\mathbb{R}$-points of T.

Proposition 10.1. *The orbit of the $\mathbb{R}$-points of T*

$$\mathrm{SL}_d(\mathbb{Z})T(\mathbb{R}) \subset X_d$$

is closed.

Proof. We consider a sequence $k_n \in T(\mathbb{R})$ and

$$\mathrm{SL}_d(\mathbb{Z})k_n \to \mathrm{SL}_d(\mathbb{Z})k$$

where $k \in \mathrm{SL}_d(\mathbb{R})$. We want to show that $k \in \mathrm{SL}_d(\mathbb{Z})T(\mathbb{R})$. The above convergence translates to the existence of elements $\gamma_n \in \mathrm{SL}_d(\mathbb{Z})$ and $\varepsilon_n \in \mathrm{SL}_d(\mathbb{R})$ such that

$$\gamma_n k_n = \varepsilon_n k$$

with $\varepsilon_n \to I_d$.

We note that as a the rational representation $r : \mathrm{SL}_d \to \mathrm{GL}_n$ is defined over $\mathbb{Q}$, it is given by polynomials over $\mathbb{Q}$. Hence we there is some $N \in \mathbb{N}$ such that

$$r(\gamma) \in \frac{1}{N}\mathrm{Mat}_n(\mathbb{Z})$$

for all $\gamma \in \mathrm{SL}_d(\mathbb{Z})$. Furthermore, we denote by M the common denominator of the entries of v and so we have that

$$r(\gamma)v \in \frac{1}{MN}\mathbb{Z}^n$$

for all $\gamma \in \mathrm{SL}_d(\mathbb{Z})$.

As

$$r(\gamma_n)v = r(\gamma_n k_n)v = r(\varepsilon_n k)v \to r(k)v$$

we have that the sequence $r(\gamma_n)v$ stabilizes for large n and hence $r(\gamma_n)v = r(k)v$ for all n large enough. Thus $\gamma_n^{-1}k \in \mathrm{SL}_d(\mathbb{Z})T(\mathbb{R})$. □

10.2 Compact Orbits and Dirichlet's Unit Theorem

Throughout this section we consider an element $\zeta \in \mathbb{R}$ that is integral over $\mathbb{Z}$ and we consider the number field

$$K = \mathbb{Q}(\zeta) = \mathbb{Q}[T]/(f_\zeta),$$

where f_ζ is the minimal polynomial of ζ. Note that $f_\zeta \in \mathbb{Z}[T]$ as ζ is integral over $\mathbb{Z}$. Denote $d = [K : \mathbb{Q}]$ and recall that then f_ζ is of degree d. So f_ζ has n zeros over

$\mathbb{C}$, where we write $\zeta_1, \dots, \zeta_r$ for the real roots of f_ζ and $\zeta_{r+1}, \overline{\zeta_{r+1}}, \dots \zeta_{r+s}, \overline{\zeta_{r+s}}$ the complex roots of f_ζ, which appear in pairs. Then we have that $d = r + 2s$ and

$$f_\zeta(T) = (T - \zeta_1) \dots (T - \zeta_r)(T - \zeta_{r+1})(T - \overline{\zeta_{r+1}}) \dots (T - \zeta_{r+s}(T - \overline{\zeta_{r+s}}).$$

Any embedding $\phi : \mathbb{Q}(\zeta) \to \mathbb{C}$ is thus of the from $\phi(f(T)) \mapsto f(\zeta_i)$. By Proposition 1.20 the set of embeddings $\phi : \mathbb{Q}(\zeta) \to \mathbb{C}$ has the cardinality d and thus the zeros of f_ζ are all distinct.

We denote by $\mathcal{O}_K$ the ring of integers in K and we recall that an *order* a subring $\mathcal{O}$ of $\mathcal{O}_K$ with an integral basis of length n. The aim of this subsection is to prove Dirichlet's Unit Theorem for number fields of the above form.

Theorem 10.2. *(Dirichlet's Unit Theorem) The unit group $\mathcal{O}^*$ of an order $\mathcal{O}$ is the direct product of the group $\mu(K)$ of roots of unity which are contained in K and a free abelian group of rank $r + s - 1$.*

The theorem will follows rather easily from the compactness of the orbit of certain subgroups in X_d. In order to consider a slightly more general setting we define the following notion: A *proper $\mathcal{O}$-ideal* is an ideal $\mathfrak{a} \subset \mathcal{O}$ which contains and integral basis of $\mathcal{O}$ of length n such that

$$\mathcal{O} = \{b \in K \,:\, b\mathfrak{a} \subset \mathfrak{a}\}.$$

Note that $\mathfrak{a} = \mathcal{O}$ is a proper $\mathcal{O}$-ideal. So everything done below applies especially to the case $\mathfrak{a} = \mathcal{O}$.

For $b \in K$ consider the map from subsection 1.2

$$T_b : K \to K, \qquad x \mapsto bx$$

and recall that we defined the norm $N_{(K:\mathbb{Q})}(b) = \det(T_b)$.

Let $a_1, \dots, a_d$ be an integral basis for $\mathcal{O}$ that is contained in $\mathfrak{a}$. Proposition 1.42 shows that $a_1, \dots, a_d$ is also a basis for K over $\mathbb{Q}$. Thus considering K as a vector space over $\mathbb{Q}$ we can identify the $\mathbb{Q}$-linear map T_b with the representation

$$\psi(b) \in \mathrm{Mat}_d(\mathbb{Q})$$

with respect to the basis $a_1, \dots, a_d$. More formally $\psi(b)$ is given as follows: Write $ba_i = \sum_{j=1}^d b_{ij} a_j$ for $a_{ij} \in \mathbb{Q}$. Then $\psi(b)$ is given by

$$\psi(b) = \begin{pmatrix} b_{11} & b_{21} & \dots & b_{d1} \\ b_{12} & b_{22} & \dots & b_{d2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1d} & b_{2d} & \dots & b_{dd} \end{pmatrix}.$$

We claim the associated map

$$\psi : K \to \mathrm{Mat}_d(\mathbb{Q}), \qquad b \mapsto \psi(b)$$

is linear and satisfies $\psi(ab) = \psi(a)\psi(b)$ for $a, b \in K$. To see the last claim, note that linearity is clear. To see $\psi(ab) = \psi(a)\psi(b)$ for $a, b \in K$ denote by

$\psi(a) = (a_{ij})$,$\psi(b) = (b_{ij})$ and $\psi(ab) = (c_ij)$. Then we have for all $i = 1, \dots, d$

$$\sum_{j=1}^{d} c_{ij}a_j = (ab)a_i = a(ba_i) = a\sum_{k=1}^{d} b_{ik}a_k$$
$$= \sum_{k=1}^{d} b_{ik}aa_k = \sum_{k=1}^{d} b_{ik}\left(\sum_{j=1}^{d} a_{kj}a_j\right) = \sum_{j=1}^{d}\left(\sum_{k=1}^{d} b_{ik}a_{kj}\right)a_j.$$

Thus we conclude as $a_1, \dots a_d$ is a basis $c_{ij} = \sum_{k=1}^{d} b_{ik}a_{kj}$, which shows that $\psi(ab) = \psi(a)\psi(b)$.

Lemma 10.3. *An element $b \in K$ is contained in $\mathcal{O}$ if and only if $\psi(b) \in \mathrm{Mat}_d(\mathbb{Z})$. Furthermore $b \in \mathcal{O}^*$ if and only if*

$$\psi(b) \in \mathrm{GL}_d(\mathbb{Z}) = \{g \in \mathrm{Mat}_d(\mathbb{Z}) : \det(g) = \pm 1\}.$$

Proof. If $b \in \mathcal{O}$, then by definition $b\mathfrak{a} \subset \mathfrak{a}$ and hence by the definition of an integral basis there are coefficients $z_{ij} \in \mathbb{Z}$ such that

$$ba_i = \sum_{j=1}^{n} z_{ij}a_j$$

and so $\psi(b) \in \mathrm{Mat}_d(\mathbb{Z})$. The converse follows again as $a_1, \dots a_d$ is an integral basis of $\mathfrak{a}$. For the second statement note that as $\psi(1) = I_d$ we conclude $\psi(b)\psi(b^{-1}) = \psi(bb^{-1}) = \psi(1) = I_d$, showing that $\psi(b^{-1}) = \psi(b)^{-1}$. This implies the second statement. □

Consider $\mathcal{O}^1 = \{b \in \mathcal{O}^* : \psi(b) \in \mathrm{SL}_d(\mathbb{Z})\}$ and note that either $\mathcal{O}^1 = \mathcal{O}^*$ or it is an index two subgroup of $\mathcal{O}^*$. We furthermore consider for $v \in \mathrm{Mat}_d(\mathbb{Q})$ the rational representation

$$r : \mathrm{SL}_d \to \mathrm{GL}_{d^2}, \qquad g \mapsto (\mathrm{Mat}_d \ni v \mapsto gvg^{-1})$$

and as in the previous subsection we denote by T the stabilizer of $v = \psi(\zeta)$ so

$$T = \{g \in \mathrm{SL}_d : r(g)\psi(\zeta) = \psi(\zeta)\}$$
$$= \{g \in \mathrm{SL}_d : g\psi(\zeta)g^{-1} = \psi(\zeta)\}.$$

The main proposition necessary for this subsection will be the following.

Proposition 10.4. *The orbit of the $\mathbb{R}$-points of T*

$$\mathrm{SL}_d(\mathbb{Z})T(\mathbb{R}) \subset X_d$$

is compact and the corresponding cocompact lattice $T(\mathbb{Z}) = \mathrm{SL}_d(\mathbb{Z}) \cap T(\mathbb{R}) < T(\mathbb{R})$ satisfies

$$T(\mathbb{Z}) = \psi(\mathcal{O}^1).$$

Proof. We first show that $T(\mathbb{Z}) = \psi(\mathcal{O}^1)$. First note that as $\psi(ab) = \psi(a)\psi(b)$ for $a, b \in K$ we have that the minimal polynomial of $\psi(\zeta)$ is also f_ζ. Note that hence the minimal polynomial of $\psi(\zeta)$ has degree d and as the minimal polynomial divides the characteristic polynomial, which is also a normed polynomial of degree d, we conclude that f_ζ is the characteristic polynomial of $\psi(\zeta)$. As the zeros of f_ζ over $\mathbb{C}$ are all distinct, this implies that $\psi(\zeta)$ is diagonalizable over $\mathbb{C}$. This yields the existence of complex matrices D, U with $D = U\psi(\zeta)U^{-1}$ such that D is diagonal. Observe

$$\{g \in \mathrm{Mat}_d \,:\, g\psi(\zeta) = \psi(\zeta)g\} = U\{g' \in \mathrm{Mat}_d \,:\, g'D = Dg'\}U^{-1}$$

and hence the space

$$\{g \in \mathrm{Mat}_d \,:\, g\psi(\zeta) = \psi(\zeta)g\}$$

has complex dimension d and moreover as $\psi(\zeta)$ is a rational matrix we note that

$$\{g \in \mathrm{Mat}_d(\mathbb{Q}) \,:\, g\psi(\zeta) = \psi(\zeta)g\}$$

has dimension d over $\mathbb{Q}$. Finally, as ψ is linear and $\psi(K) \subset \{g \in \mathrm{Mat}_d(\mathbb{Q}) \,:\, g\psi(\zeta) = \psi(\zeta)g\}$ we conclude

$$\psi(K) = \{g \in \mathrm{Mat}_d(\mathbb{Q}) \,:\, g\psi(\zeta) = \psi(\zeta)g\}. \tag{10.1}$$

This allows us to derive that

$$\begin{aligned}\psi(\mathcal{O}^1) &= \psi(\{b \in K \,:\, \psi(b) \in \mathrm{SL}_d(\mathbb{Z})\}) \\ &= \mathrm{SL}_d(\mathbb{Z}) \cap T(\mathbb{R}) = T(\mathbb{Z}).\end{aligned}$$

We proceed by showing that the orbit $\mathrm{SL}_d(\mathbb{Z})T(\mathbb{R})$ is compact. We already know by Proposition 10.1 that $\mathrm{SL}_d(\mathbb{Z})T(\mathbb{R})$ is closed so it suffices to show that the orbit is bounded.

To see this, first note that

$$N_{(K:\mathbb{Q})}(b) = \det(\psi(b))$$

and so $N_{(K:\mathbb{Q})}(b) = 0$ if and only if $b = 0$, as K is a field and hence T_b is invertible.

Furthermore denote

$$\iota : \mathbb{Q}^d \to K, \qquad (v_1, \ldots, v_d) \mapsto v_1a_1 + \ldots + v_da_d.$$

We claim that for any $m = (m_i)_{1 \le i \le d} \in \mathbb{Z}^d$ and $h = (h_{ij})_{1 \le i,j \le d} \in \mathrm{Mat}_d(\mathbb{Q})$ which is of the form $\psi(b)$ for $b \in K$ that we have

$$\iota(mh) = \iota(m)b. \tag{10.2}$$

To prove equation (10.2) note

$$\iota(mh) = \iota\left(\begin{pmatrix} \sum_{i=1}^d m_ih_{i1} \\ \vdots \\ \sum_{i=1}^d m_ih_{id} \end{pmatrix}\right) = \sum_{i,j=1}^d m_ih_{ij}a_j$$

and

$$\iota(m)b = \sum_{i=1}^{d} m_i a_i b = \sum_{i,j=1}^{d} m_i h_{ij} a_j$$

showing equation (10.2).

We finally consider the map $\psi \circ \iota : \mathbb{Q}^d \to \mathrm{Mat}_d(\mathbb{Q})$ denote by

$$\Psi : \mathbb{R}^d \to \mathrm{Mat}_d(\mathbb{Q})$$

the $\mathbb{R}$-extension of $\psi \circ \iota$. Note that by (10.1) we have for any $h \in T(\mathbb{Q})$ $b \in K$ such that $\psi(b) = h$. Thus we conclude for all $m \in \mathbb{Z}$ with the help of equation (10.2) that

$$\Psi(mh) = \psi(\iota(mh)) = \psi(\iota(m)b) = \psi(\iota(m))\psi(b) = \Psi(m)h.$$

Thus this relation holds for any element $h \in T(\mathbb{R})$ by definition of Ψ.

We now show that the orbit $\mathrm{SL}_d(\mathbb{Z})T(\mathbb{R})$ is bounded. For a contradiction assume that is not the case and hence there is some $m \in \mathbb{Z}^d \backslash \{0\}$ and $h \in T(\mathbb{R})$ such that the vector mh is small enough such that

$$|\det(\Psi(mh))| < 1.$$

As $h \in \mathrm{SL}_d(\mathbb{R})$ we have by equation (10.2)

$$|\det(\Psi(m))| = |\det(\Psi(m)h)| = |\det(\Psi(mh))| < 1.$$

This shows since $\det(\Psi(m)) \in \mathbb{Z}$ that $\iota(m) = 0$ and hence $m = 0$, a contradiction. □

Proposition 10.5. *With the notation as above*

$$T(\mathbb{R}) \cong M \times \mathbb{R}^{r+s-1},$$

where M is a compact linear group with connected component of the identity isomorphic to $(\mathbb{S}^1)^s$.

Proof. This follows mainly by the fact established in the proof of Proposition 10.4 that

$$T(\mathbb{R}) = \{g \in \mathrm{SL}_d(\mathbb{R}) \,:\, g\psi(\zeta) = \psi(\zeta)g\}$$

and some consideration involving a generalization of the Jordan normal form, which we omit here. For more details see [EW] section 3.3. □

We are now ready to prove Theorem 10.2.

Proof. (of Theorem 10.2) By Proposition 10.4 and Proposition 10.5 we see that $\mathcal{O}^1$ can be viewed as a uniform lattice in $M \times \mathbb{R}^{r+s-1}$. Thus it follows that $\mathcal{O}^1$ is of the claimed form $F \times \mathbb{R}^{r+s-1}$ with F finite as M is compact. Next note that any element of $\mathcal{O}^1$ that is of finite order, must be a root of unity, implying the claim. □

10.3 Compact Orbits and Ideals

We denote again by

$$K = \mathbb{Q}(\zeta) = \mathbb{Q}[T]/(f_\zeta)$$

a number field with $\zeta \in \mathbb{R}$ integral over $\mathbb{Z}$ and f_ζ the minimal polynomial of ζ. Assume that K is of degree d and let r be the number of real embeddings and $2s$ be the number of complex embeddings such that $r + 2s = d$. We then call the number field K of type (r, s)

Denote by $\phi_1, \dots, \phi_r$ the real embeddings and by $\phi_{r+1}, \dots, \phi_{r+s}$ complex embeddings, where we choose only one of ϕ and $\overline{\phi}$ for ϕ any complex embedding. We then call

$$\phi = (\phi_1, \dots, \phi_r, \phi_{r+1}, \dots, \phi_{r+s}) : K \to \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s}$$

the *complete Galois* embedding.

Furthermore, as in the previous section we denote by $\mathcal{O}$ an order of K and by $\mathfrak{a} \subset \mathcal{O}$ a proper $\mathcal{O}$-ideal. We start with the following observation.

Lemma 10.6. *In the above setting,*

$$\phi(\mathfrak{a}) < \mathbb{R}^{r+2s}$$

is a lattice. Furthermore, for $a_1, \dots, a_n$ an integral basis we have that

$$\operatorname{vol}(\phi(\mathfrak{a})) = \det\left(\begin{pmatrix} \phi(a_1) \\ \vdots \\ \phi(a_d) \end{pmatrix}\right) \tag{10.3}$$

Proof. To see this choose an integral basis $a_1, \dots, a_d$ of $\mathfrak{a}$ and we then claim that $\phi(a_1), \dots, \phi(a_d)$ is linearly independent. In order to show this, note that if $\phi(a_1), \dots, \phi(a_d)$ was not linearly independent, then we could find non zero elements $b \in \mathfrak{a}$ such that $\phi(b)$ is arbitrarily small. As ϕ is injective and the map

$$\psi \circ \phi^{-1} : \phi(\mathfrak{a}) \to \operatorname{Mat}_d(\mathbb{Q})$$

is linear, we conclude that there is some $b \in \mathfrak{a}$ such that

$$|\mathrm{N}_{K:\mathbb{Q}}(b)| = |\det(\psi(b))| < 1$$

and so $b = 0$ as $b \in \mathfrak{a} \subset \mathcal{O}$. This shows that $\phi(a_1), \dots, \phi(a_d)$ is linearly independent and so

$$\phi(\mathfrak{a}) = \mathbb{Z}^d \begin{pmatrix} \phi(a_1) \\ \vdots \\ \phi(a_d) \end{pmatrix}$$

is a lattice and (10.3) follows. □

By replacing a_1 by $-a_1$, we thus arrive by

$$x_\mathfrak{a} = \frac{1}{\operatorname{vol}(\phi(\mathfrak{a}))^{\frac{1}{d}}} \phi(\mathfrak{a}) \in \mathrm{X}_d$$

at a unimodular lattice and by

$$g_{\mathfrak{a}} = \frac{1}{\mathrm{vol}(\phi(\mathfrak{a}))^{1/d}} \begin{pmatrix} \phi(a_1) \\ \vdots \\ \phi(a_d) \end{pmatrix}$$

at a matrix with determinant 1.

Consider the map

$$\iota : \mathbb{C} \to \mathrm{Mat}_2(\mathbb{R}), \qquad z = x + iy \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

and the matrix

$$v_{\zeta,\mathbb{R}} = \begin{pmatrix} \zeta_1 & & & & & & \\ & \ddots & & & & & \\ & & \zeta_r & & & & \\ & & & \iota(\zeta_{r+1}) & & & \\ & & & & \ddots & & \\ & & & & & \iota(\zeta_{r+s}) \end{pmatrix} \in \mathrm{Mat}_d(\mathbb{R}).$$

Furthermore denote by $T_{r,s}$ the centralizer of $v_{\zeta,\mathbb{R}}$, so

$$T_{r,s} = \{g \in \mathrm{SL}_d \,:\, g v_{\zeta,\mathbb{R}} g^{-1} = v_{\zeta,\mathbb{R}}\}.$$

We then deduce from Proposition 10.4 the next corollary.

Corollary 10.7. *In the above setting, the orbit*

$$x_{\mathfrak{a}} T_{r,s}(\mathbb{R}) \subset X_d$$

is compact.

Proof. We use the same notation for $\psi(\zeta)$ and T as in Proposition 10.4. Assume for the moment

$$\psi(\zeta) g_{\mathfrak{a}} = g_{\mathfrak{a}} v_{\zeta,\mathbb{R}} \tag{10.4}$$

Then

$$T_{r,s} = g_{\mathfrak{a}}^{-1} T \mathfrak{g}_{\mathfrak{a}}$$

and this implies

$$\mathrm{SL}_d(\mathbb{Z}) g_{\mathfrak{a}} T_{r,s}(\mathbb{R}) = \mathrm{SL}_d(\mathbb{R}) T(\mathbb{R}) g_{\mathfrak{a}}$$

is compact by Proposition 10.4.

To see 10.4 assume without loss of generality that $\mathrm{vol}(\phi(\mathfrak{a})) = 1$ and choose first e_i a standard basis vector with $1 \le i \le r$. Then note that $\phi_i(\zeta) = \zeta_i$. By this we see

$$\psi(\zeta) g_{\mathfrak{a}} e_i = \psi(\zeta) \begin{pmatrix} \phi_i(a_1) \\ \vdots \\ \phi_i(a_d) \end{pmatrix} = \begin{pmatrix} \phi_i(\zeta a_1) \\ \vdots \\ \phi_i(\zeta a_d) \end{pmatrix} = \begin{pmatrix} \zeta_i \phi_i(a_1) \\ \vdots \\ \zeta_i \phi_i(a_d) \end{pmatrix}$$

and

$$g_{\mathfrak{a}} v_{\zeta,\mathbb{R}} e_i = \mathfrak{g}_{\mathfrak{a}} \zeta_i e_i = \begin{pmatrix} \zeta_i \phi_i(a_1) \\ \vdots \\ \zeta_i \phi_i(a_d) \end{pmatrix}.$$

The case $r < i \le 2s$ is analogous and so 10.4 is proved. □

We next discuss the question, when two proper $\mathcal{O}$-ideals $\mathfrak{a}_1, \mathfrak{a}_2$ give rise to the same orbit. This question is answered by the next proposition.

Proposition 10.8. *Two proper $\mathcal{O}$-ideals $\mathfrak{a}_1, \mathfrak{a}_2$ have the same orbit under $T_{r,s}(\mathbb{R})$ in X_d if and only if they are ideals in the same number field and order, and are equivalent, i.e. there is some $a \in K\backslash\{0\}$ such that*

$$\mathfrak{a}_2 = a\mathfrak{a}_1.$$

Proof. Assume first $\mathfrak{a}_1 = a\mathfrak{a}_2$. Let $a_1, \ldots, a_d$ be an integral basis of $\mathfrak{a}_1$. Then we have that $aa_1, \ldots, aa_d$ is an integral basis of $\mathfrak{a}_2 = a\mathfrak{a}_1$. By the same argument as for 10.4 for $\cdot a$ instead of $\cdot\zeta$ we see that

$$g_{\mathfrak{a}_2} = \psi(a)g_{\mathfrak{a}_1} = g_{\mathfrak{a}}v_{b,\mathbb{R}}.$$

Hence, as $v_{b,\mathbb{R}} \in T_{r,s}(\mathbb{R})$, this shows

$$x_{\mathfrak{a}'} \in x_{\mathfrak{a}}T_{r,s}(\mathbb{R})$$

which shows that the orbits are the same.

Conversely assume that $\mathfrak{a}_1$ is a proper $\mathcal{O}_1$-ideal in a number field K_1 and $\mathfrak{a}_2$ is a proper $\mathcal{O}_2$-ideal in a number field K_2 and denote by $x_{\mathfrak{a}_1}$ and $x_{\mathfrak{a}_2}$ be the corresponding elements in X_d and assume that $x_{\mathfrak{a}_2} = x_{\mathfrak{a}_1}t$ for some $t \in T_{r,s}(\mathbb{R})$. Next note

$$\begin{aligned}
\mathcal{O} &= \{b \in K \,:\, b\mathfrak{a}_1 \subset \mathfrak{a}_1\} \\
&\cong \{v \in \langle\psi(K)\rangle_{\mathbb{R}} \,:\, \mathbb{Z}^d v \subset \mathbb{Z}^d\} \\
&= \{v \in \mathrm{Mat}_d(\mathbb{R}) \,:\, v\psi(\zeta) = \psi(\zeta)v \text{ and } \mathbb{Z}^d v \subset \mathbb{Z}^d\} \\
&\cong \{v \in \mathrm{Mat}_d(\mathbb{R}) \,:\, vv_{\zeta,\mathbb{R}} = v_{\zeta,\mathbb{R}}v \text{ and } x_{\mathfrak{a}_1}v \subset x_{\mathfrak{a}_1}\}
\end{aligned}$$

via conjugation by $g_{\mathfrak{a}}$ and 10.4. So we see that $\mathcal{O} \cong \mathcal{O}'$ and $K \cong K'$. Now suppose that $a_1, \ldots, a_d$ is a basis of $\mathfrak{a}_1$ so that $x_{\mathfrak{a}_1} = \mathbb{Z}^d g_{\mathfrak{a}}$ as before. Choosing the basis $a'_1, \ldots, a'_d$ of $\mathfrak{a}_2$ correctly gives $x_{\mathfrak{a}_2} = \mathbb{Z}^d g_{\mathfrak{a}_2}$ and $g_{\mathfrak{a}_2} = g_{\mathfrak{a}_1}t$. Hence $\phi_i(a'_j) = \phi_i(a_j)t_i$, where t_i (in $\mathbb{R}$ or $\mathbb{C}$) is the ith entry of the block diagonal matrix $t \in T_{r,s}(\mathbb{R})$. So

$$t_i = \phi_i\left(\frac{a'_j}{a_j}\right)$$

is independent of j. Hence there exists some $b \in K$ with $t_i = \phi_i(b)$ and so

$$\mathfrak{a}_2 = b\mathfrak{a}_1.$$

□

Example 10.9. Let $K = \mathbb{Q}(\sqrt{d})$, for d a positive square-free integer. So K is of type $(2, 0)$ and hence $T_{(2,0)}$ is just the diagonal subgroup contained in $\mathrm{SL}_2(\mathbb{R})$. Let

$$\mathfrak{a} = \mathcal{O} \subset \mathcal{O}_K\mathbb{Z}\left[\frac{d+\sqrt{d}}{2}\right]$$

be an order. So there is some integral number $x \in \mathcal{O}_K$ such that $\mathbb{Q}(x) = K$ and $1, x$ is an integral basis of $\mathbb{Z}[x]$ and hence

$$\mathcal{O} = \mathbb{Z}[x] = \mathbb{Z} \oplus x\mathbb{Z}.$$

Denote by $\phi_1, \phi_2 : K \to \mathbb{R}$ the two real embeddings such that

$$\begin{pmatrix} 1 & \phi_1(x) \\ 1 & \phi_2(x) \end{pmatrix}$$

has positive determinant. Thus we have that

$$\phi(\mathcal{O}) = \mathbb{Z}^2 \begin{pmatrix} 1 & \phi_1(x) \\ 1 & \phi_2(x) \end{pmatrix}$$

is a lattice with

$$\mathrm{vol}(\phi(\mathcal{O})) = \det\left(\begin{pmatrix} 1 & \phi_1(x) \\ 1 & \phi_2(x) \end{pmatrix}\right) = \phi_2(x) - \phi_1(x) > 0.$$

Thus we have the lattice

$$x_{\mathfrak{a}} = \frac{1}{\sqrt{\mathrm{vol}(\phi(\mathcal{O}))}}\phi(\mathcal{O}) = \frac{1}{\sqrt{\phi_2(x) - \phi_1(x)}} \begin{pmatrix} 1 & \phi_1(x) \\ 1 & \phi_2(x) \end{pmatrix}.$$

11 The Borel-Harish-Chandra Theorem

11.1 Quantitive Non-Divergence for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})$

The aim of this subsection is to prove the following theorem.

Theorem 11.1. *Let $x \in X_2$ be a non-periodic point for the horocycle flow. Then there is a constant $c > 0$ and and $T_x > 0$ such that for all $\varepsilon > 0$ and $T > T_x$ we have that*

$$\frac{1}{T}|\{t \in [0,T] \,:\, h_t \cdot x \notin X_2(\varepsilon)\}| \leq c\varepsilon.$$

We start with proving a special case, from which the theorem will follow straightforwardly. The next Lemma does not need the assumption that x is a non-periodic point.

Lemma 11.2. *Let $x = \Gamma g \in X_2$ be a non-periodic point for the horocycle flow and assume that the lattice*

$$\Gamma_x = \mathbb{Z}^2 g$$

corresponding to x does not contain any non-zero vector of norm strictly less than 1. Then there is a constant $c > 0$ such that for all $\varepsilon > 0$ and $T > 0$ we have

$$\frac{1}{T}|\{t \in [0,T] \,:\, h_t \cdot x \notin X_2(\varepsilon)\}| \leq c\varepsilon.$$

Proof. Let $T > 0$ and note that for $v = (v_1, v_2) \in \Gamma_x$ we have

$$vu_{-t} = (v_1, v_2)\begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} = (v_1, v_2 - tv_1).$$

For any $\varepsilon > 0$ and $v = (v_1, v_2) \in \Gamma_x\backslash\{0\}$ we write

$$\begin{aligned} P_v^\varepsilon &= \{t \in [0,T] \,:\, ||vu_{-t}||_2 < \varepsilon\} \\ &= \{t \in [0,T] \,:\, \sqrt{v_1^2 + (v_2 - tv_1)^2} < \varepsilon\}. \end{aligned}$$

We claim that for any vector $v = (v_1, v_2)$ outside the open ball $B_{T+2}^{||\cdot||_2}(0)$ we have that the P_v^1 is empty. To see this note first that if $|v_1| \geq 1$, then P_v^1 is definitely empty. So we assume that $v_1 \leq 1$. Then, as $||v||_2 \geq T + 2$, we conclude that $|v_2| \geq T + 1$. Hence we have for all $t \in [0,T]$,

$$|v_2 - tv_1| \geq |v_2| - t|v_1| \geq |v_2| - T \geq 1.$$

So

$$||vu_{-t}||_2 \geq 1.$$

As Γ_x is a lattice, there are only finitely many vectors contained in $B_{T+2}^{||\cdot||_2}(0)$ and so by the last claim only finitely many elements $v \in \Gamma_x\backslash\{0\}$ such that P_v^1 is non-empty. We call a vector $v \in \Gamma_x\backslash\{0\}$ primitive if $\mathbb{R}v \cap \Gamma_x = \mathbb{Z}v$. We henceforth denote by

$$v_1, \ldots, v_n$$

the finitely many elements $\Gamma_x\backslash\{0\}$, which are primitive and for which P_v^1 is non-empty. We furthermore assume that the vectors $v_1, \ldots, v_n$ are pairwise linearly independent. In the following we write

$$P_i^\varepsilon = P_{v_i}^\varepsilon.$$

As the lattice $\Gamma_x u_{-t}$ is unimodular, there can't be two linearly independent elements in $\Gamma_x u_{-t}$ that are of norm less than 1. Thus the sets P_i^ε are all mutually disjoint for all $\varepsilon \leq 1$. So we conclude

$$\{t \in [0,T] \,:\, h_t \cdot x \notin X_2(\varepsilon)\} = P_1^\varepsilon \sqcup \ldots \sqcup P_n^\varepsilon. \tag{11.1}$$

Assume for the moment that we have proved the statement for $\varepsilon \leq \frac{1}{2}$ and have found a constant c that satisfies the claim for $\varepsilon \leq \frac{1}{2}$. Then $c' = \max\{c, 2\}$ satisfies the claim for any ε. So we can assume for the rest of the proof $\varepsilon \leq \frac{1}{2}$.

We claim that there is a constant $c > 0$ such that

$$|P_i^\varepsilon| \leq c\varepsilon |P_i^1| \tag{11.2}$$

for all $\varepsilon \leq 2$. Then with the help of (11.1) and the obvious fact that $|P_1^1| + \ldots + |P_n^1| \leq T$ for all $i = 1, \ldots, n$ we derive

$$\begin{aligned}\frac{1}{T}|\{t \in [0,T] \,:\, h_t \cdot x \notin X_2(\varepsilon)\}| &\leq \frac{1}{T}(|P_1^\varepsilon| + \ldots + |P_n^\varepsilon|) \\ &\leq \frac{1}{T}(c\varepsilon|P_1^1| + \ldots + c\varepsilon|P_n^1|) \\ &\leq \frac{c\varepsilon T}{T} = c\varepsilon,\end{aligned}$$

proving the lemma.

So it remains to prove (11.2). Write $v_i = (v_1^i, v_2^i)$ and note that we can assume $|v_1^i| \leq \frac{1}{2}$ because otherwise P_i^ε is empty as $\varepsilon \leq \frac{1}{2}$. For simplicity we drop the sub- and superscripts. We furthermore assume without loss of generality that $v_1, v_2 > 0$. With these assumptions we have

$$\begin{aligned}P_i^\varepsilon &= \{t \in [0,T] \,:\, v_1^2 + (v_2 - tv_1)^2 < \varepsilon^2\} \\ &\subset \{t \in [0,T] \,:\, |v_2 - tv_1| < \varepsilon\}.\end{aligned}$$

Note that the equation

$$v_2 - tv_1 = \pm\varepsilon$$

has the solution $t_\pm = \frac{v_2 \mp \varepsilon}{v_1}$ and hence we can bound

$$|P_i^\varepsilon| \leq t_- - t_+ = \frac{2\varepsilon}{v_1}. \tag{11.3}$$

Next we observe as $|v_1| \leq \frac{1}{2}$

$$\begin{aligned}P_i^1 &= \{t \in [0,T] \,:\, v_1^2 + (v_2 - tv_1)^2 < 1\} \\ &= \{t \in [0,T] \,:\, |v_2 - tv_1| < \sqrt{1 - v_1^2}\} \\ &\supset \{t \in [0,T] \,:\, |v_2 - tv_1| < \sqrt{\tfrac{3}{4}}\}.\end{aligned}$$

Assume in the following that P_i^ε is not empty. As $\varepsilon \leq \frac{1}{2}$ we have that

$$P_i^1 \supset \{t \in \mathbb{R} : v_2 - tv_1 \in (\sqrt{\tfrac{3}{4}} - \tfrac{1}{2}, \sqrt{\tfrac{3}{4}})\}.$$

This shows that

$$|P_i^1| \geq \frac{\sqrt{\frac{3}{4}} - \frac{1}{2}}{v_1}. \tag{11.4}$$

Setting

$$c = \frac{2}{\sqrt{\frac{3}{4}} - \frac{1}{2}}$$

and combining (11.3) and (11.4) we conclude

$$|P_i^\varepsilon| \leq \frac{2\varepsilon}{v_1} = \frac{d\varepsilon(\sqrt{\frac{3}{4}} - \frac{1}{2})}{v_1} \leq c\varepsilon|P_1|,$$

proving the claim and the lemma. □

Proof. (of Theorem 11.1)

□

References

[Bor69] Armand Borel. *Linear Algebraic Groups*. W.A. Benjamin, 1969.

[Bos93] Siegfried Bosch. *Algebra*. Springer, 1993.

[ELMV12] Manfred Einsiedler, Elon Lindenstrauss, Phillipe Michel, and Akshay Venkatesh. The distribution of closed geodesics on the modular surface and duke's theorem. *L'Enseignement Mathématique*, 58:249–313, 2012.

[ELW] Manfred Einsiedler, Elon Lindenstrauss, and Thomas Ward. *Entropy in Ergodic Theory and Homogeneous Dynamics*. In preparation.

[EW] Manfred Einsiedler and Thomas Ward. *Homogeneous Dynamics and Applications*. In preparation.

[EW11] Manfred Einsiedler and Thomas Ward. *Ergodic Theory with a view towards Number Theory*. Springer, 2011.

[EW18] Manfred Einsiedler and Thomas Ward. *Functional Analysis, Spectral Theory and Applications*. Springer, 2018.

[Hum75] James Humphreys. *Linear Algebraic Groups*. Springer, 1975.

[Ioz17] Alessandra Iozzi. *Lecture Notes for Symmetric Spaces*. 2017.

[IZ17] Alessandra Iozzi and Robert Zimmer. *Lecture Notes for Lie Groups*. 2017.

[Lan02] Serge Lang. *Algebra*. Springer, 2002.

[Neu07] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 2007.

[Pin16a] Richard Pink. *Notes for Commutative Algebra written by Anna Bot*. 2016. `https://polybox.ethz.ch/index.php/s/3oztxX0d7OAHiFq`.

[Pin16b] Richard Pink. *Summary for Algebra*. 2016. `https://people.math.ethz.ch/~pink/ftp/Algebra-Zusammenfassung-20160906.pdf`.

[Pin17] Richard Pink. *Summary for Commutative Algebra*. 2017. `https://people.math.ethz.ch/~pink/ftp/Commutative-Algebra-Summary-20170622.pdf`.

[Rot10] Joseph Rotman. *Advanced Modern Algebra*. American Mathematical Society, 2010.

[Spr98] T. A. Springer. *Linear Algebraic Groups*. Birkhäuser, 1998.