Mini Project - Algebraic Number Theory

Dintyala Rahul Bhardwaj
Supervisor - Dr. Biswajyoti Saha

May 7, 2024

Contents

Chapter 1

Noetherian Rings and Dedekind Rings

1.1 Noetherian rings and modules

Lemma 1. Let $(T, \leq)$ be a partially ordered set. The following statements are equivalent :

1. Every non-empty subset of T contains a maximal element.
2. Every increasing sequence $(t_n)_{n\geq 0}$ of elements of T is stationary.

Proof. Let (t_n) be an increasing sequence of elements of T with respect to $\leq$ and t_p be a maximal element of (t_n). Then for $n \geq p$, $t_p \leq t_n$, so $t_n = t_p$ for all $n \geq p$.

Pick $\varnothing \neq S \subseteq P$. Let $x_1 \in S$ be arbitrary. Given $x_k \in S$, pick $x_{k+1} \in S$ strictly bigger than x_k. By hypothesis, we will eventually run out of bigger elements to pick at say x_n. Then by construction there are no larger elements than x_n, that is, x_n is a maximal element of S. $\square$

Theorem 1. Let $\mathcal{R}$ be a ring and $\mathcal{M}$ be an $\mathcal{R}$-module. The following statements are equivalent.

1. Every non-empty collection of submodules of $\mathcal{M}$ contains a maximal element.
2. Every increasing sequence of submodules of $\mathcal{M}$ is stationary.
3. Every submodule of $\mathcal{M}$ is of finite type.

Proof. We will first establish the equivalence of (2) and (3). Assume $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ be an increasing sequence of submodules of $\mathcal{M}$. From 3, $N := \cup_{i\geq 0} N_i$ is a finitely generated submodule of $\mathcal{M}$. Suppose N is generated by $a_1, \ldots, a_k \in N$. For all $i \in \{1, \ldots, k\}$, there is some $j_i \in \mathbb{N}$ such that $a_i \in N_{j_i}$. For $j := \max\{j_1, \ldots, j_k\}$, we have $a_1, \ldots, a_k \in N_j$.

Hence $N_j = N$. Therefore, every increasing sequence of submodules of $\mathcal{M}$ is stationary.

Suppose every increasing sequence of submodules of $\mathcal{M}$ is stationary. Let N be a submodules of $\mathcal{M}$. For the sake of a contradiction, suppose N is not finitely generated. Any finitely generated submodule of N is not equal to N. So we can inductively choose a sequnce $a_i \in N \setminus \langle a_1, \ldots, a_{i-1} \rangle$. The chain : $\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \cdots$ is strictly increasing contradicting 2. Hence, every submodule of $\mathcal{M}$ is finitely generated.

The equivalence of (1) and (2) follows from Lemma 1. $\square$

Definition 1 (Noetherian Module)**.** An $\mathcal{R}$-module $\mathcal{M}$ is called Noetherian if it satisfies the equivalent conditions of Theorem 1.

Definition 2 (Noetherian Ring)**.** A ring $\mathcal{R}$ is called Noetherian if, considered as an $\mathcal{R}$-module, it is a Noetherian module.

Proposition 1. Let $0 \to \mathcal{M}' \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}'' \to 0$ be an exact sequnce of $\mathcal{R}$-modules. Then $\mathcal{M}$ is Noetherian if and only if $\mathcal{M}'$ and $\mathcal{M}''$ are Noetherian.

Proof. Suppose $\mathcal{M}$ is Noetherian. Since $\mathcal{M}'$ is isomorphic to a sub module of $\mathcal{M}$, $\mathcal{M}'$ is Noetherian. Let N'' be a submodule of $\mathcal{M}''$. Then $g^{-1}(N'')$ is a submodule of $\mathcal{M}$. Therefore there exist $x_1, \ldots, x_r \in g^{-1}(N'')$ such that $g^{-1}(N'')$ is generated by $x_1, \ldots, x_r$. Since g is surjective, we have $N'' = g(g^{-1}(N''))$. It follows that N'' is generated by $g(x_1), \ldots, g(x_r)$. Thus M'' is Noetherian.

Conversely, suppose $\mathcal{M}'$ and $\mathcal{M}''$ are Noetherian. Let N be a submodule of $\mathcal{M}$. Then $g(N)$ is a submodule of $\mathcal{M}''$. Therefore, there exist $x_1, \ldots, x_r \in N$ such that $g(x_1), \ldots, g(x_r)$ generate $g(N)$. Next, $f^{-1}(N)$ is a submodule of $\mathcal{M}'$. Therefore there exist $y_1, \ldots, y_s \in f^{-1}(N)$ such that $f^{-1}(N)$ is generated by $y_1, \ldots, y_s$. We claim that N is generated by $x_1, \ldots, x_r, f(y_1), \ldots, f(y_s)$. Let $z \in N$. Then $g(z) = \sum_{i=1}^{r} a_i g(x_i)$ with $a_1, \ldots, a_r \in \mathcal{R}$. Let $z' = z - \sum_{i=1}^{r} a_i x_i$. Then $z' \in N \cap \ker g = N \cap \operatorname{Im} f$. Therefore $z' = f(x')$ with $x' \in f^{-1}(N)$. There exist $b_1, \ldots, b_s \in \mathcal{R}$ such that $x' = \sum_{j=1}^{s} b_j y_j$. Thus $z = \sum_{i=1}^{r} a_i x_i + \sum_{j=1}^{s} b_j f(y_j)$. $\square$

Proposition 2. Let $\mathcal{R}$ be a ring, $\mathcal{M}$ an $\mathcal{R}$-module, and $\mathcal{M}'$ a submodule of $\mathcal{M}$. Then $\mathcal{M}$ is Noetherian if and only if $\mathcal{M}'$ and $\mathcal{M}/\mathcal{M}'$ are Noetherian.

Proof. Consider the short exact sequence :

$$0 \to \mathcal{M}' \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{M}/\mathcal{M}' \to 0$$

where f is the inclusion map and g takes $x \in \mathcal{M}$ to $x + \mathcal{M}'$. Note that f is clearly injective and g is surjective because for all $x + \mathcal{M}' \in \mathcal{M}/\mathcal{M}'$, $g(x) = x + \mathcal{M}'$. We observe that $\ker g = \{x \in \mathcal{M} : x + \mathcal{M}' = \mathcal{M}'\} = \mathcal{M}' = \operatorname{Im} f$. Applying proposition 1 to this sequence completes the proof. $\square$

Corollary. Let $\mathcal{R}$ be a ring and let $\mathcal{M}_1, \ldots, \mathcal{M}_n$ be Noetherian $\mathcal{R}$-modules. Then the $\mathcal{R}$-module product $\prod_{i=1}^{n} E_i$ is Noetherian.

Proof. For $n = 2$, we want to show that if $\mathcal{M}_1$ and $\mathcal{M}_2$ are Noetherian, then the product $\mathcal{M}_1 \times \mathcal{M}_2$ is Noetherian. Consider the sequence :

$$0 \to \mathcal{M}_1 \xrightarrow{f} \mathcal{M}_1 \times \mathcal{M}_2 \xrightarrow{g} \mathcal{M}_2 \to 0,$$

where $f(x) = (x, 0)$ for all $x \in \mathcal{M}_1$ and $g(x, y) = y$ for all $x, y \in \mathcal{M}_1 \times \mathcal{M}_2$. Note that f is injective and g is surjective. We observe that $\operatorname{Im} f = \{(x, 0) : x \in \mathcal{M}_1\} \cong \mathcal{M}_1 = \ker g$. Therefore, this is a short exact sequence. Applying Proposition 1 to this sequence proves the result for $n = 2$. Inductively, it follows that $\prod_{i=1}^{n} E_i$ is Noetherian. □

Corollary. Let $\mathcal{R}$ be a Noetherian ring and let $\mathcal{M}$ be an $\mathcal{R}$-module of finite type. then $\mathcal{M}$ is a Noetherian module.

Proof. Suppose $\mathcal{R}$ is generated by $x_1, \ldots x_r$. We prove the assertion by induction on r. First suppose $r = 1$. Let $g : \mathcal{R} \to \mathcal{M}$ be the map defined by $g(a) = ax_1$. Then g is a surjective homomorphism and it follows that $\mathcal{M}$ is Noetherian from Propostion 1.

Now, suppose $r \geq 2$. Let $\mathcal{M}' = Ax_r$. Let $g : \mathcal{M} \to \mathcal{M}/\mathcal{M}'$ be the natural surjection. Then $\mathcal{M}/\mathcal{M}'$ is generated by $g(x_1), \ldots, g(x_{r-1})$. Therefore by induction both $\mathcal{M}'$ and $\mathcal{M}/\mathcal{M}'$ are Noetherian. Therefore by Propostion 1, $\mathcal{M}$ is Noetherian. □

1.2 An application concerning integral elements

Lemma 2. Let $\mathcal{R}$ be an integrally closed ring. Let $\mathcal{K}$ be its field its field of fractions, $\mathcal{L}$ be an extension of finite degree n of $\mathcal{K}$, and $\mathcal{R}'$ is the integral closure of $\mathcal{R}$ in $\mathcal{L}$. Suppose $\mathcal{K}$ is of characteristic 0. Then $\mathcal{R}'$ is an $\mathcal{R}'$-submodule of a free $\mathcal{R}$-module of rank n.

Proof. Let $(x_1, \ldots, x_n)$ be a base of $\mathcal{L}$ over $\mathcal{K}$. Each x_i is algebraic over $\mathcal{K}$, so for any i, we have an equation of the form $a_n x^n + a_{n-1} x^n + \cdots + a_0 = 0 (a_j \in \mathcal{R}\ \forall\ j)$. We may assume $a_n \neq 0$. Multiplying through by a_n^{n-1}, we see that $a_n x_i$ is integral over $\mathcal{R}$. Put $x_i' = a_n x_i$. Then $(x_1', \ldots, x_n')$ is a base for $\mathcal{L}$ over $\mathcal{K}$ contained in $\mathcal{R}'$. Hence, there exists another base $(y_1, \ldots, y_n)$ of $\mathcal{L}$ over $\mathcal{K}$ such that $\operatorname{Tr}(x_i' y_j) = \delta_{ij}$. Let $z \in \mathcal{R}'$. Since $(y_1, \ldots, y_n)$ is a base for $\mathcal{L}$ over $\mathcal{K}$, we may write $z = \sum_{j=1}^{n} b_j y_j$ with $b_j \in \mathcal{K}$. For any i, we have $x_i' z \in \mathcal{R}'$. Therefore, $\operatorname{Tr}(x_i' z) \in \mathcal{R}$. Thus, $\operatorname{Tr}(x_i' z) = \operatorname{Tr}(\sum_j b_j x_i' y_j) = \sum b_j \operatorname{Tr}(x_i' y_j) = \sum b_j \delta_{ij} = b_i$. Hence, it follows that $b_i \in \mathcal{R}$ for all i, which implies that $\mathcal{R}'$ is a submodule of the free $\mathcal{R}$-module $\sum_{j=1}^{n} \mathcal{R} y_j$. □

Proposition 3. Let $\mathcal{R}$ be a Noetherian integrally closed ring. Let $\mathcal{K}$ be its field of fractions, $\mathcal{L}$ a finite extension of $\mathcal{K}$, and $\mathcal{R}'$ the integral closure of $\mathcal{R}$ in $\mathcal{L}$. Suppose that $\mathcal{K}$ is of charactersitic 0. Then $\mathcal{R}'$ is a $\mathcal{R}$-module of finite type and a Noetherian ring.

Proof. From previous lemma we know that $\mathcal{R}'$ is a submodule of a free $\mathcal{R}$-module of rank n. Thus $\mathcal{R}$' is a $\mathcal{R}$-module of finite type, and therefoe, a Noetherian module. On the other hand, the ideals of $\mathcal{R}'$ are special cases of $\mathcal{R}$-submodules of $\mathcal{R}$'. They satisfy the maximal condition, so $\mathcal{R}'$ is a Noetherian ring. □

1.3 Some preliminaries concerning ideals

Definition 3 (Prime and Maximal Ideals)**.** Let $\mathcal{R}$ be a non-zero ring and $\mathcal{P}$ be an ideal of $\mathcal{R}$. We say that $\mathcal{P}$ is a **prime ideal** of $\mathcal{R}$ is the following hold :

1. $\mathcal{P} \neq \mathcal{R}$,
2. if there exist ideals $\mathcal{I}, \mathcal{J}$ of $\mathcal{R}$ such that $\mathcal{I}, \mathcal{J} \subseteq \mathcal{R}$, then $\mathcal{I} \subseteq \mathcal{P}$ or $\mathcal{J} \subseteq \mathcal{P}$.

An ideal $\mathcal{M}$ of $\mathcal{R}$ is called a **maximal ideal** if the following hold :

1. $\mathcal{M} \neq \mathcal{R}$,
2. if there exists any ideal $\mathcal{I}$ of $\mathcal{R}$ such that $\mathcal{M} \subseteq \mathcal{I}$, then either $\mathcal{I} = \mathcal{M}$ or $\mathcal{I} = \mathcal{R}$.

Proposition 4. Let $\mathcal{R}$ be a non-zero commutative ring with unity. Then an ideal $\mathcal{P}$ is prime ideal if and only if for any $a, b \in \mathcal{R}$ whenever $a \cdot b \in \mathcal{P}$, then $a \in \mathcal{P}$ or $b \in \mathcal{P}$.

Proof. Let $x, y \in \mathcal{R}$ such that $xy \in \mathcal{P}$. So, $(xy) \subseteq \mathcal{P}$. Since $\mathcal{R}$ is commutative $(xy) = (x)(y) \subseteq \mathcal{R}$. By definition, either $(x) \subseteq \mathcal{P}$ or $(y) \subseteq \mathcal{P}$. Hence, either $x \in \mathcal{P}$ or $y \in \mathcal{P}$, proving the forward direction.

Let $\mathcal{I}, \mathcal{J} \subseteq \mathcal{P}$. Without loss of generality, let $\mathcal{I} \subsetneq \mathcal{P}$. Then there exists $x \in \mathcal{I}$ such that $x \notin \mathcal{P}$. Let $y \in \mathcal{J}$. Since $\mathcal{J}$ is an ideal, $xy \in \mathcal{J}$. But $xy \in \mathcal{I}\mathcal{J} \subseteq \mathcal{P}$, so $xy \in \mathcal{P}$. Hence, either $x \in \mathcal{P}$ or $y \in \mathcal{P}$. Since we assumed $x \notin \mathcal{P}$, $y \in \mathcal{P}$. Since choice of y was arbitrary, $\mathcal{J} \subseteq \mathcal{P}$, proving the reverse direction. □

Proposition 5. Let $\mathcal{R}$ be a commutative ring with unity. Then an ideal $\mathcal{P}$ of $\mathcal{R}$ is a prime ideal if and only if the quotient ring $\mathcal{R}/\mathcal{P}$ is an integral domain.

Proof. Let $\mathcal{P}$ be a prime ideal, $a + \mathcal{P}, b + \mathcal{P} \in \mathcal{R}/\mathcal{P}$. If $(a + \mathcal{P})(b + \mathcal{P}) = p$, then we get $ab \in \mathcal{P}$. Hence, $a \in \mathcal{P}$ or $b \in \mathcal{P}$. So $a + \mathcal{P} = \mathcal{P}$ or $b + \mathcal{P} = \mathcal{P}$.

Hence, $\mathcal{R}/\mathcal{P}$ is an integral domain.

Now let $\mathcal{R}/\mathcal{P}$ be an integral domain. Let $a \notin \mathcal{P}$ and $b \notin \mathcal{P}$ then $a + \mathcal{P} = \mathcal{P}$ and $b + \mathcal{P} \neq \mathcal{P}$. Therefore $(a + \mathcal{P})(b + \mathcal{P}) \neq p$. Hence, $ab + \mathcal{P} \neq \mathcal{P}$ implies $ab \notin \mathcal{P}$. Hence, $\mathcal{P}$ is prime. □

Proposition 6. Let $\mathcal{R}$ be a commutative ring with unity. Then an ideal $\mathcal{M}$ of $\mathcal{R}$ is a maximal ideal if and only if the quotient ring $\mathcal{R}/\mathcal{M}$ is a field.

Proof. Let $\mathcal{M}$ be a maximal ideal. Let $a + \mathcal{M}$ be a non zero element of $\mathcal{R}/\mathcal{M}$. Hence $a + \mathcal{M} \neq \mathcal{M}$, or $a \notin \mathcal{M}$. Consider the ideal $\mathcal{M} + (a)$. Observe that $\mathcal{M} \subsetneq \mathcal{M} + (a) \subseteq \mathcal{R}$. Since $\mathcal{M}$ is maximal $\mathcal{M} + (a) = \mathcal{R}$. Hence, there exist $r \in \mathcal{R}$, $m_0 \in \mathcal{M}$ such that $m_0 + ra = 1$. It follows that $(a + \mathcal{M})(r + \mathcal{M}) = ar + \mathcal{M} = 1 - m_0 + \mathcal{M} = 1 + \mathcal{M}$. Hence, $a + \mathcal{M}$ is a unit. Since choice of a was arbitrary, it follows every non-zero element in $\mathcal{R}/\mathcal{M}$ is a unit. Hence, $\mathcal{R}/\mathcal{M}$ is a field.

Now let $\mathcal{I}$ be an ideal such that $\mathcal{M} \subsetneq \mathcal{I} \subseteq \mathcal{R}$. Then there exists an $r \in \mathcal{I} \setminus \mathcal{M}$. Since $\mathcal{R}/\mathcal{M}$ is a field, since $r \notin \mathcal{M}$, $r + \mathcal{M}$ has an inverse, say $r_1 + \mathcal{M}$. Now $(r + \mathcal{M})(r_1 + \mathcal{M}) = 1 + \mathcal{M} \Rightarrow rr_1 + \mathcal{M} = 1 + \mathcal{M}$, or $rr_1 - 1 \in \mathcal{M} \subset \mathcal{I}$. Since $r \in \mathcal{I}, r_1 \in \mathcal{R}$, we get $rr_1 \in \mathcal{I}$, so $rr_1 - (rr_1 - 1) \in \mathcal{I}$ or $1 \in \mathcal{I}$. Hence, $\mathcal{I} = \mathcal{R}$. Therefore, $\mathcal{M}$ is maximal. □

Lemma 3. Let $\mathcal{R}$ be a ring, $\mathcal{P}$ be a prime ideal of $\mathcal{R}$, and let $\mathcal{R}'$ be a subring of $\mathcal{R}$. Then $p \cap \mathcal{R}'$ is a prime ideal of $\mathcal{R}'$.

Proof. Let $x \in \mathcal{R}'$ and $\alpha \in \mathcal{P} \cap \mathcal{R}'$, then $\alpha \in \mathcal{P} \Rightarrow x\alpha \in \mathcal{P}$. Since, $x \in \mathcal{R}'$ and $\alpha \in \mathcal{R}$, we ger $x\alpha \in \mathcal{P} \cap \mathcal{R}'$. Therefore, $p \cap \mathcal{R}'$ is an ideal of $\mathcal{R}'$. Consider the map ψ defined as $\psi : \mathcal{R}'/\mathcal{R}' \cap \mathcal{P} \to \mathcal{R}/\mathcal{P}, x + \mathcal{R}' \cap \mathcal{P} \mapsto x + \mathcal{P}$. ψ is clearly a homomorphism. The kernel of $\psi = \{x + \mathcal{R}' \cap \mathcal{P} : x + \mathcal{P} = \mathcal{P}\} = \{x + \mathcal{R}' \cap \mathcal{P} : x \in \mathcal{P}\} = \{\mathcal{R}' \cap \mathcal{P}\}$. Hence, we have $\mathcal{R}'/\mathcal{R}' \cap \mathcal{P}$ is a subring of $\mathcal{R}/\mathcal{P}$, so it must be an integral domain. □

Definition 4 (Sum and product of ideals)**.** Let $\mathcal{R}$ be a ring and $\mathcal{I}, \mathcal{J}$ be two ideals of $\mathcal{R}$. We define the sum of two ideals $\mathcal{I}, \mathcal{J}$ as follows :

$$\mathcal{I} + \mathcal{J} := \{x + y : x \in \mathcal{I}, y \in \mathcal{J}\}.$$

We define the product of two ideals $\mathcal{I}, \mathcal{J}$ of $\mathcal{R}$ as follows :

$$\mathcal{I}\mathcal{J} := \left\{ \sum_{i=1}^{n} x_i y_i : n \in \mathbb{N}, x_i \in \mathcal{I}, y_i \in \mathcal{J} \right\}.$$

Lemma 4. If a prime ideal $\mathcal{P}$ of $\mathcal{R}$ contains a product $\mathcal{I}_1 \cdots \mathcal{I}_n$ of ideals. Then $\mathcal{P}$ contains at least one of the ideals $\mathcal{I}_i$.

Proof. If $\mathcal{I}_i \not\subset \mathcal{P}$ for any i, then there exist $a_i \in \mathcal{I}_i \setminus \mathcal{P}$ for all i. Therefore, $a_i \cdots a_n \notin \mathcal{P}$, since $\mathcal{P}$ is prime. But $a_i \cdots a_n \in \mathcal{I}_1 \cdots \mathcal{I}_n$ which contradicts the hypothesis of the lemma. □

Lemma 5. In a Noetherian ring every ideal contain a product of prime ideals. In a Noetherian integral domain $\mathcal{R}$, every non-zero ideal contains a product of prime ideals.

Proof. Let Φ be the set of non zero ideals of $\mathcal{R}$ which don't contain product of non-zero prime ideals. We want to show that Φ is non-empty. For the sake of a contradiction, let $|\Phi| > 0$. Since $\mathcal{R}$ is Noetherian, Φ contains a maximal element $\mathcal{B}$. The ideal $\mathcal{B}$ cannot be prime; otherwise $\mathcal{B} \in \Phi$. Thus, there exist $x, y \in \mathcal{R} \setminus \mathcal{B}$ such that $xy \in \mathcal{B}$. The ideals $\mathcal{B} + (x)$ and $\mathcal{B} + (y)$ contain $\mathcal{B}$ as a proper subset. Therefore, since $\mathcal{B}$ is maximal, they do not belong to Φ. It follows that they both contain products of non zero prime ideals.

$$\mathcal{B} + (x) \supset p_1 \cdots p_n, \quad \mathcal{B} + (y) \supset q_1 \cdots q_r$$

Since $xy \in \mathcal{B}$,

$$(\mathcal{B} + (x))(\mathcal{B} + (y)) \subset \mathcal{B}.$$

Hence, $p_1 \cdots p_n \cdot q_1 \cdots q_r \subset \mathcal{B}$, a contradiction. Hence, $|\Phi| = 0$. □

Definition 5 (Fractional ideals)**.** Let $\mathcal{R}$ be an integral domain and $\mathcal{K}$ be its field of fractions. Let $\mathcal{I}$ be an $\mathcal{R}$-submodule. We call $\mathcal{I}$, a fractional ideal of $\mathcal{K}$ if there exists a $d \in \mathcal{R} \setminus \{0\}$ such that $d \cdot \mathcal{I} \subseteq \mathcal{R}$.

The ordinary ideals of $\mathcal{R}$ are fractional ideals with $d = 1$. They are also called **integral ideals** to distinguish them from fractional ideals.

Proposition 7. The following are true :

1. Any $\mathcal{R}$-submodule $\mathcal{I}$ of finite type contained in $\mathcal{K}$ is a fractional ideal.
2. If $\mathcal{R}$ is Noetherian, every fractional ideal $\mathcal{I}$ is an $\mathcal{R}$-module of finite type.
3. If $\mathcal{I}$ and $\mathcal{I}'$ are fractional ideals, then the sets $\mathcal{I} \cap \mathcal{I}'$, $\mathcal{I} + \mathcal{I}'$, and $\mathcal{I}\mathcal{I}'$ are all fractional ideals.

Proof.

1. Since $\mathcal{I}$ is an $\mathcal{R}$-submodule of finite type it must be generated by a finite set of generators $\langle a_1, \ldots, a_n \rangle$. If $a_i = p_i/q_i$ for all i, then the product $d = \prod_{i=1}^{n} q_i$ is a common denominator for $\mathcal{I}$.
2. Since $d \cdot \mathcal{I} \subseteq \mathcal{R}$, we get $\mathcal{I} \subseteq d^{-1}\mathcal{R}$. Since $d^{-1}\mathcal{R}$ is isomorphic to $\mathcal{R}$, $\mathcal{I}$ is a Noetherian module.
3. If d and d' are the common denominators for $\mathcal{I}$ and $\mathcal{I}'$ respectively then dd' is a common denominator for $\mathcal{I} \cap \mathcal{I}'$, $\mathcal{I} + \mathcal{I}'$, and $\mathcal{I}\mathcal{I}'$.

□

1.4 Dedekind Domains

Definition 6 (Dedekind domain). An integral domain $\mathcal{R}$ is called a Dedekind domain if it is Noetherian and integrally closed, and if every non-zero prime ideal of $\mathcal{R}$ is maximal.

Example. Every principal ideal ring is a Dedekind domain.

Theorem 2. Let $\mathcal{R}$ be a Dedekind domain, $\mathcal{K}$ be its field of fractions. Let $\mathcal{L}$ be a finite extension of $\mathcal{K}$ and $\mathcal{R}'$ be the integral closure of $\mathcal{R}$ in $\mathcal{L}$. If $\mathcal{K}$ is of characteristic 0. Then $\mathcal{R}'$ is a Dedekind domain and an $\mathcal{R}$-module of finite type.

Proof. We need to show three things. That $\mathcal{R}'$ is integrally close, that $\mathcal{R}'$ is Noetherian, and that every non-zero prime ideal of $\mathcal{R}$ is maximal. The first part is done for us by construction. From Proposition 3, we get that $\mathcal{R}'$ is Noetherian and a $\mathcal{R}$-module of finite type. It remains to show that every prime ideal $\mathcal{P}' \neq (0)$ of $\mathcal{R}'$ is maximal. Let $x \in \mathcal{P}' \notin (0)$ and the following be its minimal polynomial over $\mathcal{R}$:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0. \qquad (a_i \in \mathcal{R})$$

Note that $a_0 \neq 0$, because if not then dividing through by x, we get a polynomial of lower degree. Note that since $a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$, we get that $a_0 \in \mathcal{R}'x$. But since $a_0 \in \mathcal{R}$, we have that $x \in \mathcal{R}'x \cap \mathcal{R} \subseteq \mathcal{P}' \cap \mathcal{R}$. Hence, $\mathcal{P}' \cap \mathcal{R} \neq (0)$. Since $\mathcal{P}'$ is a prime ideal, $\mathcal{P}' \cap \mathcal{R}$ is a prime ideal. Since $\mathcal{R}$ is a Dedekind ring $\mathcal{P}' \cap \mathcal{R}$ is a maximal ideal of $\mathcal{R}$ and so $\mathcal{R}/\mathcal{P}' \cap \mathcal{R}$ is a field. Consider the map $\varphi : \mathcal{R} \to \mathcal{R}'/\mathcal{P}'$ such that $x \mapsto x + \mathcal{P}'$. This is clearly a well defined homomorphism. The kernel of this map is $\ker\varphi := \{x \in \mathcal{R} : x + \mathcal{P}' = \mathcal{P}'\} = \mathcal{R} \cap \mathcal{P}'$. It follows that $\mathcal{R}/\mathcal{R} \cap \mathcal{P}'$ is a subring of $\mathcal{R}'/\mathcal{P}'$.

We note that $\mathcal{R}'/\mathcal{P}'$ is integral over $\mathcal{R}/\mathcal{P}' \cap \mathcal{R}$ [a]. Thus $\mathcal{R}'/\mathcal{P}'$ is a field, so $\mathcal{P}'$ is maximal. □

[a] Pick an element $x + \mathcal{P}' \in \mathcal{R}'/\mathcal{P}'$. Since $x \in \mathcal{R}'$, there exist $n \in \mathbb{Z}, a_0, \ldots, a_{n-1} \in \mathcal{R}$ such that $a_0 + a_1 x + \cdots + x^n = 0$. Hence, $(a_0 + \mathcal{R} \cap \mathcal{P}') + (a_1 + \mathcal{R} \cap \mathcal{P}')(x + \mathcal{P}') + \cdots + (1 + \mathcal{R} \cap \mathcal{P}')(x + \mathcal{P}')^n = \mathcal{R} \cap \mathcal{P}'$ or $x + \mathcal{P}'$ is integral over $\mathcal{R}/\mathcal{R} \cap \mathcal{P}'$.

Theorem 3. Let $\mathcal{R}$ be a Dedekind domain which is not a field. Every maximal ideal of $\mathcal{R}$ is invertible in the monoid of fractional ideals of $\mathcal{R}$.

Proof. The set of frational ideals forms a monoid under multiplication. Closure follows Proposition 7.3. Associativity follows from the associativity of $\mathcal{R}$, and $\mathcal{R}$ acts as the identity.

Let $\mathcal{M}$ be a maximal ideal of $\mathcal{R}$. Then $\mathcal{M} \neq (0)$, since $\mathcal{R}$ is not a field. Put

$$\mathcal{M}' = \{x \in \mathcal{K} | x\mathcal{M} \subseteq \mathcal{R}\}.$$

Note that $\mathcal{M}'$ is an $\mathcal{R}$-submodule of $\mathcal{K}$ and is a fractional ideal of $\mathcal{R}$. We need to show that $\mathcal{M}\mathcal{M}' = \mathcal{R}$. From the definition of $\mathcal{M}'$, it must be that $\mathcal{M}\mathcal{M}' \subseteq \mathcal{R}$. As $\mathcal{M}$ is a maximal ideal, $\mathcal{M} = \mathcal{R}\mathcal{M} \subseteq \mathcal{M}'\mathcal{M} \subseteq \mathcal{R}$

we get that either $\mathcal{M}\mathcal{M}' = \mathcal{M}$ or $\mathcal{M}\mathcal{M}' = \mathcal{R}$. It suffices to show that $\mathcal{M}\mathcal{M}' \neq \mathcal{M}$.

For the sake of contradiction, suppose $\mathcal{M}'\mathcal{M} = \mathcal{M}$. Then for any $x \in \mathcal{M}'$ we have $x\mathcal{M} \subseteq \mathcal{M}$, $x^2\mathcal{M} \subseteq x\mathcal{M} \subseteq \mathcal{M}$. Inductively, $x^n\mathcal{M} \subseteq \mathcal{M}$ for all $n \in \mathbb{N}$. Hence any non-zero element $d \in \mathcal{M}$ acts as a common denominator for all powers x^n of $x, n \in \mathbb{N}$. It follows that $\mathcal{R}[x]$ is a fractional ideal of $\mathcal{M}$. Since $\mathcal{R}$ is Noetherian, $\mathcal{R}[x]$ is a $\mathcal{R}$-module of finite type, so x is integral over $\mathcal{R}$. But $\mathcal{R}$ is integrally closed, therefore $x \in \mathcal{R}$ and hence $\mathcal{M}'\mathcal{M} = \mathcal{M} \Rightarrow \mathcal{M}' = \mathcal{R}$. It suffices to show that $\mathcal{M}'$ is never equal to $\mathcal{R}$.

Let $0 \neq a \in \mathcal{M}$. The ideal $\mathcal{R}a$ contains a product $p_1p_2\cdots p_n$ of non-zero prime ideals. Let n be as small as possible. Note that $\mathcal{M} \supseteq \mathcal{R}a \supset p_1p_2\cdots p_n$, so there exists $i \in \{1, \cdots, n\}$ such that $\mathcal{M} \supseteq p_i$. Since p_i is prime, it is also maximal ($\mathcal{R}$ is a Dedekind domain) we get that $\mathcal{M} = p_i$. Therefore, $\mathcal{R}a \supseteq p_i \prod_{j\neq i} p_j$ and $\mathcal{R} \supsetneq \prod_{j\neq i} p_j$, since our n was minimal. Hence, there exists a $b \in \prod_{j\neq i} p_j$ such that $b \notin \mathcal{R}a$. But $\mathcal{M}\prod_{j\neq i} p_j \subseteq \mathcal{R}a$ so $\mathcal{M}b \subseteq \mathcal{R}a$ or $\mathcal{M}ba^{-1} \subseteq \mathcal{R}$. From the definition of $\mathcal{M}'$, it follows that $ba^{-1} \in \mathcal{M}'$. Since $b \notin \mathcal{R}a$, we get $ba^{-1} \notin \mathcal{R}$. Therefore $\mathcal{M}' \neq \mathcal{R}$.

□

Theorem 4. Let $\mathcal{R}$ be a Dedekind domain and let $\mathrm{spec}(\mathcal{R})$ be the set of non-zero prime ideals of $\mathcal{R}$. Then :

1. Every non-zero fractional ideal $\mathfrak{b}$ of $\mathcal{R}$ may be uniquely expressed in the form :
$$\mathfrak{b} = \prod_{\mathfrak{p}\in\mathrm{spec}(\mathcal{R})} \mathfrak{p}^{n_p(\mathfrak{b})},$$
where, for any $\mathfrak{p} \in \mathrm{spec}(\mathcal{R}), n_\mathfrak{p}(\mathfrak{b}) \in \mathbb{Z}$ and for almost all $\mathfrak{p} \in \mathrm{spec}(\mathcal{R}), n_\mathfrak{p}(\mathfrak{b}) = 0$.

2. The monoid of non-zero fractional ideals of $\mathcal{R}$ is a group.

Proof. Let $\mathfrak{b}$ be a non-zero fractional ideal of $\mathcal{R}$. Then by definition there exists a $d \in \mathcal{R} \setminus \{0\}$ such that $d\mathfrak{b} \subseteq \mathcal{R}$, or $d\mathfrak{b}$ is an integral ideal of $\mathcal{R}$. Let Γ be the set of non-zero ideals in $\mathcal{R}$ which are not product of prime ideals. For the sake of contradiction, lets assume $|\Gamma| > 0$. By Zorn's Lemma, there exists $\mathfrak{a}$ be a maximal element of Γ. Since $\mathcal{R}$ is the product of the empty collection of prime ideals, so $\mathfrak{a} = \mathcal{R}$.

Every ideal is contained in a maximal ideal, so let $\mathfrak{a} \subseteq \mathfrak{p}$. Let $\mathfrak{p}'$ be the inverse fractional ideal of $\mathfrak{p}$ in the monoid of fractional ideals of , the existence of which we proved earlier. Now since $\mathfrak{a} \subseteq \mathfrak{p}$, we get $\mathfrak{a}\mathfrak{p}' \subseteq \mathfrak{p}\mathfrak{p}' = \mathcal{R}$. Since $\mathcal{R} \subseteq \mathfrak{p}'$, $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}'$. □

Chapter 2

Ideal Classes and the Unit Theorem

2.1 Preliminaries concerning discrete subgroups of $\mathbb{R}^n$

Definition 7 (Discrete Subgroup of $\mathbb{R}^n$)**.** A subgroup H of $\mathbb{R}^n$ is discrete if and only if, for any compact subset K of $\mathbb{R}^n$, the intersection $H \cap K$ is finite.

Theorem 5. Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is generated over $\mathbb{Z}$ by r vectors $e_1, \ldots, e_r$ which are linearly independent over $\mathbb{R}$.

Proof. Choose $\mathbf{e} = e_1, \ldots, e_r$ in H such that they are $\mathbb{R}$-linearly independent and r is maximal. Define $\mathscr{P}$ as follows :

$$\mathscr{P} := \left\{ \sum_{i=1}^{r} \alpha_i e_i | \alpha_i \in [0,1] \right\},$$

The set $\mathscr{P}$ is called the fundamental pallelogram of H with respect to the basis $e_1, \ldots, e_r$. We can immediately see that $\mathscr{P}$ is compact because it is homeomorphic to $\mathbb{R}^n$. Let $x \in H$. Then we can write x in the form :

$$x = \sum_{i=1}^{r} \lambda_i e_i,$$

for $\lambda_i \in \mathbb{R}$. If x cannot be written in this form, we can add x to $\{e_1, \ldots, e_r\}$, contradicting the maximality of r. Now for $j \in \mathbb{Z}$, let :

$$x_j := jx - \sum_{i=1}^{r} \lfloor \lambda_i j \rfloor e_j = \sum_{i=1}^{r} (\lambda_i j - \lfloor \lambda_i j \rfloor) e_i. \qquad (j \in \mathbb{Z})$$

Hence, $x_j \in \mathscr{P}$. It follows that $x_j \in \mathscr{P} \cap H$. Since H is discrete, $\mathscr{P} \cap H$

is finite since $\mathscr{P}$ is compact. For $j = 1$, we have :

$$x = x_1 + \sum_{i=1}^{r} \lfloor \lambda_i \rfloor e_i.$$

So x is in the $\mathbb{Z}$ span of a finite set. Hence, H is finitely generated over $\mathbb{Z}$. Since $\mathscr{P} \cap H$ is finite, there exist $j \neq k$ such that $x_j = x_k$. It follows that :

$$\sum_{i=1}^{r} \lambda_i (j-k) e_i = \sum_{i=1}^{r} (\lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor) e_i.$$

Linear independence of $\{e_i\}$ gives us :

$$\lambda_i (j-k) = \lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor.$$

Hence $\lambda_i \in \mathbb{Q}$ for all i. So far we've shown that for any $x \in \mathscr{P} \cap H$, $x = \sum_{i=1}^{r} \lambda_i e_i$ where $\lambda_i \in \mathbb{Q}$ for all i. Let d be the least common multiple of the denominators of λ_i's. Then for any $x \in H$, we know :

$$x = x_1 + \sum_{i=1}^{r} \lfloor \lambda_i \rfloor e_i \in \frac{1}{d} \sum_{i=1}^{r} \mathbb{Z} e_i.$$

We conclude that : $H \subseteq \frac{1}{d} \sum_{i=1}^{r} \mathbb{Z} e_i \Rightarrow \sum_{i=1}^{r} \mathbb{Z} e_i \subseteq H \subseteq \frac{1}{d} \mathbb{Z} e_i$. Therefore we must have that H is finitely generated of rank r over $\mathbb{Z}$ on some linear combination of the vectors $\{\frac{1}{d} e_i\}$. This basis is linearly independent over $\mathbb{R}$ as desired. □

Definition 8 (Lattice). A discrete subgroup of rank n of $\mathbb{R}^n$ is called a lattice in $\mathbb{R}^n$.

By Theorem 1, a lattice is generated over $\mathbb{Z}$ by a base of $\mathbb{R}^n$, wich is then a $\mathbb{Z}$-base for the given lattic. For each $\mathbb{Z}$-base $e = (e_1, \ldots, e_n)$ of a lattice H we shall write $\mathscr{P}_e$ for the half open parallelotope :

$$\mathscr{P}_e = \left\{ x \in \mathbb{R}^n | x = \sum_{i=1}^{n} \alpha_i e_i, \alpha_i \in [0,1) \right\}$$

Thus every point of $\mathbb{R}^n$ is congruent modulo H to one and only one point of P_e for any fixed e (we say, in this case, that P_e is a fundamental domain for H). We shall write μ to denote the Lebesgue measure in $\mathbb{R}^n$, i.e. if S is a measurable subset of $\mathbb{R}^n$, $\mu(S)$ will stand for its measure (which we will also call its volume).

Lemma 6. The volume $\mu(\mathscr{P}_e)$ is independent of the base e chosen for H.

Proof. Let $f = (f_1, \dots, f_n)$ be another base for H. Then :

$$f_i = \sum_{j=1}^{n} \alpha_i j e_j. \qquad (\alpha_{ij} \in \mathbb{Z})$$

By calculus we know that $\mu(\mathscr{P}_f) = |\det(\alpha_{ij})|\mu(\mathscr{P}_e)$. The change of bases matrix $(\alpha_{ij}) \in GL_n(\mathbb{Z})$, so $\det(\alpha_{ij}) = \pm 1$. Hence, $\mu(\mathscr{P}_f) = \mu(\mathscr{P}_e)$. ☐

Definition 9 (Volume of a Lattice). The volume of the parallelotope $\mathscr{P}_e$ associated with any base e of H is called the volume of the lattice H and is denoted by $\mathrm{vol}(H)$.

Theorem 6 (Minkowski). Let H be a lattice in $\mathbb{R}^n$ and let S be a measurable subset of $\mathbb{R}^n$ such that $\mu(S) > \mathrm{vol}(H)$. Then there exist two distinct points $x, y \in S$ such that $x - y \in H$.

Proof. Consider the sets $S_x = S \cap (x + \mathscr{P}_e)$, where $x \in H$. Notice that these sets form a partition of S, i.e. they are pairwise disjoint and :

$$S = \cup_{x \in H} S_x.$$

In particular we have :

$$\mathrm{vol}(S) = \sum_{x \in H} \mathrm{vol}(S_x).$$

Notice that the translated sets $S_x - x = (S - x) \cap \mathscr{P}_e$ are all contained in $\mathscr{P}_e$. We want to prove that the S_x cannot be all mutually disjoint. Since $\mathrm{vol}(S_x) = \mathrm{vol}(S_x - x)$, we have :

$$\mathrm{vol}(H) < \mathrm{vol}(S) = \sum_{x \in H} \mathrm{vol}(S_x) = \sum_{x \in H} \mathrm{vol}(S_x - x).$$

The facts that $S_x - x \subseteq \mathscr{P}_e$ and $\sum_{x \in H} \mathrm{vol}(S_x - x) > \mathrm{vol}(H)$ imply that these sets cannot be disjoint, i.e. there exist two distinct vectors $x \neq y \in H$ such that $(S_x - x) \cap (S_y - y) \neq 0$. Let z be any vector in the (non-empty) intersection $(S_x - x) \cap (S_y - y)$ and define :

$$\begin{aligned} z_1 &= z + x \in S_x \subseteq S \\ z_2 &= z + y \in S_y \subseteq S. \end{aligned}$$

These two vectors satisfy $z_1 - z_2 = x - y \in H$. ☐

Theorem 7 (Minkowski's convex body theorem). Let H be a full-dimensional lattice in $\mathbb{R}^n$ and let $C \subseteq \mathbb{R}^n$ be a convex set symmetric about the origin $(i.e. x \in C \Rightarrow -x \in C)$. Suppose that either :

1. $\mathrm{vol}(C) > \cdot 2^n \cdot \mathrm{vol}(H)$, or

2. $\mathrm{vol}(C) \geq \cdot 2^n \cdot \mathrm{vol}(H)$ and C is compact.

Then $\mathbb{C} \cap (H \setminus \{0\}) \neq \varnothing$.

Proof. It is easy to see that the volume of the set $\frac{1}{2}C = \{x/2 : x \in C\}$ is $2^{-m}\,\mathrm{vol}(C)$, and therefore, we can apply previous theorem to find $\frac{1}{2}x_0, \frac{1}{2}x_1 \in \frac{1}{2}C$ such that $z = \frac{1}{2}x_1 - \frac{1}{2}x_0 \in H$. Clearly $z = \frac{1}{2}x_1 + \frac{1}{2}(-x_0) \in C$, since C is convex and symmetric. □

2.2 The canonical imbedding of a number field

Definition 10 (Canonical imbedding of a number field)**.** Let K be a number field and let n be its degree. There are n distinct isomorphisms $\sigma_i : K \to C$. There are exactly n, because the minimal polynomial for a primitive element of K ove $\mathbb{Q}$ has only n roots in $\mathbb{C}$. Let $\alpha : \mathbb{C} \to \mathbb{C}$ be complex conjugation. Then, for any $i = 1, \ldots, n$, we have : $\alpha\sigma_i = \sigma_j$ if and only if $\sigma_i(K) \subseteq \mathbb{R}$. We write r_1 for the number of indices such that $\sigma_i(K) \subseteq \mathbb{R}$. Then $n - r$ is an even number, so we may write :

$$r_1 + 2r_2 = n$$

Let us renumber the σ_i's so that $\sigma_i(K) \subseteq \mathbb{R}$ for $1 \leq i \leq r_1$ and so that $\sigma_{i+r_2}(x) = \overline{\sigma_j(x)}$ for $r_1+1 \leq j \leq r_1+r_2$. Then the first r_1+r_2 isomorphisms determine the last r_2. For $x \in K$, we define :

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma(x_{r_1+r_2})) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

We call σ the canonical imbedding of K in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$; it is an injective ring homomorphism. We shall frequently identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$.

Proposition 8. If M is a free $\mathbb{Z}$-submodule of K of rank n and if $(x_i)_{1\leq i\leq n}$ is a $\mathbb{Z}$-base for M then $\sigma(M)$ is a lattice in $\mathbb{R}^n$, whose volume is :

$$\mathrm{vol}(\sigma(M)) = 2^{-r_2}|\det_{1\leq i,j\leq n}(\sigma_i(x_j))|.$$

Proof. For fixed i the coordinates of $\sigma(x_i)$ with respect to the canonical base of $\mathbb{R}^n$ are :

$$\langle \sigma_1(x_i), \ldots, \sigma_{r_1}(x_i), \Re(\sigma_{r_1+1}(x_i)), \Im(\sigma_{r_1+1}(x_i)), \ldots, \Re(\sigma_{r_1+r_2}(x_i)), \Im(\sigma_{r_1+r_2}(x_i)) \rangle$$

We calculate the determinant D of the matrix whose ith column is given as above. We know that $\Re(z) = \frac{1}{2}(z+\bar{z})$ and $\Im(z) = \frac{1}{2i}(z-\bar{z})$ for $z \in \mathbb{C}$. We obtain $D = (2i)^{-r_2}\det(\sigma_j(x_i))$. We apply the transformation $R_i \mapsto iR_{i+1}$ for $i = r_1, r_1+2, \ldots, r_1+2r_n$. So we end up with the determinant $D = (2i)^{-r_2}\det_{1\leq i,j\leq n}(\sigma_j(x_i))$. Since x_i's form a base for K over $\mathbb{Q}$, $\det_{1\leq i,j\leq n}(\sigma_j(x_i)) \neq 0$ and therefore $D \neq 0$. Thus the vectors $\sigma(x_i)$ are linearly independent in $\mathbb{R}^n$, so that the $\mathbb{Z}$-module they generate (call it $\sigma(M)$) is a lattice in $\mathbb{R}^n$. So we get

$$\mathrm{vol}(\sigma(M)) = |(2i)^{-r_2}\det(\sigma_j(x_i))| = 2^{-r_2}|\det(\sigma_j(x_i))|$$

as required. $\square$

Proposition 9. Let d be the absolute discriminant of K, let A be the ring of integers in K, and let $\mathfrak{a}$ be a non-zero integral ideal of A. Then $\sigma(A)$ and $\sigma(\mathfrak{a})$ are lattices. Moreover,

$$\mathrm{vol}(\sigma(A)) = 2^{-r_2}|d|^{\frac{1}{2}} \quad \text{and} \quad \mathrm{vol}(\sigma(\mathfrak{a})) = 2^{-r_2}|d|^{\frac{1}{2}}N(\mathfrak{a}).$$

Proof. We know that A and $\mathfrak{a}$ are free $\mathbb{Z}$-modules of rank n, so we may apply the previous proposition. On the other hand, if (x_i) is a $\mathbb{Z}$-base for A, then $d = \det_{1\le i,j\le n}(\sigma_i(x_j))^2$. This proves the first result. The second formula follows from the first and the observation that $\sigma(\mathfrak{a})$ is a subgroup of $\sigma(A)$ of index $N(\mathfrak{a})$. A fundamental domain for $\sigma(\mathfrak{a})$ may obviously constructed as the disjoint union of $N(\mathfrak{a})$ copies of a fundamental domain for $\sigma(A)$. $\square$

2.3 Finiteness of the ideal class group

Proposition 10. Let $r_1, r_2 \in \mathbb{N}$ such that $n = r_1 + 2r_2$, $t \in \mathbb{R}$ and let $B(r_1, r_2, t)$ be the set of all elements $(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ such that :

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \le t.$$

Let μ denote the Lebesgue measure in $\mathbb{R}^n$. Then,

$$\mu(B(r_1, r_2, t)) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} \qquad \text{(for any } t \ge 0.)$$

Proof. We induct on n. The two base cases : $r_1 = 1, r_2 = 0$ and $r_1 = 0$ and $r_2 = 1$. In the former $B(1,0,t) = \{x \in \mathbb{R} : |x| \le t\}$ has volume $2t = \frac{2^1}{1!}\left(\frac{\pi}{2}\right)^0 t^1$. In the latter case, $B(0,1,t) = \{y \in \mathbb{C} : 2|y| \le t\}$ which has volume $\pi(t/2)^2 = \frac{2^0}{2!}\left(\frac{\pi}{2}\right)^1 t^2$.

To go from $n-1 \to n$, we could either fix r_2 and increment r_1 or we could fix r_1 and increment r_2. In the both cases, we assume the formula is true for $n-1 = r_1+2r_2$. Now for n, the volume in the first case $r_1 \mapsto r_1+1$ fixing r_2 is :

$$\begin{aligned}
\mu(B(r_1+1,r_2,t)) &= \int_{-t}^{t} B(r_1,r_2,t-|x|)\mathrm{d}x \\
&= \int_{-t}^{0} B(r_1,r_2,t+x)\mathrm{d}x + \int_{0}^{t} B(r_1,r_2,t-x)\mathrm{d}x \\
&= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{1}{(n-1)!}\left[\int_{-t}^{0}(t+x)^{n-1}\mathrm{d}x + \int_{0}^{t}(t-x)^{n-1}\mathrm{d}x\right] \\
&= 2^{r_1+1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}
\end{aligned}$$

The volume in the second case $r_2 \mapsto r_2+1$ fixing r_1 is :

$$\begin{aligned}
\mu(B(r_1,r_2+1,t)) &= \int_{\{0\le|z|\le t/2\}} B(r_1,r_2,t-2|x|)\mathrm{d}x \\
&= \frac{2^{r_1}}{(n-2)!}\left(\frac{\pi}{2}\right)^{r_2}\int_{0}^{t/2}\int_{0}^{2\pi} x(t-2x)^{n-1}\mathrm{d}\theta\mathrm{d}x \\
&= \frac{2^{r_1}}{(n-2)!}\left(\frac{\pi}{2}\right)^{r_2}\cdot 2\pi\int_{0}^{t/2} x(t-2x)^{n-2}\mathrm{d}x \\
&= \frac{2^{r_1}}{(n-2)!}\left(\frac{\pi}{2}\right)^{r_2}\cdot 2\pi\frac{t^n}{n(n-1)} = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\frac{t^n}{n!}
\end{aligned}$$

Therefore the formula holds for all n. □

Proposition 11. Let K be a number field, n its degree, r_1 and r_2 are integers defined earlier, d the absolute discriminant of K, and $\mathfrak{a}$ a non-zero integral ideal of K. Then $\mathfrak{a}$ contains a non-zero element x such that :

$$|N_{K/\mathbb{Q}}(x)| \le \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d|^{\frac{1}{2}}N(\mathfrak{a}).$$

Proof. Choose t such that $\mu(B(r_1,r_2,t)) = 2^n\,\mathrm{vol}(\sigma(\mathfrak{a}))$. So,

$$2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} = 2^{n-r_2}|d|^{\frac{1}{2}} \implies t^n = 2^{n-r_1}\pi^{-r_2}n!|d|^{\frac{1}{2}}N(\mathfrak{a}) \qquad ((\star))$$

Since $B(r_1,r_2,t)$ is symmetric, convex and compact, there exists a nonzero $x \in \mathfrak{a}\cap B(r_1,r_2,t)$. By virtue of being in $B(r_1,r_2,t)$, this element satisfies :

$$\sum_{i=1}^{n}|\sigma_i(x)| \le t.$$

Combining this with the inequality of geometric and arithmetic means, we have :

$$|N(x)| = \left|\prod_{i=1}^{n}\sigma_i(x)\right| = \left(\frac{\sum_{i=1}^{n}|\sigma_i(x)|}{n}\right)^n\frac{t^n}{n!}.$$

Using $(\star)$, we get the desired inequality :

$$N(x) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{\frac{1}{2}} N(\mathfrak{a}).$$

$\square$