Lecture Notes to a Course on Algebraic Number Theory

Taught by Prof. Uri Shapira at Technion IIT during Spring 2022

Typed by Elad Tzorani

April 10, 2022

Course Information

The course will be based on lecture notes by Ehud De Shalit on algebraic number theory, and partially on Milne's text on algebraic number theory (henceforward, ANT).

Prerequisites

The course will assume undergraduate knowledge in ring theory and Galois theory.

1 Notations & Conventions

- All rings are assumed to be commutative and unital, unless mentioned otherwise.
- The rings of integers, reals and complex numbers are respectively denoted $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$.
- For $n \in \mathbb{Z}_+$ we denote $[n] = \{1, \ldots, n\}$.
- We denote by K an algebraic number field and by n its degree $\deg_{\mathbb{Q}}(K)$ over $\mathbb{Q}$, when none of these are specified.

2 A Short Review on Rings

Definition 2.1 (Euclidean Ring)**.** Let R be a ring. We say R is *Euclidean* if there is a map $N\colon R \to \mathbb{Z}_+$ that satisfies the following properties.

(i) *Sub-multiplicativity:* $N(a) = 0$ if and only if $a = 0$, and

$$N(\alpha\beta) \leq N(\alpha) N(\beta).$$

(ii) For all $\alpha, \beta \in R$ such that $\alpha \neq 0$, there are $q, r \in R$ such that

$$\beta = q\alpha + r, \quad N(r) < N(\alpha).$$

Such a map is called the *Euclidean norm* of R.

Definition 2.2 (Group of Units in a Ring)**.** Let R be a ring. The *group of units* in R is

$$R^\times := \{\alpha \in R \mid \exists \beta \in R\colon \alpha\beta = 1\}.$$

Definition 2.3 (Associate Elements)**.** Let R be a ring and let $\alpha, \beta \in R$. We say that α, β are *associates*, and denote $\alpha \sim \beta$, if there's $\varepsilon \in R^\times$ such that $\alpha = \varepsilon\beta$.

Definition 2.4 (Reducible Element)**.** Let R be a ring and let $\alpha \in R \setminus \{0\}$. We say that α is *reducible* if there are $\beta, \gamma \in R \setminus R^\times$ such that $\alpha = \beta \cdot \gamma$.

Remark 2.5. The subset of reducible elements of R is $R^\times \cdot R^\times$.

Definition 2.6 (Irreducible Element)**.** Let R be a ring. An element $\alpha \in R$ is *irreducible* if it isn't reducible.

Definition 2.7 (Prime Elements)**.** Let R be a ring and let $\alpha \in R \setminus (R^\times \cup \{0\})$. We say that α is *prime* if for $\beta, \gamma \in R$ such that $\alpha \mid \beta \cdot \gamma$ one has either $\alpha \mid \beta$ or $\alpha \mid \gamma$.

Definition 2.8 (Ideal in a Ring)**.** Let R be a ring. An *ideal* of R is a strict non-zero subset $I \subseteq R$ that is an additive subgroup and such that $aI, Ia \subseteq I$ for all $a \in R$.

Notation 2.9. Let R be a ring. We denote $I \leq R$ to say that I is an ideal of R.

Definition 2.10 (Prime Ideal)**.** Let R be a ring and let $I \leq R$. We say that I is *prime* if whenever $\beta, \gamma \in R$ are such that $\beta \cdot \gamma \in I$, one has $\beta \in I$ or $\gamma \in I$.

Definition 2.11 (Principal Ideal)**.** Let R be a ring and let $\alpha \in R$. We denote

$$(\alpha) \coloneqq \alpha \cdot R = \{\alpha \cdot \beta \mid \beta \in R\}.$$

Ideals of this form are called *principal ideals.*

Definition 2.12. Let R be a ring. We say that R is a *principal ideal domain (PID)* if any ideal of R is principal.

Theorem 2.13. *Any Euclidean domain is PID.*

Lemma 2.14. *Let R be a ring and let $\alpha \in R$. Then α is prime if and only if (α) is a prime ideal.*

Lemma 2.15. *Let R be a ring. Prime elements of R are irreducible.*

Exercise 2.1. Let R be a ring and let $I \leq R$. Then I is prime if and only if R/I is an integral domain.

Exercise 2.2. Let R be a ring. An ideal $I \leq R$ is maximal if and only if R/I is a field.

Corollary 2.16. *Maximal ideals are prime.*

Exercise 2.3. Let R be a ring and let $\alpha \in R$. Then α is irreducible if and only if (α) is maximal among principal ideals.

Definition 2.17 (Unique Factorization Domain)**.** Let R be a ring. We say that R is a *unique factorization domain (UFD)* if any $\alpha \in R$ can be written as $\alpha = \beta_1 \cdot \ldots \cdot \beta_k$ where $\beta_i \in R$ are irreducible, and if $\beta_1 \cdot \ldots \cdot \beta_k = \gamma_1 \cdot \ldots \cdot \gamma_\ell$ are two products of irreducible elements of R, then $\ell = k$ and there is a bijection $\sigma \colon [k] \to [k]$ such that $\beta_i \sim \gamma_{\sigma(i)}$.

Corollary 2.18. *Let R be a PID or a UFD. Any irreducible ideal of R is prime.*

Exercise 2.4. A PID is also a UFD.

Example 2.19. Consider the ring $R \coloneqq \mathbb{Z}\left[\sqrt{-5}\right]$. We can write

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$$

which are two possible decompositions of 6 in $\mathbb{Z}\left[\sqrt{-5}\right]$. We claim that $2, 3, \left(1 + \sqrt{-5}\right), \left(1 + \sqrt{-5}\right)$ are all irreducible and non-associates, which implies that $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD.

On R we have a multiplicative *norm* map (that doesn't make it an Euclidean domain)

$$\begin{aligned} N\colon \mathbb{Z}\left[\sqrt{-5}\right] &\to \mathbb{Z} \\ a+b\sqrt{-5} &\mapsto \left(a+b\sqrt{-5}\right)\left(a-b\sqrt{-5}\right)=a^2+5b^2. \end{aligned}$$

One can use N to check that $2,3,\left(1+\sqrt{-5}\right),\left(1+\sqrt{-5}\right)$ are irreducible and non-associates.

Exercise 2.5. Use N to check that $2,3,\left(1+\sqrt{-5}\right),\left(1+\sqrt{-5}\right)$ are irreducible and non-associates.

3 Preliminaries to Algebraic Number Theory

3.1 Definition and Motivation

ANT is the study of finite field extensions of $\mathbb{Q}$ and their rings of integers. ANT is used in solving and analysis of questions about integers.

Definition 3.1 (Number Field)**.** A field K is called a *number field* if $\mathbb{Q}\subseteq K$ and

$$[K:\mathbb{Q}]\coloneqq \deg\left(K/\mathbb{Q}\right)<\infty.$$

Definition 3.2 (p-Adic Valuation)**.** Let $n\in\mathbb{Z}$ and let $p\in\mathbb{Z}$ be a prime. For $n\neq 0$, we denote by $v_p(n)$ the power in which p appears in the decomposition of n into primes; we denote also $v_p(0)=\infty$. We call $v_p\colon\mathbb{Z}\to\mathbb{Z}\cup\{\infty\}$ the *p-adic valuation.*

Theorem 3.3 (Fermat)**.** *An integer $n\in\mathbb{Z}$ is a sum of two squares if and only if for any $q\in\mathbb{Z}$ satisfying $q\equiv 3\pmod 4$ one has $v_q(n)\in 2\mathbb{Z}$.*

Proof. Consider the ring $R=\mathbb{Z}[i]$ of *Gaussian integers* and the *norm*

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{Z} \\ a+bi &\mapsto (a+bi)(a-bi)=a^2+b^2. \end{aligned}$$

- We first claim that R is an Euclidean domain. We show this by showing that N is an Euclidean norm. Let $\alpha,\beta\in R$ with $\alpha\neq 0$. We want to find $q,r\in\mathbb{Z}[i]$ such that $N(r)<N(\alpha)$ and $\beta=q\alpha+r$. Write $\beta=\beta/\alpha\cdot\alpha$ in $\mathbb{Q}[i]=\operatorname{Frac}(R)$. For any $q\in\mathbb{Z}[i]$ we can write

$$\begin{aligned} \beta &= \alpha+\frac{\beta}{\alpha}\cdot\alpha-q\cdot\alpha \\ &= q\cdot\alpha+\alpha\left(\frac{\beta}{\alpha}-q\right). \end{aligned}$$

Extend $N\colon \mathbb{Q}(i) \to \mathbb{Q}$ via $N(a+bi) = a^2 + b^2$. We show that there's $q \in \mathbb{Z}[i]$ such that $N(\beta/\alpha - q) < 1$, from which $N(\alpha(\beta/\alpha - q)) < N(\alpha)$ by sub-multiplicativity, as required. Indeed, each point of $\mathbb{C}$ is within distance at most 1 from the lattice $\mathbb{Z}[i]$.[1]

- We now show that

$$\begin{aligned}\mathbb{Z}[i]^{\times} &= \{\alpha \in \mathbb{Z}[i] \mid N(\alpha \in \{\pm 1\})\} \\ &= \{\pm 1, \pm i\}.\end{aligned}$$

  Let $\alpha \in R$. If $N(\alpha) = \alpha\bar{\alpha} = 1$, we get that $\alpha \in \mathbb{Z}[i]^{\times}$. On the other hand, if $\alpha \cdot \beta = 1$, we get

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$$

  so $N(\alpha) \in \mathbb{Z}^{\times}$ so $N(\alpha) \in \{\pm 1\}$. [2]

- We want to understand

$$\mathrm{im}(N) = \{N(z) = z\bar{z} \mid z \in \mathbb{Z}\} = \left\{a^2 + b^2 \;\middle|\; a, b \in \mathbb{Z}\right\}.$$

  - Let p be a *rational prime* (i.e. prime in $\mathbb{Z}$. We have

$$\begin{aligned}\mathbb{Z}[i]/(p) &\cong \mathbb{Z}[x]/\left(x^2+1, p\right) \\ &\cong \mathbb{F}_p[x]\end{aligned}$$

    so p remains a prime in $\mathbb{Z}[i]$ if and only if -1 is not a square in $\mathbb{F}_p$.
  - We claim that -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$. From this and the above calculation we get that p remains a prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$.
    Consider

$$\begin{aligned}\varphi\colon \mathbb{F}_p^{\times} &\to \mathbb{F}_p^{\times} \\ \alpha &\mapsto \alpha^2.\end{aligned}$$

    We have $\ker(\varphi) = \{\pm 1\}$, so by the isomorphism theorem $\mathrm{im}(\varphi)$ is a subgroup of $\mathbb{F}_p^{\times}$ of size $\#\mathbb{F}_p / \#\{\pm 1\} = \frac{p-1}{2}$. We get that

[1] We say that the *covering radius* of $\mathbb{Z}[i] \subseteq \mathbb{C}$ is $\sqrt{2}/2$, since this is the smallest number for which any ball in $\mathbb{C}$ of radius r contains a point of $\mathbb{Z}](i)$.

[2] Note that in our case, $N(\alpha) \geq 0$ so it follows that $N(\alpha) = 1$. The statement is more general when one requires $N(\alpha) \in \{\pm 1\}$ instead.

$-1 \in \operatorname{im}(\varphi)$ if and only if $\ker(\varphi)|_{\operatorname{im}(\varphi)} \neq \{1\}$. Now, $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ and $\operatorname{im}(\varphi) \subseteq \mathbb{F}_p^\times$ is another cyclic group of size $\frac{p-1}{2}$; hence this is the case when 2 and $\frac{p-1}{2}$ are coprime, or equivalently $p \equiv 1 \pmod 4$.

- Note that $2 = (1+i)(1-i)$, where $1 \pm i$ are irreducible because $N(1+i)$ is prime in $\mathbb{Z}$. Hence this is a decomposition of 2 into a product of irreducible elements and in particular 2 isn't prime in $\mathbb{Z}[i]$. (**Exercise:** Write formally why $1 \pm i$ are irreducible elements of $\mathbb{Z}[i]$.)
- If $p \equiv 1 \pmod 4$ is a rational prime, we claim that there's an irreducible element $\pi \in \mathbb{Z}[i]$ for which $p = \pi\bar{\pi}$ and $N(\pi) = p$.

  To show this, write $p = \pi\lambda$ for π irreducible and λ non-unit. We get

  $$\begin{aligned} p^2 &= N(p) \\ &= N(\pi) \cdot N(\lambda) \\ &= \pi\bar{\pi} \cdot \lambda\bar{\lambda}. \end{aligned}$$

  Since λ is a non-unit, we get $\lambda\bar{\lambda} \neq 1$, so $\lambda\bar{\lambda} \in \{p, p^2\}$. Similarly, $\pi\bar{\pi} \in \{p, p^2\}$, hence $\pi\bar{\pi} = \lambda\bar{\lambda} = p$, as required.
- We claim that if $\pi \in \mathbb{Z}[i]$ is an irreducible element other than $1 \pm i$ and not in $\mathbb{Z}$, then $pcoloneqq\pi\bar{\pi}$ is a rational prime with $p \equiv 1 \pmod 4$.

  Indeed, consider $p \coloneqq N(\pi) = \pi\bar{\pi}$ is a product of rational primes. By the uniqueness of the decomposition it follows that $p \equiv 1 \pmod 4$ is a rational prime.

In conclusion, taking $z \in \mathbb{Z}[i]$ we can write

$$z = \varepsilon (1+i)^r \left(\prod_{i \in [k]} \pi_i^{m_i} \right) \left(\prod_{j \in [\ell]} q_j^{n_j} \right)$$

for $\varepsilon \in \mathbb{Z}[i]$ a unit, π_i primes in $\mathbb{Z}[i]$ of norms p_i which are rational primes with $p_i \equiv 1 \pmod 4$, and q_j are rational primes with $q_j \equiv 3 \pmod 4$. We get that

$$N(z) = 2^r \left(\prod_{i \in [k]} p_i^{m_i} \right) \left(\prod_{j \in [\ell]} q_j^{2m_j} \right).$$

From here one gets the result.

$\square$

3.2 Field Embeddings

Definition 3.4 (Field Embedding)**.** Let K, L be two fields. Field homomorphisms $\sigma\colon K \to L$ are called *field embeddings.* The collection of such embeddings is denoted $\operatorname{Emb}(K, L)$.

Definition 3.5 (Real & Complex Embeddings)**.** An embedding $\sigma \in \operatorname{Emb}(K, \mathbb{C})$ is called *real* if $\sigma(K) \subseteq \mathbb{R}$. It is called *complex* otherwise.

Theorem 3.6. *Let K be a degree n number field. There are exactly n distinct embeddings $\sigma_i\colon K \to \mathbb{C}$.*

Corollary 3.7. *Let K be an algebraic number field of degree n. There are $r_1, r_2 \in \mathbb{Z}$ non-negative with r_1 real embeddings and $2r_2$ complex embeddings which are divided into pairs of the form $\sigma, \bar{\sigma}$. We have $n = r_1 + 2r_2$.*

We fix an ordering of $\operatorname{Emb}(K, \mathbb{C})$*:*

$$\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \dots, \sigma_{r_1+2r_2}$$

such that $\sigma_{r_1+1}, \dots, \sigma_{r_1}$ are real embeddings, $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ are non-conjugate complex embeddings, and for all $i \in [r_2]$ one has $\bar{\sigma}_{r_1+r_2+j} = \sigma_{r_1+j}$.

Definition 3.8 (Geometric Embedding of a Field into $\mathbb{R}^n$)**.** Let K be an algebraic number field of degree n. Let r_1, r_2 be as in the above corollary. We define a $\mathbb{Q}$-linear map

$$\begin{aligned}\varphi\colon K &\to \mathbb{R}^n \cong \mathbb{R}^{r_1} \times \left(\mathbb{R}^2\right)^{r_2} \\ \alpha &\mapsto \left(\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_{r_1}(\alpha), \Re\left(\sigma_{r_1+1}(\alpha)\right), \Im\left(\sigma_{r_1+1}(\alpha)\right), \dots, \Re\left(\sigma_{r_1+r_2}(\alpha)\right), \Im\left(\sigma_{r_1+r_2}(\alpha)\right)\right).\end{aligned}$$

This is called the *geometric embedding of K into* $\mathbb{R}^n$.

Proposition 3.9. *Let K be an algebraic number field of degree n, and let φ be as above. Then $\varphi(K)$ contains an $\mathbb{R}$-basis of $\mathbb{R}^n$.*

4 Full Modules & Lattices

4.1 Full Modules

Definition 4.1 (Full Module)**.** A $\mathbb{Z}$-module $\Lambda \subseteq K$ in a field K is called a *full module* of K if it is a finitely-generated $\mathbb{Q}$-module and also $\operatorname{Span}_{\mathbb{Q}}(\Lambda) = K$.

Example 4.2. Taking $K = \mathbb{Q}$, there is a full module $\mathbb{Z} \subseteq K$.

Example 4.3. Taking $K = \mathbb{Q}$, the subset $\mathbb{Z}\left[\frac{1}{2}\right]$ isn't a full module of K because it is *not* finitely generated.

Example 4.4. If $\alpha \in K$ is the root of a monic degree-n irreducible polynomial,

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

for $a_i \in \mathbb{Z}$, we get that $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of $K/\mathbb{Q}$. Then $\Lambda = \mathbb{Z}[\alpha]$ is a full module of K.

Lemma 4.5. *The following are equivalent for a $\mathbb{Z}$-module $\Lambda \subseteq K$.*

1. *Λ is a finitely-generated $\mathbb{Z}$-module such that $\operatorname{Span}_{\mathbb{Q}}(\Lambda) = K$.*
2. *Λ is a finitely-generated $\mathbb{Z}$-module that contains a $\mathbb{Q}$-basis of K.*
3. *$\Lambda = \operatorname{Span}_{\mathbb{Z}}(\alpha_1, \ldots, \alpha_n)$ for some basis $(\alpha_1, \ldots, \alpha_n)$ of $K/\mathbb{Q}$.*

Proof. Clearly, the third condition implies the first two. We show that the second condition implies the third.

By the structure theorem of finitely-generated abelian groups, we have $\Lambda \cong \mathbb{Z}^m$ (as $\mathbb{Z}$-modules) for some $m \in \mathbb{N}_+$ (since there is no torsion in the additive group of K). If $m < n$, we get a contradiction to the assumption that Λ contains a $\mathbb{Q}$-basis of K. If $m > n$, we get a contradiction by the same reasoning. Hence $m = n$ which gives the result. □

Definition 4.6. Let M_1, M_2 be submodules of K. We define

$$M_1 \cdot M_2 := \left\{ \sum_{i \in [\ell]} a_i b_i \;\middle|\; \substack{\ell \in \mathbb{N} \\ a_i \in M_1 \\ b_i \in M_2} \right\}$$

which is the module generated by the products ab for $a \in M_1$ and $b \in M_2$.

Proposition 4.7. *Let $\Lambda_1, \Lambda_2 \subseteq K$ be full modules. Then $\Lambda_1 \cdot \Lambda_2$ is also a full module of K.*

Proof. We have to show that $\Lambda_1 \cdot \Lambda_2$ is a finitely-generated $\mathbb{Z}$-module, which is indeed the case since if $\Lambda_1 = \operatorname{Span}_{\mathbb{Z}}(\alpha_1, \ldots, \alpha_n)$ and $\Lambda_2 = \operatorname{Span}_{\mathbb{Z}}(\beta_1, \ldots, \beta_n)$, then

$$\Lambda_1 \cdot \Lambda_2 = \operatorname{Span}_{\mathbb{Z}}(\alpha_i \beta_j)_{i,j \in [n]}.$$

□

Proposition 4.8. *Let*

$$\Lambda = \mathrm{Span}_{\mathbb{Z}}(\alpha_1, \ldots, \alpha_n) = \mathrm{Span}_{\mathbb{Z}}(\beta_1, \ldots, \beta_n)$$

be a full module in K. Then

$$[\mathrm{id}_{\mathbb{Z}}]^{\vec{\alpha}}_{\vec{\beta}}, [\mathrm{id}_K]^{\vec{\beta}}_{\vec{\alpha}}$$

are inverse $\mathbb{Z}$-matrices and are therefore in $\mathrm{GL}_n(\mathbb{Z})$.

4.2 Lattices

Definition 4.9. An additive subgroup $L \leq \mathbb{R}^n$ is a *lattice* if $L = \mathrm{Span}_{\mathbb{Z}}(v_1, \ldots, v_n)$ for an $\mathbb{R}$-basis $(v_1, \ldots, v_n)$ of $\mathbb{R}^n$.

Remark 4.10. The theorem from the beginning of the class can be restated as saying that the geometric embedding of a full module is a lattice.

Exercise 4.1. Show that the following are equivalent for an additive subgroup $L \leq \mathbb{R}^n$.

1. L is discrete and $\mathrm{Span}_{\mathbb{R}}(L) = \mathbb{R}^n$.
2. L is discrete and contains an $\mathbb{R}$-basis of $\mathbb{R}^n$.
3. $L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \ldots, v_n\}$ for some $\mathbb{R}$-basis $(v_1, \ldots, v_n)$.
4. L is discrete and co-compact.

Hint: The third condition implies the first because L can be seen as $A\mathbb{Z}^n$ for $A = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}$. The second condition implies the third by taking the $\mathbb{R}$-basis in the assumption and using the fact that L is discrete.

Proposition 4.11. *If*

$$L = \mathrm{Span}_{\mathbb{Z}}(v_1, \ldots, v_n) = \mathrm{Span}_{\mathbb{Z}}(w_1, \ldots, w_n)$$

and

$$g := \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}, \quad h := \begin{pmatrix} | & & | \\ w_1 & \cdots & w_n \end{pmatrix}$$

then $h^{-1}g \in \mathrm{GL}_n(\mathbb{Z})$ and in particular $|\det(g)| = |\det(h)|$.

Proof. By the assumption $L := g\mathbb{Z}^n = h\mathbb{Z}^n$, so

$$h^{-1}g\mathbb{Z}^n = \mathbb{Z}^n.$$

Hence $h^{-1}g$ has integral coefficients. Similarly, $\mathbb{Z}^n = g^{-1}h\mathbb{Z}^n$, so $g^{-1}h$ has integral coefficients, hence the result. $\square$

Definition 4.12. Let $L \leq \mathbb{R}^n$ be a lattice in $\mathbb{R}^n$. We define

$$\mathrm{Vol}\left(\mathbb{R}^n/L\right) := \left|\det\left(g\right)\right|$$

where $L = g\mathbb{Z} = \mathrm{Span}_{\mathbb{Z}}\left(v_!, \ldots, v_n\right)$.

Remark 4.13. Note that

$$F_0 := \left\{ \begin{pmatrix} x_1 \\ v_n \end{pmatrix} \in \mathbb{R}^n \;\middle|\; 0 \leq x_i < 1 \right\}$$

and

$$\mathbb{R}^n = \bigsqcup_{\vec{m} \in \mathbb{Z}^n} F_0 + \vec{m},$$

hence $L = g\mathbb{Z}^n$ implies

$$\mathbb{R}^n = g\mathbb{R}^n = \bigcup_{v \in L} gF_0 + v.$$

Definition 4.14. Let $(v_1, \ldots, v_n)$ be a basis of $\mathbb{R}^n$ and let $g = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}$. Then $gF_0 = \left\{ \sum_{i \in [n]} x_i v_i \;\middle|\; 0 \leq x_i < 1 \right\}$ is called the *parallelopiped* spanned by $v_1, \ldots, v_n$.

Definition 4.15. Let $H_1 \leq H_2$ be abelian groups. We say that a subset $F \subseteq H_2$ is a *fundamental domain* for H_1 if

$$H_1 = \bigsqcup_{v \in H_1} \left(F + v\right).$$

Remark 4.16. In the above terminology, the parallelopiped $g \cdot F_0$ is a fundemntal domain for $L = g\mathbb{Z}^n$ in $\mathbb{R}^n$.

Proposition 4.17. *Let $H_1 \leq H_2 \leq H_3$ be abelian groups, let $F_1 \subseteq H_2$ be a fundamental domain for H_1 and let $F_2 \subseteq H_3$ be a fundamental domain for H_2. Then $F_1 + F_2$ is a fundamental domain of H_1 in H_3.*

Proof. By assumption

$$H_2 = \bigsqcup_{v \in H_1} F_1 + v$$
$$H_3 = \bigsqcup_{w \in H_2} F_2 + w.$$

So,

$$\begin{aligned} H_3 &= \bigsqcup_{v \in H_1} \bigsqcup_{f \in F_1} (F_2 + f + v) \\ &= \bigsqcup_{v \in H_1} (F_2 + F_1 + v) \,. \end{aligned}$$

In fact, $\bigsqcup_{f \in F_1} F_2 + f = F_1 + F_2$. $\square$

Exercise 4.2. Let $L \subseteq \mathbb{Z}^2$ be the lattice of points where the sum of standard coordinates is even. Check that a fundamental domain for L cannot be built up as unions of translations of the standard cube.

Corollary 4.18. *If $L_1 \leq L_2 \leq \mathbb{R}$ are abelian groups, and L_2 is a lattice then L_1 is a lattice in $\mathbb{R}^n$ if and only if $[L_2 : L_1] < \infty$. Furthermore, in this case*

$$\mathrm{Vol}\,(\mathbb{R}^n / L_1) = [L_2 : L_1]\,\mathrm{Vol}\,(\mathbb{R}^n / L_2) \,.$$

Lemma 4.19. *If $F_1, F_2 \subseteq \mathbb{R}^n$ are two fundamental domains of a discrete subgroup $M \leq \mathbb{R}^n$, then* $\mathrm{Vol}\,(F_1) = \mathrm{Vol}\,(F_2)$.

Proof. Write

$$\mathbb{R}^n = \bigsqcup_{w \in L} (F_1 + w) = \bigsqcup_{w \in L} (F_2 + w) \,.$$

We get that

$$F_1 = F_1 \cap \mathbb{R}^n = F_! \cap \bigsqcup_{w \in L} (F_2 + w) = \bigsqcup_{w \in L} (F_1 \cap (F_2 + w))]text.$$

Then

$$\mathrm{Vol}\,(F_1) = \sum_{w \in L} \mathrm{Vol}\,(F_1 \cap (F_2 + w)) = \sum_{W \in L} \mathrm{Vol}\,((F_1 + w) \cap F_2)$$

and by the same reasoning this is equal to $\mathrm{Vol}\,(F_2)$, hence the result. $\square$

4.18. Choose a fundamental domain F for L_2 in $\mathbb{R}^n$ and choose a set of representatives $(v_i)_{i\in I}$ of L_2/L_1. The union $\bigsqcup_{i\in I} F + v_i$ is disjoint and forms a fundamental domain fr L_1 in $\mathbb{R}^n$.

If $L_1 \leq L_2$ is of finite index, we've found a fundamental domain of L_1 of volume $[L_2 : L_1] \operatorname{Vol}(\mathbb{R}^n/L_2)$ by Theorem 4.19. $\square$

Notation 4.20. We denote by $\lambda(A)$ the Lebesgue measure of a measurable subset $A \subseteq \mathbb{R}^n$.

Definition 4.21. Let $L \leq \mathbb{R}^n$ be a discrete subgroup. We define

$$\operatorname{Vol}(\mathbb{R}^n/L)$$

to be $\lambda(F)$ for any choice of measurable fundamental domain F of L.

Corollary 4.22. *Let $L_1 \leq L_2 \leq \mathbb{R}^2$ be subgroups of $\mathbb{R}^n$ and assume that L_2 is a lattice. Then L_1 is a lattice iff $|L_2/L_1| < \infty$, and in this case $\operatorname{Vol}(\mathbb{R}^n/L_1) = [L_2 : L_1] \cdot \operatorname{Vol}(\mathbb{R}^n/L_2)$.*

Proof. If $\{v_i\}_{i\in I}$ is a set of representatives of L_2/L_1 in L_2., and F is a parallelopiped of L_2 in $\mathbb{R}^n$, then by the above $\tilde{F} = \bigsqcup_{i\in I}(F + v_i)$ is a measurable fundamental domain for L_1 in $\mathbb{R}^n$. If $[L_2 : L_1] = |I|$ is finite, then by definition we have

$$\begin{aligned}\operatorname{Vol}(\mathbb{R}^n/L_1) &= |I| \cdot \lambda(F)\\ &= [L_2 : L_1] \operatorname{Vol}(\mathbb{R}^n/L_2)\end{aligned}$$

and also L_1 is a lattice since it is discrete and cocompact. If $|I| = \infty$, then $\operatorname{Vol}(\mathbb{R}^n/L_1) = \infty$. Then L_1 cannot be a lattice. $\square$

Definition 4.23. Let $\Lambda \subseteq K$ be a full module. The *discriminant* $\Delta(\Lambda)$ is defined as

$$\Delta(\Lambda) \coloneqq \det\begin{pmatrix} | & & | \\ \vec{\sigma}(\alpha_1) & \cdots & \vec{\sigma}(\alpha_n) \\ | & & | \end{pmatrix}^2$$

where

$$\Lambda = \operatorname{Span}_{\mathbb{Z}}(\alpha_1, \ldots, \alpha_n).$$

Exercise 4.3. Show that $\Delta(\Lambda)$ is independent of the ordering of $\sigma_1, \ldots, \sigma_n$ of the embeddings and of the choice of basis for Λ.

Remark 4.24. Note that if $\vec{\alpha}, \vec{\beta}$ are two ordered bases of $K/\mathbb{Q}$, then

$$\det\begin{pmatrix} | & & | \\ \vec{\sigma}(\alpha_1) & \cdots & \vec{\sigma}(\alpha_n) \\ | & & | \end{pmatrix} [\mathrm{id}_K]_{\vec{\alpha}}^{\vec{\beta}} = \det\begin{pmatrix} | & & | \\ \vec{\sigma}(\beta_1) & \cdots & \vec{\sigma}(\beta_n) \\ | & & | \end{pmatrix}.$$

We also saw that $\mathrm{Span}_{\mathbb{Z}}(\alpha) = \mathrm{Span}_{\mathbb{Z}}\left(\vec{\beta}\right)$, so it follows that $[\mathrm{id}_K]_{\vec{\alpha}}^{\vec{\beta}} \in \mathrm{GL}_n(\mathbb{Z})$.

Remark 4.25. It holds that $\Delta(\Lambda) \in \mathbb{Q}$ by looking at automorphisms of $\mathbb{C}$ over $\mathbb{Q}$.

Remark 4.26. Recall that the matrix $B \coloneqq \begin{pmatrix} | & & | \\ \vec{\sigma}(\alpha_1) & \cdots & \vec{\sigma}(\alpha_n) \\ | & & | \end{pmatrix}$ is tightly related to $A \coloneqq \begin{pmatrix} | & & | \\ \varphi(\alpha_1) & \cdots & \varphi(\alpha_n) \\ | & & | \end{pmatrix}$. We've shown that

$$\det(B) = \pm(2i)^{r_2} \cdot \det(A).$$

It follows that

$$\Delta(\Lambda) = 4^{r_2}(-1)^{r_2}\,\mathrm{Vol}^2\left(\mathbb{R}^2/\varphi(\Lambda)\right).$$

This has sign $(-1)^{r_2}$.

Remark 4.27. There is a third important way to interpret the discriminant $\Delta(\Lambda)$.

We look at the trace map

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}} \colon K &\to \mathbb{Q} \\ \alpha &\mapsto \sum_{i\in[n]} \sigma_i(\alpha) \end{aligned}$$

and define

$$\begin{aligned} B \colon K \times K &\to \mathbb{Q} \\ (\alpha, \beta) &\mapsto \mathrm{Tr}(\alpha \cdot \beta). \end{aligned}$$

If we choose the basis $(\alpha_1, \ldots, \alpha_n)$ of Λ and represent B by the basis

$(\alpha_!, \ldots, \alpha_n)$ we get

$$\begin{aligned}
[B]_{\vec{\alpha}} &= \left(\operatorname{Tr}(\alpha_i, \alpha_j)\right)_{i,j\in[n]} \\
&= \left(\langle \vec{\sigma}(\alpha_i), \vec{\sigma}(\alpha_j)\rangle\right)_{i,j\in[n]} \\
&= \begin{pmatrix} | & & | \\ \vec{\sigma}(\alpha_1) & \cdots & \vec{\sigma}(\alpha_n) \\ | & & | \end{pmatrix}^t \begin{pmatrix} | & & | \\ \vec{\sigma}(\alpha_1) & \cdots & \vec{\sigma}(\alpha_n) \\ | & & | \end{pmatrix}.
\end{aligned}$$

We see that $\Delta(\Lambda)$ is just the determinnat of a representing matrix of the trace form with respect to a basis of Λ over $\mathbb{Z}$. This again shows the rationality of $\Delta(\Lambda)$.

Example 4.28. Suppose $K = \mathbb{Q}(\alpha)$ and take

$$\Lambda = \operatorname{Span}_{\mathbb{Z}}\left(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right).$$

This is a full module in K, and we would like to find $\Delta(\Lambda)$. By definition,

$$\Delta(\Lambda) = \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \cdots & \sigma_1(\alpha)^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \sigma_n(\sigma) & \sigma_n(\alpha)^2 & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2$$

which is a Vandermonde matrix. The determinant is then $\prod_{i>j}(\sigma_i(\alpha) - \sigma_j(\alpha))^2$.

Remark 4.29. Consider $p(x_1, \ldots, x_n) \coloneqq \prod_{i>j}(x_i - x_j)^2$, which is a symmetric polynomial. Let R be the subring of symmetric polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$. Then R contains

$$\begin{aligned}
s_1 &\coloneqq x_1 + \ldots + x_n \\
s_2 &\coloneqq \sum_{i<j} x_i x_j \\
&\vdots \\
s_n &= x_1 \cdot \ldots \cdot x_n.
\end{aligned}$$

Hence R contains

$$\{q(s_1, \ldots, s_n) \mid q \in \mathbb{Z}[x_1, \ldots, x_n]\}.$$

A theorem states that this is in fact equality.

So, in the above example, $\Sigma(\Lambda)$ is a polynomial in the s_i, which are the coefficients of the minimal polynomial of α over $\mathbb{Q}$. This happens to be the discriminant of that minimal polynomial.

Example 4.30. If $\mathbb{Q}(\alpha)$ is quadratic and the minimal polynomial of α is $x^2 + bx + c$, then

$$\Delta\left(\operatorname{Span}_{\mathbb{Z}}(1, \alpha)\right) = \det \begin{pmatrix} 1 & \frac{-b+\sqrt{b^2-4c}}{2} \\ 1 & \frac{-b-\sqrt{b^2-4c}}{2} \end{pmatrix}^2 = b^2 - 4c$$

which is the usual discriminant.

Definition 4.31 (Order)**.** An *order* $\mathscr{O}$ in K is a full module in K which is also a ring.

Example 4.32. If $K = \mathbb{Q}(\alpha)$ and the minimal polynomial of α is over $\mathbb{Z}$, write

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

for $a_i \in \mathbb{Z}$. Then

$$\mathbb{Z}[\alpha] = \operatorname{Span}_{\mathbb{Z}}\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}.$$

Then $\mathscr{O} \coloneqq \mathbb{Z}[\alpha]$ is an order.

Remark 4.33. If α satisfies $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0$ with coefficients in $\mathbb{Q}$. Taking m to be the lowest-common-multipler of the denominators, we get

$$\sum_{i=0}^{n} m^{n-i} a_i (m\alpha)^i$$

where $a_n = 1$. We get that there's $m \in \mathbb{Z}$ such that $m\alpha$ has a minimal polynomial over $\mathbb{Z}$.

We give another example that shows orders exist.

Example 4.34. Let $\vec{\alpha} \coloneqq (\alpha_1, \ldots, \alpha_n)$ be a basis of $K/\mathbb{Q}$. Consider the $\mathbb{Q}$-linear map $m_\beta \colon K \to K$ which is multiplication by β. We consider the matrix $[m_\beta]_{\vec{\alpha}} \in M_n(\mathbb{Q})$. Then the map $\beta \mapsto [m_\beta]_{\vec{\alpha}}$ is a $\mathbb{Q}$-algebra homomorphism (and is in particular a field embedding).

Pulling back $M_n(\mathbb{Z})$ under this homomorphism, one can check that it contains a basis. Hence this gives an order inside K.

Remark 4.35. If $\Lambda = \operatorname{Span}_{\mathbb{Z}}(\alpha_1, \ldots, \alpha_n)$ is a full module, then Λ is an order if and only if $[m_{\alpha_i}]_{\vec{\alpha}} \in M_n(\mathbb{Z})$ for all $i \in [n]$, and $1 \in \Lambda$.

Proposition 4.36. *If $\mathscr{O} \subseteq K$ is an order, then $\Delta(\mathscr{O}) \in \mathbb{Z}$.*

Proof. Let $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$ be a basis of $\mathscr{O}$ over $\mathbb{Z}$. We conclude that

$$[m_{\alpha_i}]_{\vec{\alpha}} \left[m_{\alpha_j}\right]_{\vec{\alpha}} = \left[m_{\alpha_i \cdot \alpha_j}\right]_{\vec{\alpha}} \in M_n(\mathbb{Z})$$

so

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) \overset{(*)}{=} \mathrm{Tr}\left[m_{\alpha_i \cdot \alpha_j}\right]_{\vec{\alpha}} \in \mathbb{Z}$$

so

$$\Delta(\mathscr{O}) = \det(\mathrm{Tr}(\alpha_i \alpha_j)) \in \mathbb{Z}.$$

We're left to explain $(*)$. For $\beta \in K$ we defined

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta) = \sum_{i \in [n]} \sigma_i(\beta).$$

But, it holds that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta) = \mathrm{Tr}\,[m_\beta]_B$$

for any $\mathbb{Q}$-basis B of K (this is the usual definition). □

Proposition 4.37. *Any two orders in K are contained in a single order.*

Proof. If $\mathscr{O}_1, \mathscr{O}_2 \subseteq K$ are order, the product

$$\mathscr{O}_1 \cdot \mathscr{O}_2 = \left\{ \sum_{i \in [\ell]} a_i b_i \;\middle|\; \substack{a_i \in \mathscr{O}_1 \\ b_i \in \mathscr{O}_2} \right\}$$

is clearly an order that contains both $\mathscr{O}_1$ and $\mathscr{O}_2$. □

Theorem 4.38. *There exists a unique maximal order in K.*

Proof. By the previous proposition, it suffices to show that any sequence of order $\mathscr{O}_1 \subseteq \mathscr{O}_2 \subseteq \dots$ stabilizes.

Note that $[\mathscr{O}_{i+1} : \mathscr{O}_i] < \infty$ for all $i \in \mathbb{Z}_+$. Now, $[\mathscr{O}_{i+1} : \mathscr{O}_i] = [\varphi(\mathscr{O}_{i+1}) : \varphi(\mathscr{O}_i)]$ and by the index formula we get

$$\mathrm{Vol}(\mathbb{R}^n/\varphi(\mathscr{O}_1))^2 = [\mathscr{O}_i \colon \mathscr{O}_1]^2\, \mathrm{Vol}(\mathbb{R}^n/\varphi(\mathscr{O}_i))^2.$$

Because both volumes squared are integral up to $(-4)^{r_2}$, we get that $[\mathscr{O}_i : \mathscr{O}_1]^2$ must divide a given fixed integer. Hence $[\mathscr{O}_i : \mathscr{O}_1]$ must stabilize. □

Exercise 4.4. Note that the argument proving the stabilization of $\mathscr{O}_i$ relied on the following lemma: If $\Lambda_1 \leq \Lambda_2$ are two full modules, then

$$\Delta(\Lambda_2) \cdot [\Lambda_2 : \Lambda_1] = \Delta(\Lambda_1).$$

Prove this in two ways:

1. Using $\Delta(\Lambda) = \left((2i)^{r_2} \operatorname{Vol}(\mathbb{R}^n/\varphi(\Lambda))\right)^2$.

2. Using $\Delta(\Lambda) = \det(\sigma_i(\alpha_j))_{i,j\in[n]}$, where $(\alpha_1, \ldots, \alpha_n)$ is a $\mathbb{Z}$-basis.

Notation 4.39. Denote by $\mathscr{O}_K$ the maximal order of a field K.

Example 4.40. We calculate $\mathscr{O}_K$ for $K = \mathbb{Q}\left(\sqrt{d}\right)$ with $d \in \mathbb{Z}\backslash\{0,1\}$ which is square-free. Let $\mathscr{O} = \mathbb{Z}\left[\sqrt{d}\right]$, which is an order. We calculate

$$\Delta(\mathscr{O}) = \det\begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}\left(\sqrt{d}\right) \\ \operatorname{Tr}\left(\sqrt{d}\right) & \operatorname{Tr}\left(\sqrt{d}\right) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

By the relation

$$\mathbb{Z} \ni \Delta(\mathscr{O}) = [\mathscr{O}_K : \mathscr{O}]^2 \, \Delta(\mathscr{O}_K)$$

we see that the only option for strict in inclusion is an order $\mathscr{O} \subsetneq \mathscr{O}_K$ containing 0 as a subgroup of index 2. Assuming this is the case, there are $a, b \in \mathbb{Z}$ such that $\frac{a+b\sqrt{d}}{2} \in \mathscr{O}_K \setminus \mathscr{O}$. WLOG we can assume $a, b \in \{0,1\}$ where not both are 0, and $a = 1, b = 0$ is impossible because $\frac{1}{2}$ has norm $\frac{1}{4}$ and therefore doesn't belong to any order. By similar reasoning, we cannot have $a = 0, b = 1$, since $N\left(\frac{\sqrt{d}}{2}\right) = -\frac{d}{4}$ which isn't an integer since d is square-free.

We're left with the possibility $(a,b) = (1,1)$. In this case we have

$$\mathscr{O}_K = \operatorname{Span}_{\mathbb{Z}}\left(1, \frac{1+\sqrt{d}}{2}\right).$$

Indeed, we get $\mathscr{O} \subseteq \operatorname{Span}_{\mathbb{Z}}\left\{1, \frac{1+\sqrt{d}}{2}\right\} \subseteq \mathscr{O}_K$ and $[\mathscr{O}_K : \mathscr{O}]$ so there's nothing in between.

Denote $\alpha = \frac{1+\sqrt{1}}{2}$, and $B = (1, \alpha)$. Then

$$[m_\alpha]_B = \begin{pmatrix} 0 & \frac{d-1}{4} \\ 1 & 1 \end{pmatrix}.$$

Hnece $\operatorname{Span}_{\mathbb{Z}}(1, \alpha)$ is an order if and only if $\frac{d-1}{4} \in \mathbb{Z}$. We deduce that $\mathscr{O}$ is the maximal order if and only if $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$. If $d \equiv 1 \pmod 4$, then $\mathscr{O} \subsetneq \mathscr{O}_K$ so $\mathscr{O}$ isn't maximal.

Exercise 4.5. Calculate the maximal order in $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

Solution. Let $\alpha = \sqrt[3]{2}$ and guess that $\mathscr{O} \coloneqq \mathbb{Z}[\alpha] = \operatorname{Span}_{\mathbb{Z}}\left(1, \alpha, \alpha^2\right)$ is a maximal order. We calculate

$$\Delta(\mathscr{O}) = \det \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\alpha) & \operatorname{Tr}\left(\alpha^2\right) \\ \operatorname{Tr}(\alpha) & \operatorname{Tr}\left(\alpha^2\right) & \operatorname{Tr}(2) \\ \operatorname{Tr}\left(\alpha^2\right) & \operatorname{Tr}(2) & 2\operatorname{Tr}(\alpha) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix} = -2^2 \cdot 3^3.$$

If $\mathscr{O}$ is *not* maximal, we should look for a full module Λ that contains $\mathscr{O}$ as a subgroup of index 2, 3, or 6, since the order must divide $\Delta(\mathscr{O})$.

Exercise 4.6. Let $\xi \coloneqq e^{\frac{2\pi i}{5}}$ be a primitive fifth root of unity, with minimal polynomial $\Phi(x) \coloneqq x^4 + x^3 + x^2 + x + 1$. Calculate $\mathscr{O}_{\mathbb{Q}(\xi)}$.

4.3 Rings of Integers & Integral Extensions

Let Ω be a field and let $A \subseteq \Omega$ be a ring.

Definition 4.41 (Integral Element)**.** An element $\alpha \in \Omega$ is *integral* over A if there is a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Example 4.42. If A is a field, then α is integral over A if and only if α is algebraic over A.

Theorem 4.43. *The following are equivalent.*

1. *$\alpha \in \Omega$ is integral over A.*
2. *The ring $A[\alpha]$ is a finitely-generated A-module.*
3. *There exists a finitely-generated A-module $M \subseteq \Omega$ which is α-stable in the sense of $\alpha M \subseteq M$.*

Proof. (1) $\implies$ (2)**:** Assume that $p(\alpha)$ for some $p(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$. Then $\alpha^n = \sum_{i=0}^{n-1} a_i \alpha^i$ so $A[\alpha]$ is generated as an A-module by $1, \alpha, \ldots, \alpha^{n-1}$.

(2) $\implies$ (3)**:** This is clear by taking $M = A[\alpha]$.

(3) $\implies$ (1)**:** Let M be as in condition (3). Let $\beta_1, \ldots, \beta_n \in M$ generate M as an A-module. Consider the map

$$\begin{aligned} \varphi \colon A^n &\to M \\ \begin{pmatrix} a_1 \\ \cdots \\ a_n \end{pmatrix} &\mapsto \sum_{i \in [n]} a_i \beta_i, \end{aligned}$$

which is therefore onto.

The fact that M is α-stable means that there are $a_{i,j} \in A$ such that

$$m_\alpha(\beta_j) = \alpha\beta_j = \sum_{i\in[n]} a_{i,j}\beta_j.$$

Let $L = (a_{i,j})_{i,j\in[n]}$. We get a commutative diagram

$$\begin{tikzcd} A^n \arrow[r] \arrow[d, "L"'] & M \arrow[d, "m_\alpha"] \\ A^n \arrow[r] & M \end{tikzcd}$$

where the upper map is $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum a_i\beta_i$. We get

$$(\beta_1, \ldots, \beta_n) L = (\alpha\beta_1, \ldots, \alpha\beta_n),$$

so α is an eigenvalue of L. We get that α is a root of the characteristic polynomial of L, which is monic over A.

□

Theorem 4.44. *The set*

$$\bar{A}^\Omega := \{\alpha \in \Omega \mid \alpha \textit{ is integral over } A.\}$$

forms a subring over Ω.

Proof. Clearly $\bar{A}^\Omega$ contains A, so it contains the unit. We have to show that it is closed under addition and multiplication. Let $\alpha, \beta \in \bar{A}^\Omega$. By Theorem 4.43 there are $M, N \subseteq \Omega$ both finitely-generated such that M, N are respectively α, β-stable.

Then $M \cdot N$ is an A-module which is finitely-generated (it is generated by the products of generators of M and of N). Clearly, this is $\alpha + \beta$-stable and $\alpha \cdot \beta$-stable, hence Theorem 4.43 gives the result. □

Definition 4.45. The above-mentioned ring is called the *integral closure* of A in Ω.

Example 4.46. Let $A \subseteq \Omega$ be a field. Then $\bar{A}^\Omega$ is the subfield of A-algebraic elements in Ω.

For example, $\mathbb{Q}^{\mathbb{C}} = \mathbb{Q}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Proposition 4.47. *Let $\Omega = K$ be a number field, and let $A = \mathbb{Z} \subseteq \Omega$. Then $\bar{\mathbb{Z}}^K = \mathscr{O}_K$.*

Proof. For $\alpha \in \mathscr{O}_K$ we know that $\mathscr{O}_K$ is a finitely-generated $\mathbb{Z}$-module in Ω that is α-stable. By Theorem 4.43 we get that α is integral over $\mathbb{Z}$.

In the other direction, if α i integral over $\mathbb{Z}$, the ring $\mathbb{Z}[\alpha]$ is finitely-generated by Theorem 4.43. Then $\mathbb{Z}[\alpha]$ is an order, which contains $\mathscr{O}_K$ and therefore equals to it. We get that $\alpha \in \mathscr{O}_K$, as required. □

Lemma 4.48. *Let $A \subseteq \Omega_1 \subseteq \Omega_2$ where A is a ring and Ω_i are fields. Then*

1. $\bar{A}^{\Omega_2} \cap \Omega_1 = \bar{A}^{\Omega_1}$.
2. $\bar{A}^{\Omega_2} = \overline{\bar{A}^{\Omega_1}}^{\Omega_2}$.

Proof.

1. This is immediate from definition.
2. Since $A \subseteq \bar{A}^{\Omega_1}$, we have $\bar{A}^{\Omega_2} \subseteq \overline{\bar{A}^{\Omega_1}}^{\Omega_2}$. We have to show that there's actual equality.

   Let $\alpha \in \overline{\bar{A}^{\Omega_1}}^{\Omega_2}$. We can write

   $$\alpha^n = \sum_{i=0}^{n-1} b_i \alpha^i$$

   for $b_i \in \bar{A}^{\Omega_1}$. We show that the ring $A[b_1, \ldots, b_{n-1}, \alpha] \subseteq \Omega_2$ is finitely-generated as an A-module and get the result by Theorem 4.43. This follows from induction by the following lemma.

Lemma 4.49. *Let*

□