Reminder:

Let A be a Dedekind ring, that is, a noetherien normal integral domain of Krull dimension 1.

Theorem 1.10.5: Any non-zero ideal of A is a product of maximal ideals and the factors are unique up to permutation. *(Unique factorization of ideals)*

Theorem 1.10.6: (a) The set J_A of fractional ideals is an abelian group with the above product and inverse and the unit element $(1) = A$.

(b) The group J_A is the free abelian group with basis the maximal ideals of A.

Proof (a) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$, $(1)\mathfrak{a} = \mathfrak{a}$, $\Rightarrow$ $\mathfrak{a} = \frac{1}{b} \cdot b\mathfrak{a}$

$\forall \mathfrak{a} : \exists b \in A \setminus \{0\} : \mathfrak{a} \subset \left(\frac{1}{b}\right) \Rightarrow b \cdot \mathfrak{a} \subset (1) = A.$

Write $\mathfrak{a} \cdot b = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ with $\mathfrak{p}_i$ maximal $\Rightarrow \forall i : \mathfrak{p}_i^{-1}\mathfrak{p}_i = (1).$

$\Rightarrow \mathfrak{a} \cdot b \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} = (1).$ $\Rightarrow$ Existence of inverse element.

$\Rightarrow$ abelian group.

Remains to prove: $\forall \mathfrak{a} : \mathfrak{a}^{-1}\mathfrak{a} = (1).$ $\Leftarrow$ LATER

(b) Write $(b) = \mathfrak{q}_1 \cdots \mathfrak{q}_s \Rightarrow \mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r (\mathfrak{q}_1 \cdots \mathfrak{q}_s)^{-1}$

If $\prod p_i^{\nu_i} = (1)$ with $\nu_i \in \mathbb{Z}$, p_i distinct $\Rightarrow \prod_i p_i^{\max\{0,\nu_i\}} = \prod_i p_i^{\max\{0,-\nu_i\}}$

$\Rightarrow$ all $\nu_i = 0$. qed.

1.11 Ideals

Consider any non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset A$.

Definition 1.11.1: We write $\mathfrak{b}|\mathfrak{a}$ and say that $\mathfrak{b}$ *divides* $\mathfrak{a}$ if and only if $\mathfrak{a} \subset \mathfrak{b}$.

Proposition 1.11.2: For any $a, b \in A \setminus \{0\}$ we have $b|a$ if and only if $(b)|(a)$.

Proof: $b | a \Leftrightarrow \exists c \in A : bc = a \Leftrightarrow a \in (b) \Leftrightarrow (a) \subset (b) \Leftrightarrow (b) | (a)$. qed.

Proposition 1.11.3: We have $\mathfrak{b}|\mathfrak{a}$ if and only if there is a non-zero ideal $\mathfrak{c} \subset A$ with $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$.

Proof: $\mathfrak{b}\mathfrak{c} = \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{b}\mathfrak{c} \subset \mathfrak{b} \Rightarrow \mathfrak{b} | \mathfrak{a}$.

If $\mathfrak{b} | \mathfrak{a}$ set $\mathfrak{c} := \mathfrak{b}^{-1}\mathfrak{a} \Rightarrow \mathfrak{b}\cdot\mathfrak{c} = \mathfrak{b}\cdot\mathfrak{b}^{-1}\cdot\mathfrak{a} = \mathfrak{a}$.

fractional ideal.

$\mathfrak{a} \subset \mathfrak{b} \Rightarrow \mathfrak{b}^{-1}\mathfrak{a} \subset \mathfrak{b}^{-1}\mathfrak{b} = (1) = A$. qed.

Definition 1.11.4: Ideals $\mathfrak{a}, \mathfrak{b} \subset A$ with $\mathfrak{a} + \mathfrak{b} = A$ are called *coprime.*

Proposition 1.11.5: For any non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset A$ the following are equivalent:

(a) $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.

(b) Their factorizations in maximal ideals do not have a common factor.

(c) $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Chinese Remainder Theorem 1.11.6: For any pairwise coprime ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \subset A$ we have a ring isomorphism

$$\boxed{\begin{aligned} A/\mathfrak{a}_1 \cdots \mathfrak{a}_r &\xrightarrow{\ \sim\ } A/\mathfrak{a}_1 \times \ldots \times A/\mathfrak{a}_r, \\ a + \mathfrak{a}_1 \cdots \mathfrak{a}_r &\longmapsto (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_r). \end{aligned}}$$

Proof: Induction on r $\Rightarrow$ WLOG $r = 2$.

So take ideals $\mathfrak{a}, \mathfrak{b} < A$ with $\mathfrak{a} + \mathfrak{b} = A$.

$\Rightarrow$ Homo $\varphi : A \longrightarrow A/\mathfrak{a} \times A/\mathfrak{b}$, $\quad x \mapsto (x+\mathfrak{a}, x+\mathfrak{b})$

$\ker(\varphi) = \mathfrak{a} \cap \mathfrak{b} \supset \mathfrak{a}\cdot\mathfrak{b}$ $\Rightarrow$ $\bar{\varphi} : A/\mathfrak{a}\mathfrak{b} \longrightarrow A/\mathfrak{a} \times A/\mathfrak{b}$.

Choose $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ with $a + b = 1$. $\quad A/\mathfrak{a}\mathfrak{b} \longleftarrow A/\mathfrak{a} \times A/\mathfrak{b}$

$bx + ay + \mathfrak{a}\mathfrak{b} \longleftarrow\!\shortmid (x+\mathfrak{a}, y+\mathfrak{b})$

Well defined: change x to $x + a'$ for $a' \in \mathfrak{a}$ $\Rightarrow$ image changes by $ba' \in \mathfrak{a}\mathfrak{b}$

" y to $y + b'$ " $b' \in \mathfrak{b}$ $\Rightarrow$ " " " $ab' \in \mathfrak{a}\mathfrak{b}$.

Mutually inverse: $x + \mathfrak{a}\mathfrak{b} \mapsto (x+\mathfrak{a}, x+\mathfrak{b}) \mapsto bx + ax + \mathfrak{a}\mathfrak{b} = x(a+b) + \mathfrak{a}\mathfrak{b}$

$= x + \mathfrak{a}\mathfrak{b}$.

$(x+\mathfrak{a}, y+\mathfrak{b}) \mapsto bx + ay + \mathfrak{a}\mathfrak{b} \mapsto (bx + ay + \mathfrak{a}, bx + ay + \mathfrak{b})$

$bx = x - ax$

$= (x + \underbrace{a(y-x)}_{\in \mathfrak{a}} + \mathfrak{a}, \ y + \underbrace{b(x-y)}_{\in \mathfrak{b}} + \mathfrak{b})$.

$\boxed{\text{Note: This means } \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\cdot\mathfrak{b}.}$

$= (x + \mathfrak{a}, y + \mathfrak{b})$. $\quad$ qed.

Proposition 1.11.7: For any fractional ideals $\mathfrak{a} \subset \mathfrak{b}$ there exists $b \in \mathfrak{b}$ with $\mathfrak{b} = \mathfrak{a} + (b)$.

Proof: Write $\mathfrak{b} = \prod_i \mathfrak{p}_i^{\mu_i}$ with $\mathfrak{p}_i$ distinct, and $\mathfrak{b}^{-1}\mathfrak{a} = \prod_i \mathfrak{p}_i^{\lambda_i - \mu_i}$ $\Rightarrow$ all $\lambda_i \geq \mu_i$, and $\mathfrak{a} = \prod_i \mathfrak{p}_i^{\lambda_i}$.

Then $\forall j$: $\prod_{i \neq j} \mathfrak{p}_i \not\subset \mathfrak{p}_j$. $\Rightarrow$ $\mathfrak{b} \cdot \prod_{i \neq j} \mathfrak{p}_i \not\subset \mathfrak{b} \cdot \mathfrak{p}_j$. Choose $b_j \in \mathfrak{b} \cdot \prod_{i \neq j} \mathfrak{p}_i \setminus \mathfrak{b} \cdot \mathfrak{p}_j$.

$\Rightarrow \forall i,j$: $\begin{vmatrix} b_j \in \mathfrak{b}\mathfrak{p}_i & \text{if } i \neq j \\ b_j \notin \mathfrak{b}\mathfrak{p}_j & \end{vmatrix}$ $\Rightarrow \forall i$: $b := \sum_j b_j \notin \mathfrak{b}\mathfrak{p}_i$, $b \in \mathfrak{b}$ $\Rightarrow$ $\mathfrak{a}' := \mathfrak{a} + (b) \subset \mathfrak{b}$.

$\forall i$: $\mathfrak{a}' \not\subset \mathfrak{b} \cdot \mathfrak{p}_i$.

$\Rightarrow \mathfrak{a}' = \prod_{i=1}^{n} \mathfrak{p}_i^{\nu_i}$ with $\lambda_i \geq \nu_i \geq \mu_i$

$\Rightarrow \forall i: \nu_i = \mu_i \Rightarrow \mathfrak{a}' = \mathfrak{b}$.

qed

Proposition 1.11.8: Every fractional ideal of A is generated by 2 elements.

Proof: Choose $a \in \mathfrak{a} \setminus \{0\}$, by 1.11.7 choose $b \in \mathfrak{a}$ with $(a) + (b) = \mathfrak{a}$. [$(a) \subset \mathfrak{a}$]

$$\overset{\parallel}{(a, b)}.$$

qed

Proposition 1.11.9: For any non-zero ideal $\mathfrak{a}$ and any fractional ideal $\mathfrak{b}$ of A there exists an isomorphism of A-modules $A/\mathfrak{a} \cong \mathfrak{b}/\mathfrak{a}\mathfrak{b}$.

Proof: Apply 1.11.7 to $\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$ $\Rightarrow$ $\mathfrak{b} = \mathfrak{a}\mathfrak{b} + (b)$

$\leadsto$ homo: $\varphi: A \to \mathfrak{b}/\mathfrak{a}\mathfrak{b}$, $x \mapsto x \cdot b + \mathfrak{a}\mathfrak{b}$. $\Rightarrow$ surjective.

$x \in \ker(\varphi) \Leftrightarrow x \cdot b \in \mathfrak{a}\mathfrak{b}$

$\Leftrightarrow x \cdot (\mathfrak{a}\mathfrak{b} + (b)) \subset \mathfrak{a}\mathfrak{b}$.

$\Leftrightarrow (x) \cdot \mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$

$\Leftrightarrow (x) \subset \mathfrak{a} \Leftrightarrow x \in \mathfrak{a}$.

$\Rightarrow A/\mathfrak{a} \xrightarrow{\sim} \mathfrak{b}/\mathfrak{a}\mathfrak{b}$.

qed.

1.12 Ideal class group

Definition 1.12.1: The factor group

$$\mathrm{Cl}(A) := \{\text{fractional ideals}\} \,/\, \{\text{principal ideals}\}$$

is called the *ideal class group of A*. Its order $h(A) := |\,\mathrm{Cl}(A)|$ is called the *class number of A*.

Proposition 1.12.2: Any ideal class is represented by a non-zero ideal of A.

Pf: $\forall\, \mathfrak{a}$ fractional ideal: $\exists\, b \in A \setminus \{0\}$: $\mathfrak{a} < \left(\frac{1}{b}\right) \Rightarrow b \cdot \mathfrak{a} < A$.

and $\mathfrak{a} \sim (b) \cdot \mathfrak{a}$ modulo principal ideals. qed.

$\subset A$.

Proposition 1.12.3: There is a fundamental exact sequence

$$\boxed{1 \longrightarrow A^\times \longrightarrow K^\times \longrightarrow J_A \longrightarrow \mathrm{Cl}(A) \longrightarrow 1.}$$

$x \longmapsto (x)$

$(x) = A \Leftrightarrow x \in A^\times$.

2 Minkowski's lattice theory

2.1 Lattices

Fix a finite dimensional $\mathbb{R}$-vector space V.

Proposition 2.1.1: There exists a unique topology on V such that for any basis $v_1, \ldots, v_n$ of V the isomorphism $\mathbb{R}^n \to V$, $(x_i)_i \mapsto \sum_{i=1}^n x_i v_i$ is a homeomorphism.

Proof: Change basis:

$$\begin{array}{ccc} \mathbb{R}^n & \xrightarrow{\sim} & V \\ & L_u \searrow \quad \nearrow & \\ & \mathbb{R}^n & \end{array}$$

for $u \in GL_n(\mathbb{R})$.

$\Rightarrow L_u, L_u^{-1}$ continuous.

$\Rightarrow$ homeo.

qed.

Definition 2.1.2: A subset $X \subset V$ is called ...

(a) ... *bounded* if and only if the corresponding subset of $\mathbb{R}^n$ is bounded.

(b) ... *discrete* if and only if the corresponding subset of $\mathbb{R}^n$ is discrete, that is, if its intersection with any bounded subset is finite.

Now we are interested in an (additive) subgroup $\Gamma \subset V$.

Definition-Proposition 2.1.3: The following are equivalent:

(a) Γ is discrete.

(b) $\Gamma = \bigoplus_{i=1}^m \mathbb{Z}v_i$ for $\mathbb{R}$-linearly independent elements $v_1, \ldots, v_m$.

Such a subgroup is called a *lattice*.

Proof: (b) $\Rightarrow$ (a) Extend $v_1, \ldots, v_m$ to a basis of V $\rightsquigarrow$ $\Gamma \to \mathbb{Z}^m \times \{0\}^{n-m} \subset \mathbb{R}^n$ discrete.

(a) $\Rightarrow$ (b) Set $V' := \mathbb{R}\cdot\Gamma$, $m := \dim_{\mathbb{R}}(V')$, take $\gamma_1, \ldots, \gamma_m \in \Gamma$ which generate V' over $\mathbb{R}$.

$\Rightarrow \Gamma' := \mathbb{Z}\gamma_1 \oplus \ldots \oplus \mathbb{Z}\gamma_m \subset \Gamma$. Set $\Phi := \left\{ \sum_{i=1}^m x_i\gamma_i \,\middle|\, \forall i: x_i \in \mathbb{R},\ 0 \le x_i \le 1 \right\}$.

$\Rightarrow \Phi$ compact and $\Gamma' + \Phi = V'$. Also $\Gamma \subset V'$.

$\Rightarrow \Gamma = (\Gamma' + \Phi) \cap \Gamma = \Gamma' + \underbrace{(\Phi \cap \Gamma)}$. finite by (a).

$\Rightarrow [\Gamma : \Gamma'] < \infty$. $\Rightarrow$ Γ fin. gen. $\mathbb{Z}$-module.

$\Gamma \subset V \Rightarrow \Gamma$ torsion free. $\Rightarrow \Gamma \cong \mathbb{Z}^l$ for some l.

$[\Gamma : \Gamma'] < \infty \Rightarrow l = m$.

Write $\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m \Rightarrow v_1, \ldots, v_m$ generate V'

$\Rightarrow \mathbb{R}$-lin. independent. qed.

Definition-Proposition 2.1.4: The following are equivalent:

(a) Γ is discrete and there exists a bounded subset $\Phi \subset V$ such that $\Gamma + \Phi = V$.

(b) Γ is discrete and V/Γ is compact.

(c) $\Gamma = \bigoplus_{i=1}^{n} \mathbb{Z}v_i$ for an $\mathbb{R}$-basis $v_1, \ldots, v_n$ of V.

Such a subgroup is called a *complete lattice.*

Proof: (c) $\Rightarrow$ $\Phi := \{ \sum_{i=1}^{n} x_i v_i \mid$ all $x_i \in [0,1] \}$ $\Rightarrow$ $\Gamma + \Phi = V$. $\Rightarrow$ (a)

(a) $\Rightarrow$ $\Gamma + \Phi = V$. Suppose $V' := \mathbb{R}\Gamma \subsetneq V$.

w.l.o.g. Φ compact.

Then $\exists\, \ell : V \to \mathbb{R}$ nonzero linear form with $V' < \ker(\ell)$.

$\Rightarrow \ell(\Gamma) = 0 \Rightarrow \underset{\text{non-compact}}{\mathbb{R}} = \ell(V) = \ell(\Gamma + \Phi) = \ell(\Phi) =$ compact.

$\Rightarrow$ Contradiction.

(a) $\Leftarrow$ (b) Exercise.

qed.