Groups, Rings and Modules

June 3, 2023

Contents

Lectures

Start of lecture 1

0. Introduction

This course will consist of 3 main sections:

- Groups – Continuation from IA, focussing on:
  - Simple groups, p-groups, p-subgroups.
  - Main result in this part of the course will be the Sylow theorems.
- Rings – Sets where you can add, subtract and multiply. For example
  - $\mathbb{Z}$ or $\mathbb{C}[X]$.
  - Rings of integers $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ (more in part II number fields)
  - Polynomial rings (Part II Algebraic Geometry)

  A ring where you can divide is a field, for example $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ (prime p).
- Modules – Analogue of vector spaces where the scalars belong to a ring instead of a field. We will classify modules over certain nice rings
  - Allows us to prove Jordan Normal form and classify finite abelian groups.

Chapter I

Groups

Contents

1. Revision and Basic Theory

Definition (Group)**.** A group is a pair $(G, \cdot)$ where G is a set and $\cdot\colon G \times G \to G$ is a binary operator satisfying:

- Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$.
- Identity: $\exists e \in G$ such that $e \cdot g = g \cdot e = g \quad \forall g \in G$.
- Inverses: $\forall g \in G \ \exists g^{-1} G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Remarks

(i) In checking $\cdot$ is well-defined, need to check *closure*, i.e. $a, b \in G \implies a \cdot b \in G$. (This is implicit in the notation $\cdot\colon G \times G \to G$).

(ii) If using additive (multiplicative) notation, then often write 0 (or 1) for identity.

Definition (Subgroup)**.** A subset $H \subset G$ is a subgroup (written $H \leq G$) if $h \cdot h' \in H \ \forall h, h' \in H$ and $(H, \cdot)$ is a group.

Remark. A subset H of G is a subgroup if H is non-empty and $a, b \in H \implies a \cdot b^{-1} \in H$.

Examples

(i) Additive groups $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

(ii) Cyclic and dihedral groups. C_n = cyclic group of order n, D_{2n} = symmetric of a regular n-gon.

(iii) Abelian groups: those $(G, \cdot)$ such that

$$a \cdot b = b \cdot a \quad \forall a, b \in G$$

(iv) Symmetric and alternating groups

$$S_n = \text{all permutations of } \{1, \ldots, n\}$$

$$A_n \leq S_n \text{subgroup of even permutations}$$

(v) Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with

$$ij = k, \quad ji = -k, \quad i^2 = -1, \ldots$$

(vi) General and special linear groups.

- $\mathrm{GL}_n(\mathbb{R}) = \{n \times n$ matrices over $\mathbb{R}$ with $\det \neq 0$, and $\cdot$ is matrix multiplication.$\}$
- $\mathrm{SL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ subgroup of matrices with determinant 1.

Definition. The (direct) product of groups G and H is the set $G \times H$ with operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

Let $H \leq G$, the left cosets of H in G are the sets $gH := \{gh \colon h \in H\}$ for $g \in G$. These partition G, and each has the same cardinality as H. Deduce

Theorem 1.1 (Lagrange's Theorem)**.** Let G be a finite group and $H \leq G$. Then $|G| = |H| \cdot [G : H]$ where $[G : H]$ is the number of left cosets of H in G. $[G : H]$ is the index of H in G.

Remark. Can also carry this out with right cosets. Lagrange $\implies$ number of left cosets = number of right cosets.

Definition. Let $g \in G$. If $\exists n \geq 1$ such that $g^n = 1$, then the least such n is the order of g. Otherwise g has infinite order.

Remark. If g has order d, then

(i) $g^n = 1 \implies d \mid n$.

(ii) $\{1, g, \ldots, g^{d-1}\} \leq G$ and so if G is finite then $d \mid |G|$ (Lagrange).

A subgroup $H \leq G$ is normal if $g^{-1}Hg = H$ $\forall g \in G$. We write $H \trianglelefteq G$.

Proposition 1.2. If $H \trianglelefteq G$, then the set G/J of left cosets of H in G is a group (called the quotient) with operation $g_1 H \cdot g_2 H = g_1 g_2 H$.

Proof. Check $\cdot$ well defined. Suppose $g_1 H = g_1' H$ and $g_2 H = g_2' H$. Then $g_1' = g_1 h_1$ and $g_2' = g_2 h_2$ for some $h_1, h_2 \in H$. Then

$$\implies g_1' g_2' = g_1 h_1 g_2 h_2 = g_1 g_2 \underbrace{(g_2^{-1} h_1 g_2)}_{\in H} \underbrace{h_2}_{\in H}$$

$$\implies g_1' g_2' H = g_1 g_2 H$$

Associativity is inherited from G, the identity is $H = eH$ and the inverse of gH is $g^{-1}H$. □

Definition. If G, H are groups, a function $\phi : G \to H$ is a group homomorphism if

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \ \forall g_1, g_2 \in G$$

It has kernel $\ker(\phi) := \{g \in G \mid \phi(g) = 1\} \leq G$, and image $\mathrm{Im}(\phi) := \{\phi(g) \mid g \in G\} \leq H$.

If $a \in \ker(\phi)$ and $g \in G$, then

$$\phi(g^{-1}ag) = \phi(g^{-1}) \underbrace{\phi(a)}_{=1} \phi(g) = 1$$

so $g^{-1}ag \in \ker(\phi)$. So $\ker(\phi) \trianglelefteq G$.

Start of lecture 2

Definition. An isomorphism of groups is a group homomorphism that is also a bijection. We say G and H are isomorphic (written $G \cong H$) if $\exists$ isomorphism $\phi \colon G \to H$. (Exercise: Check $\phi^{-1} \colon H \to G$ is a group homomorphism).

Theorem (First Isomorphism Theorem)**.** Let $\phi \colon G \to H$ be a group homomorphism. Then $\ker(\phi) \trianglelefteq G$ and $G/\ker(\phi) \cong \mathrm{Im}(\phi)$.

Proof. Let $K = \ker(\phi)$. Already checked K is normal. Define $\Phi \colon G/K \to \mathrm{Im}(\phi)$, $gK \mapsto \phi(g)$. Check Φ is well-defined and injective:

$$\begin{aligned} g_1 K = g_2 K &\iff g_2^{-1} g_1 \in K \\ &\iff \phi(g_2^{-1} g_1) = 1 \\ &\iff \phi(g_2) = \phi(g_1) \end{aligned}$$

Check Φ is a group homomorphism:

$$\begin{aligned} \Phi(g_1 K g_2 K) &= \Phi(g_1 g_2 K) \\ &= \phi(g_1 g_2) \\ &= \phi(g_1)\phi(g_2) \\ &= \Phi(g_1 K)\Phi(g_2 K) \end{aligned}$$

Φ is surjective: Let $x \in \mathrm{Im}(\phi)$, say $\phi(g) = x$ for some $g \in G$. Then $x = \Phi(gK) \in \mathrm{Im}(\Phi)$. □

Example. $\phi\colon \mathbb{C} \to \mathbb{C}^\times = \{x \in \mathbb{C} \mid x \neq 0\}$, $z \mapsto e^z$. Since $e^{z+w} = e^z e^w$, this is a group homomorphism from $(\mathbb{C}, +)$ to $(\mathbb{C}^\times, x)$.

$$\ker(\phi) = \{z \in \mathbb{C} \mid e^z = 1\} = 2\pi i\mathbb{Z}$$

$$\operatorname{Im}(\phi) = \mathbb{C}^\times \qquad \text{(by existence of log)}$$

therefore $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^\times$.

Theorem (Second Isomorphism Theorem)**.** Let $H \leq G$, and $K \trianglelefteq G$. Then $HK = \{hk\colon h \in H, k \in K\} \leq G$ and $H \cap K \trianglelefteq H$. Moreover

$$HK/K \cong H/H \cap K$$

Proof. Let $h_1k_1, h_2k_2 \in HK$ (so $h_1, h_2 \in H$, $k_1, k_2 \in K$). Then

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1h_2^{-1}}_{\in H}\underbrace{h_2k_1k_2^{-1}h_2^{-1}}_{\in K} \in HK$$

Thus $HK \leq G$ (by Remark from last lecture).

Let $\phi\colon H \to G/K$, $h \mapsto h \to hK$. This is the composite of $H \hookrightarrow G$ and the quotient map $G \to G/K$, hence ϕ is a group homomorphism.

$$\ker(\phi) = \{h \in H \mid hK = k\} = H \cap K \trianglelefteq H$$

$$\operatorname{Im}(\phi) = \{hK \mid h \in H\} = HK/K$$

First isomophism theorem implies $H/H \cap K \cong HK/K$. □

Remark. Suppose $K \trianglelefteq G$. There is a bijection

$$\{\text{subgroups of } G/K\} \leftrightarrow \{\text{subgroups of } G \text{ containing } H\}$$

defined by $X \mapsto \{g \in G : gK \in X\}$ and $H/K \leftarrow H$. This restricts to a bijection

$$\{\text{normal subgroups of } G/K\} \leftrightarrow \{\text{normal subgroups of } G \text{ containing } K\}$$

Theorem 1.3 (Third Isomorphism Theorem)**.** Let $K \trianglelefteq H \trianglelefteq G$ be normal subgroups of G. Then

$$\frac{G/K}{H/K} \cong G/H$$

Proof. Let $\phi : G/K \to G/H$, $gK \mapsto gH$. If $g_1K = g_2K$, then $g_2^{-1}g_1 \in K \leq H \implies g_1H = g_2H$. Thus ϕ well-defined. ϕ is surjective group homomorphism with kernel H/K. □

If $K \trianglelefteq G$ then studying the groups K and G/K gives some information about G. This is not always available.

Definition. A group G is *simple* if 1 and G are its only normal subgroups, except if G is the trivial group (convention).

Lemma 1.4. Let G be an abelian group. G is simple if and only if $G \cong C_p$ for some prime p.

Proof. $\Leftarrow$ Let $H \leq C_p$. By Lagrange's Theorem, $|H| \mid |C_p| = p$. So $|H|$ is 1 or p, i.e. $H = \{1\}$ or $H = C_p$. Thus C_p is simple.

$\Rightarrow$ Let $1 \neq g \in G$. G contains the subgroup $\langle g \rangle = \langle \dots, g^{-2}, g^{-1}, 1, g, g^2, \dots \rangle$ - normal in G since G is abelian. Since G is simple, $\langle g \rangle = G$. If G is infinite, $G \cong (\mathbb{Z}, +)$ and $2\mathbb{Z} \leq \mathbb{Z}$, contradiction. Otherwise $G \cong C_n$ for some n, so $g^n = 1$. If $m \mid n$, then $g^{n/m}$ generates a subgroup of order m inside G. So G is simple $\implies$ only factors of n are 1 and n, so n is prime.

□

Lemma 1.5. If G is a finite group, then G has a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{m-1} \trianglelefteq G_m = G$$

with each quotient G_i/G_{i-1} simple.

Warning. G_i need not be normal in G; we only necessarily know that G_i is normal in G_{i+1}.

Proof. Induct on $|G|$. Case $|G| = 1$. If $|G| > 1$, let G_{m-1} be a normal subgroup of largest possible order $\neq |G|$. By earlier Remark, G/G_{m-1} must be simple. Apply induction to G_{m-1}. □

Start of lecture 3

2. Group Actions

Definition. For X a set, let $\mathrm{Sym}(X)$ be the group of all bijections $X \to X$ under composition (identity $\mathrm{id} = \mathrm{id}_X$).

Definition. A group G is a permutation group of degree n if $G \leq \mathrm{Sym}(X)$ with $|X| = n$.

Example. $S_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$ is a permutation group of degree n, as is $A_n \leq S_n$. $D_{2n} = \{\text{symmetries of a regular } n\text{-gon}\}$ so is a subgroup of $S_n \cong \mathrm{Sym}(\{\text{vertices of } n\text{-gon}\})$.

Definition. An action of a group G on a set X is a function $*\colon G \times X \to X$ satisfying

(i) $e * x = x$ for all $x \in X$

(ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G$ and for all $x \in X$.

Proposition 2.1. An action of a group G on a set X is equivalent to specifying a group homomorphism $\phi\colon G \to \mathrm{Sym}(X)$.

Proof. For each $g \in G$, let $\phi_g\colon X \to X$, $x \mapsto g * x$. We have

$$\begin{aligned} \phi_{g_1 g_2}(x) &= (g_1 g_2) * x \\ &= g_1 * (g_2 * x) \\ &= \phi_{g_1}(g_2 * x) \\ &= \phi_{g_1} \circ \phi_{g_2}(x) \end{aligned}$$

Then $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}$ (†).

In particular, $\phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \phi_e = \mathrm{id}$. Thus $\phi_y \in \mathrm{Sym}(X)$.

Define $\phi\colon G \to \mathrm{Sym}(X)$, $g \mapsto \phi_g$ (a group homomorphism by (†)). Conversely let $\phi\colon G \to \mathrm{Sym}(X)$ be a group homomorphism. Define $*\colon G \times X \to X$, $(g, x) \mapsto \phi(g)(x)$. Then

(i) $e * x = \phi(e)(x) = \mathrm{id}(x) = x$.

(ii)

$$\begin{aligned}(g_1 g_2) * x &= \phi(g_1 g_2)(x) \\ &= \phi(g_1) \circ \phi(g_2)(x) \\ &= g_1 * (g_2 * x)\end{aligned}$$

□

Definition. We say $\phi\colon G \to \mathrm{Sym}(X)$ is a permutation representation of G.

Definition. Let G act on a set X.

(i) The orbit of $x \in X$ is

$$\mathrm{orb}_G(x) = \{g \in x \mid g \in G\} \subseteq X.$$

(ii) The stabiliser $x \in X$ is

$$G_x = \{g \in G \mid g * x = x\} \leq G.$$

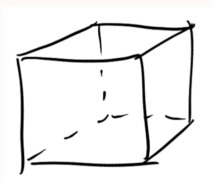
Recall Groups IA: Orbit-Stabiliser theorem. There is a bijection

$$\mathrm{orb}_G(x) \leftrightarrow G/G_x$$

(where G/G_x is the set of left cosets of G_x in G). In particular if G is finite,

$$|G| = |\,\mathrm{orb}_G(x)||G_x|$$

Example. Let G be the group of all symmetries of a cube. X = set of vertices, $x \in X$, $|\,\mathrm{orb}_G(x)| = 8$, $|G_x| = 6$.



Hence $|G| = 48$.

Remark. (i) $\ker \phi = \bigcap_{x \in X} G_x$ is called the kernel of the group action.

(ii) The orbits partition X. We say the action is *transitive* if there is only one orbit.

(iii) $G_{g*x} = gG_xg^{-1}$, so if $x, y \in X$ belong to the same orbit, then their stabilizers are conjugate.

Examples

Example. Let G act on itself by left multiplication, i.e. $g * x = g \cdot x$. The kernel of this action is

$$\{g \in G \mid g \cdot x = x \ \forall x \in G\} = \{e\}$$

Thus $G \hookrightarrow \mathrm{Sym}(G)$. This proves:

Theorem 2.2 (Cayley's Theorem)**.** Any finite group G is isomorphic to a subgroup of S_n for some n. (Take $n = |G|$).

Example. Let $H \leq G$. G acts on G/H (left cosets) by left multiplication, i.e. $g * xH = gxH$. This action is transitive (since $(x_2x_1^{-1})x_1H = x_2H$) with

$$G_{xH} = \{g \in G \mid gxH = xH\} = \{g \in G \mid x^{-1}gx \in H\} = x^{-1}Hx$$

Thus $\ker(\phi) = \bigcap_{x \in G} xHx^{-1}$. This is largest normal subgroup of G that is contained in H.

Theorem 2.3. let G be a non-abelian simple group, and $H \leq G$ a subgroup of index $n > 1$. Then $n \geq 5$ and G is isomorphic to a subgroup of A_n.

Proof. Let G act on $X = G/H$ by left multiplication and let $\phi\colon G \to \mathrm{Sym}(X) = S_n$ be the associated permutation representation. As G is simple, $\ker(\phi) = 1$ or $\ker(\phi) = G$. If $\ker(\phi) = G$, then $\mathrm{Im}(\phi) = 1$, contradiction since G acts transitively on X and $|X| > 1$. Thus $\ker(\phi) = 1$ and $G \cong \mathrm{Im}(\phi) \leq S_n$. Since $G \leq S_n$ and $A_n \trianglelefteq S_n$, second isomorphism theorem gives:

$$G \cap A_n \trianglelefteq G$$

and

$$G/G \cap A_n \cong GA_n/A_n \leq S_n/A_n \cong C_2$$

G simple implies that $G \cap A_n = 1$ or G. If it equals 1 then $G \hookrightarrow C_2$ contradicts G non-abelian. If it equals G then $G \le A_n$. Finally, if $n \le 4$, then A_n has no non-abelian simple subgroup (just list them!). □

Start of lecture 4

Example. Let G act on itself by conjugation, i.e. $g * x = gxg^{-1}$.

Definition. $\text{orb}_G(x) = \{gxg^{-1} \mid g \in G\} = \text{ccl}_G(x)$ – the conjugacy class of x in G.

Definition. $G_x = \{g \in G \mid gx = xg\} = C_G(x) \le G$ – the centraliser of x in G.

Definition. $\ker(\phi) = \{g \in G \mid gx = xg, \forall x \in G\} = Z(G)$ – center of G.

Note. The map $\phi(g) \colon G \to G$, $h \mapsto ghg^{-1}$ satisfies

$$\begin{aligned} \phi(g)(h_1 h_2) &= g h_1 h_2 g^{-1} \\ &= g h_1 g^{-1} g h_2 g^{-1} \\ &= \phi(g)(h_1) \phi(g)(h_2) \end{aligned}$$

so $\phi(g)$ is a group homomorphism, and also a bijection, so $\phi(g)$ is an isomorphism.

Definition.

$$\text{Aut}(G) = \{\text{group isomorphism } f \colon G \to G\}$$

Then $\text{Aut}(G) \le \text{Sym}(X)$ and $\phi \colon G \to \text{Sym}(X)$ has image in $\text{Aut}(G)$.

Example. Let X be the set of all subgroups of G. Then G acts on X by conjugation, i.e. $g * H = gHg^{-1}$. The stabiliser of H is

$$\{g \in G \mid gHg^{-1} = H\} = N_G(H)$$

the *normaliser* of H in G. This is the largest subgroup of G containing H as a normal subgroup.

3. Alternating Groups

Part IA: elements in S_n are conjugate if and only if they have the same cycle type.

Example. In S_5, we have

cycle type	# elements
id	1
$(* \ *)$	10
$(* \ *)(* \ *)$	15
$(* \ * \ *)$	20
$(* \ * \ *)(* \ *)$	20
$(* \ * \ * \ *)$	30
$(* \ * \ * \ * \ *)$	24
total	120

Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$ if there exists odd permutation commuting with g. Then $|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)|$ and $|\operatorname{ccl}_{A_n}(g)| = |\operatorname{ccl}_{S_n}(g)|$ otherwise $|C_{A_n}(g)| = |C_{S_n}(g)|$ and $|\operatorname{ccl}_{A_n}(g)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(g)|$.

Example. Taking $n = 5$, $(1\ 2)(3\ 4)$ commutes with $(1\ 2)$ and $(1\ 2\ 3)$ commutes with $(4\ 5)$ (and $(1\ 2)$ and $(4\ 5)$ are both odd). But if $h \in C_{S_5}(g)$ where $g = (1\ 2\ 3\ 4\ 5)$, then $(1\ 2\ 3\ 4\ 5) = h(1\ 2\ 3\ 4\ 5)h^{-1} = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))$. So $h \in \langle g \rangle \le A_5$. $|\operatorname{ccl}_{A_5}(g)| = \frac{1}{2}|\operatorname{ccl}_{A_5}(g)| = 12$. Thus A_5 has conjugacy classes of sizes $1, 15, 20, 12, 12$.

If $H \trianglelefteq A_5$, then H is a union of conjugacy classes. So $|H| = 1 + 15a + 20b + 12c$ for some integers $a, b \in \{0, 1\}$, $c \in \{0, 1, 2\}$ and by Lagrange's Theorem $|H| \big| 60$. One can check that the only way that this can happen is if $|H| = 1$ or $|H| = 60$. So A_5 is simple.

Lemma 3.1. A_n is generated by 3-cycles.

Proof. Each $\sigma \in A_n$ is product of an even number of transpositions. Thus suffices to write the product of any two transpositions as a product of 3-cycles.

For a, b, c, d distinct, the possible distinct cases are $(a\ b)(a\ b)$, $(a\ b)(b\ c)$ and $(a\ b)(c\ d)$. We can check these are all a product of 3-cycles:

$$\begin{aligned} (a\ b)(a\ b) &= \text{id} \\ (a\ b)(b\ c) &= (a\ b\ c) \\ (a\ b)(c\ d) &= (a\ c\ b)(a\ c\ d) \end{aligned}$$

□

Lemma 3.2. If $n \geq 5$ then all 3-cycles in A_n are conjugate.

Proof. We claim that any 3-cycle is conjugate to $(1\ 2\ 3)$. Indeed if $(a\ b\ c)$ is a 3-cycle then $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \notin A_n$ then replace by $\tilde{\sigma} = \sigma(4\ 5)$. □

Theorem 3.3. A_n is simple for all $n \geq 5$.

Proof. Let $1 \neq N \trianglelefteq A_n$. Suffices to show that N contains a 3-cycle, since by Lemma 3.1 and Lemma 3.2 we have $N = A_n$.

Take $1 \neq \sigma \in N$ and write σ as a product of disjoint cycles.

- Case 1: σ contains a cycle of length $r \geq 4$. Without loss of generality $\sigma = (1\ 2 \cdots r)\tau$. Let $\delta = (1\ 2\ 3)$. Then

  $$\begin{aligned} \underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} &= (r \cdots 2\ 1)(1\ 3\ 2)(1\ 2\ 3 \cdots r)(1\ 2\ 3) \\ &= (2\ 3\ r) \end{aligned}$$

  So N contains a 3-cycle.

- Case 2: σ contains two 3-cycles. Without loss of generality $\sigma = (1\ 2\ 3)(4\ 5\ 6)\tau$. Let $\delta = (1\ 2\ 4)$. Then

  $$\begin{aligned} \underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} &= (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 2\ 3)(4\ 5\ 6)(1\ 2\ 4) \\ &= (1\ 2\ 4\ 3\ 6) \end{aligned}$$

  So now done by case 1.

- Case 3: σ contains two 2-cycles. Without loss of generality $\sigma = (1\ 2)(3\ 4)\tau$. Let $\delta = (1\ 2\ 3)$. Then

  $$\begin{aligned} \underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} &= (1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3) \\ &= (1\ 4)(2\ 4) \end{aligned}$$

  Let $\varepsilon = (2\ 3\ 5)$ $(n \geq 5)$. Then

  $$\begin{aligned} \underbrace{\pi^{-1}\varepsilon^{-1}\pi\varepsilon}_{\in N} &= (1\ 4)(2\ 3)(2\ 5\ 3)(1\ 4)(2\ 3)(2\ 3\ 5) \\ &= (2\ 5\ 3) \end{aligned}$$

  So N contains a 3-cycle.

Conclusion of proof: Remains to consider σ with one of these cycle types:

- Case $(* \, *)$ or $(* \, *)(* \; * \; *)$ but then $\sigma \notin A_n$, contradiction.
- Case $(* \; * \; *)$ but then σ is a 3-cycle so we're already done. $\square$

Start of lecture 5

4. p-groups and p-subgroups

Definition. Let p be a prime. A finite group G is a p-group if $|G| = p^n$, $n \geq 1$.

Theorem 4.1. If G is a p-group, then $Z(G) \neq 1$.

Proof. For $g \in G$, we have $|\operatorname{ccl}_G(g)||C_G(g)| = |G| = p^n$, so each conjugacy class has size a power of p. Since G is a union of conjugacy classes:

$$|G| = \#(\text{conjugacy classes of size 1}) \pmod p$$

Note that

$$\begin{aligned} g \in Z(G) &\iff gxg^{-1} = x \ \forall x \in G \\ &\iff x^{-1}gx = g \ \forall x \in G \\ &\iff \operatorname{ccl}_G(g) = \{g\} \end{aligned}$$

So $|Z(G)| = \#(\text{conjugacy classes of size 1})$. So $0 \equiv |Z(G)| \pmod p$. We know $|Z(G)| \geq 1$ since $e \in Z(G)$, so therefore $|Z(G)| \geq p > 1$. □

Corollary 4.2. The only simple p-group is C_p.

Proof. Let G be a simple p-group. Since $Z(G) \trianglelefteq G$ we have $Z(G) = 1$ or G. But by the previous theorem, $Z(G) \neq 1$, so $Z(G) = G$, so G is abelian. Conclude by Lemma 1.3. □

Corollary. Let G be a p-group of order p^n. Then G has a subgroup of order p^n for all $0 \leq r \leq n$.

Proof. By Lemma 1.4, G has a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{m-1} \trianglelefteq G_m = G,$$

with each G_i/G_{i-1} being simple, and also since G is a p-group, G_i/G_{i-1} is a p-group, so $G_i/G_{i=1} \cong C_p$ by Corollary 4.2.

Thus $|G_i| = p^i$ for $0 \leq i \leq m$ and $m = n$. □

Lemma 4.3. For G a group, if $G/Z(G)$ is cyclic, then G is abelian (and so $G/Z(G)$ is trivial).

Proof. Let $gZ(G)$ be a generator for $G/Z(G)$. Then each coset is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$. Thus $G = \{g^r z : r \in \mathbb{Z}, z \in G(Z)\}$. Then

$$\begin{aligned}(g^{r_1} z_1) \cdot (g^{r_2} z_2) &= g^{r_1+r_2} z_1 z_2 \\ &= g^{r_1+r_2} z_2 z_1 \\ &= (g^{r_2} z_2) \cdot (g^{r_1} z_1)\end{aligned}$$

So G is abelian. □

Corollary 4.4. If $|G| = p^2$, then G is abelian.

Proof. We consider the 3 possible cases for $|Z(G)|$ ($|Z(G)| \bigm| p^2$ by Lagrange's theorem)

- If $|Z(G)| = 1$, then this contradicts Theorem 4.1.
- If $|Z(G)| = p$, then $|G/Z(G)| = p$. Apply Lemma 4.1, contradiction.
- $|Z(G)| = p^2$, then $Z(G) = G$ so G is abelian. □

See example sheet for case $|G| = p^3$.

4.1. Sylow Theorems

Theorem (Sylow)**.** Let G be a finite group of order $p^a m$ where p is a prime with $p \nmid m$. Then

(i) The set $\mathrm{Syl}_p(G) = \{P \le G : |P| = p^a\}$ of Sylow p-subgroups is non-empty.

(ii) All elements of $\mathrm{Syl}_p(G)$ are conjugate.

(iii) $n_p := |\mathrm{Syl}_p(G)|$ satisfies $n_p \equiv 1 \pmod p$ and $n_p \bigm| |G|$ (and hence $n_p \mid m$).

Corollary 4.5. If $n_p = 1$, then the unique Sylow p-subgroup is normal.

Proof. Let $g \in G$ and $P \in \mathrm{Syl}_p(G)$. Then $gPg^{-1} \in \mathrm{Syl}_p(G)$ and so $gPg^{-1} = P$. Thus $p \trianglelefteq G$. □

Example. Let $|G| = 1000 = 2^3 \times 5^3$. Then $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 8$, so $n_5 = 1$. Thus the unique Sylow 5-subgroup is normal, and hence G is not simple.

Example. $|G| = 132 = 2^3 \times 3 \times 11$. $n_{11} \equiv 1 \pmod{11}$ and $n_{11} \mid 12$, so $n_{11} = 1$ or $n_{11} = 12$. Suppose G is simple. Then $n_{11} \neq 1$ (otherwise the Sylow 11 subgroup is normal) and hence $n_{11} = 12$. Now $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 44$. So $n_3 = 4, 22$ ($n_3 \neq 1$ if G is simple).

Suppose $n_3 = 4$. Then letting G act on $\mathrm{Syl}_3(G)$ by conjugation gives a group homomorphism $\phi \colon G \to S_4$. Since G is simple, we must have $\ker(\phi) = 1$ or $\ker(\phi) = G$. But $\ker(\phi) = G$ contradicts Sylow (ii). So $\ker(\phi) = G$, so $G \hookrightarrow S_4$. But this is not possible since $|G| > |S_4|$.

Thus $n_3 = 22$ and $n_{11} = 12$. So G has $22 \times (3-1) = 44$ elements of order 3 and $12 \times (11-1) = 120$ elements of order 11. But $44 + 120 > 132 = |G|$.

Hence there does not exist a simple group of order 132.

Proof of Sylow Theorems

Let $|G| = p^a m$, p prime, $p \nmid m$.

(i) Let Ω be the set of all subsets of G of size p^a.

$$|\Omega| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a} \cdot \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 1}{1}$$

For $0 \leq k < p^a$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same power of p. Therefore $|\Omega|$ is coprime to p (†).

Let G act on Ω by left multiplication, i.e. for $g \in G$ and $X \in \Omega$

$$g * X = \{gx \colon x \in X\} \in \Omega$$

For any $X \in \Omega$ we have $|G_X||\operatorname{orb}_G(X)| = |G| = p^a m$. By (†) there exists X such that $|\operatorname{orb}_G(X)|$ is coprime to p. Thus $p^a \mid |G_X|$ (1). On the other hand, if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$ and hence

$$G = \bigcup_{g \in G} g * X = \bigcup_{Y \in \operatorname{orb}_G(X)} Y$$

$$\implies |G| \leq |\operatorname{orb}_G(X)||X|$$

$$\implies |G_X| = \frac{|G|}{|\operatorname{orb}_G(X)|} \leq |X| = p^a \qquad (2)$$

(1) and (2) implies

$$|G_X| = p^a$$

i.e. $G_X \in \mathrm{Syl}_p(G)$.

Start of lecture 6

(ii) We prove a stronger result:

Lemma 4.6. If $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is a p-subgroup then $Q \leq gPg^{-1}$ for some $g \in G$.

Proof. Let Q act on the left cosets G/P by left multiplication, ie

$$q \cdot gP = qgP$$

By the orbit-stabiliser theorem, each orbit has size dividing $|Q|$ so either 1 or a multiple of p. Since $|G/P| = m$ is coprime to p, there exists orbit of size 1, i.e. there exists $g \in G$ such that $qgP = gP$ for all $q \in Q$.

$$\begin{aligned} &\implies g^{-1}qg \in P \quad \forall q \in Q \\ &\implies Q \leq gPg^{-1} \end{aligned}$$

□

(iii) Let G act on $\mathrm{Syl}_p(G)$ by conjugation. Sylow (ii) implies action is transitive. Then the orbit-stabiliser theorem implies

$$n_p = |\mathrm{Syl}_p(G)| \;\big|\; |G|$$

Now let $P \in \mathrm{Syl}_p(G)$. Then P acts on $\mathrm{Syl}_p(G)$ by conjugation. The orbits have size dividing $|P| = p^a$, so either 1 or a multiple of p. To show $n_p \equiv 1 \pmod p$ it suffices to show that $\{P\}$ is the unique orbit of size 1.

If $\{Q\}$ is an orbit of size 1, then P normalizes Q, i.e. $P \leq N_G(Q)$. Now P and Q are Sylow p-subgroups of $N_G(Q)$, hence by (ii) are conjugate in $N_G(Q)$, hence equal since $Q \trianglelefteq N_G(Q)$. Thus $\{P\}$ is the unique orbit of size 1.

5. Matrix Groups

Let F be a field (for example $\mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$). Let

$$\begin{aligned}\mathrm{GL}_n(F) &:= n\times n \text{ invertible matrices with entries in } F.\\ \mathrm{SL}_n(F) &:= \ker(\mathrm{GL}_n(F) \xrightarrow{\det} F^\times) \trianglelefteq \mathrm{GL}_n(F)\end{aligned}$$

Let $Z \trianglelefteq \mathrm{GL}_n(F)$ be the subgroup of scalar matrices.

Definition.

$$\begin{aligned}\mathrm{PGL}_n(F) &= \frac{\mathrm{GL}_n(F)}{Z}\\ \mathrm{PSL}_n(F) &= \frac{\mathrm{SL}_n(F)}{Z\cap \mathrm{SL}_n(F)} \cong \frac{Z\,\mathrm{SL}_n(F)}{Z} \leq \mathrm{PGL}_n(F)\end{aligned}$$

Example 5.1. $G = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. A list of n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ are columns of some $A \in G$ if and only if they are linearly independent. Thus

$$\begin{aligned}|G| &= \underbrace{(p^n-1)}_{\text{first column}}\cdot\underbrace{(p^n-p)}_{\text{second column}}\cdots(p^n-p^2)\cdots\underbrace{(p^n-p^{p-1})}_{\text{last column}}\\ &= p^{1+2+\cdots+(n-1)}(p^n-1)(p^{n-1}-1)\cdots(p-1)\\ &= p^{\binom{n}{2}}\prod_{i=1}^{n}(p^i-1)\end{aligned}$$

So Sylow p-subgroups have size $p^{\binom{n}{2}}$. Let

$$U = \left\{\begin{pmatrix}1 & * & \cdots & *\\ 0 & 1 & \cdots & *\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots 1\end{pmatrix}\right\} \leq G$$

set of upper triangular matrices with 1's on the diagonal. Then $U \in \mathrm{Syl}_p(G)$, since there are $\binom{n}{2}$ entries above the diagonal to fill and each can take p values. Just as $\mathrm{PGL}_2(\mathbb{C})$ acts on $\mathbb{C}\cup\{\infty\}$ via Möbius maps, $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z}\cup\{\infty\}$. Indeed $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}$ acts as

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix} : z \mapsto \frac{az+b}{cz+d}$$

and since scalars act trivially, we obtain an action of $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 5.2. The permutation representation $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \to S_{p+1}$ is injective (in fact an isomorphism if $p = 2$ or $p = 3$).

Proof. Suppose $\frac{az+b}{cz+d} = z$ for all $z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. Setting $z = 0$ gives $b = 0$, $z = \infty$ gives $c = 0$, $z = 1$ gives $a = d$, so

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a scalar matrix, hence trivial in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. □

Lemma 5.3. If p is an odd prime then

$$|\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})| = \frac{p(p-1)(p+1)}{2}$$

Proof. By Example 5.1

$$|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = p(p-1)(p^2-1)$$

The group homomorphism

$$\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p\mathbb{Z})^\times$$

is surjective:

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mapsto a$$

therefore $|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \frac{\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})}{p-1} = p(p-1)(p+1)$. If

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$$

then $\lambda^2 \equiv 1 \pmod p$

$$\begin{aligned} &\implies p \mid (\lambda-1)(\lambda+1) \\ &\implies \lambda \equiv \pm 1 \pmod p \end{aligned}$$

Thus $Z \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \{\pm I\}$ (distinct since $p > 2$). Thus

$$\begin{aligned} |\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})| &= \frac{1}{2}|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| \\ &= \frac{p(p-1)(p+1)}{2} \end{aligned}$$

□

Start of lecture 7

Example 5.4. Let $G = \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$. Then $|G| = \frac{4\times5\times6}{2} = 60 = 2^2 \times 3 \times 5$. Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : 2 \mapsto \frac{az+b}{cz+d}$$

By Lemma 5.2 the permutation representation

$$\phi : G \to \mathrm{Sym}(\{0,1,2,3,4,\infty\}) \cong S_6$$

is injective.

Claim: $\mathrm{Im}(\phi) \le A_6$, i.e. $\psi : G \xrightarrow{\phi} S_6 \xrightarrow{\mathrm{sgn}} \{\pm1\}$ is trivial.
Proof: Let $g \in G$ have order d. Write $d = 2^n m$ with m odd. Then h^m has order 2^n. If $\psi(h^m) = 1$ then $\psi(h)^m = 1$ so $\psi(h) = 1$. So it suffices to show that $\psi(g) = 1$ for all $g \in G$ with order a power of 2.
Lemma 4.7 implies every such g belongs to a Sylow 2-subgroup.
Therefore it suffices to check $\psi(H) = 1$ for H a Sylow 2-subgroup. (since $\ker(\psi) \trianglelefteq G$ and all Sylow 2-subgroups are conjugate).

Take

$$H = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \{\pm I\}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \{\pm I\} \right\rangle \le G = \frac{\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})}{\{\pm I\}}$$

We compute

$$\phi \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = (1\ 4)(2\ 3)$$
$$\phi \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix} = (0\ \infty)(1\ 4)$$

Both of these are even, therefore $\psi(H) = 1$. This proves the claim.

On Example Sheet 1, Question 14 we will prove that if $G \le A_6$ and $|G| = 60$ then $G \cong A_5$.

Facts (not proved in this course)

$\mathrm{PSL}_n(\mathbb{Z}/p\mathbb{Z})$ is a simple group $\forall n \ge 2$, p prime except $(n,p) = (2,2),(2,3)$ (these are examples of finite groups of Lie type). The smallest non-abelian simple groups are

$$A_5 \cong \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$$

(order 60) and

$$\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z}) \cong \mathrm{GL}_3(\mathbb{Z}/7\mathbb{Z})$$

(order 168).

6. Finite abelian groups

Later we prove (in the modules chapter)

Theorem 6.1. Every finite abelian group is isomorphic to a product of cyclic groups.

However it may be possible to write the same group as a product of cyclic groups in more than one way.

Lemma 6.2. If $m, n \in \mathbb{Z}_{\geq 1}$ coprime then

$$C_m \times C_n \cong C_{mn}$$

Proof. let g and h be generators of C_m and C_n. Then $(g,h) \in C_m \times C_n$ and $(g,h)^r = (g^r, h^r)$. Then

$$\begin{aligned}(g,h)^r = 1 &\iff m \mid r \text{ and } n \mid r \\ &\iff mn \mid r\end{aligned}$$

(since m, n coprime). Thus (g,h) has order $mn = |C_m \times C_n|$. Therefore $C_m \times C_n \cong C_{mn}$. □

Corollary 6.3. Let G be a finite abelian group. Then

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$$

where each n_i is a prime power.

Proof. If $n = p_1^{a_1} \cdots p_r^{a_r}$ ($p_1, \ldots, p_r$ distinct primes), then Lemma 6.2 shows

$$C_n \cong C_{p_1^a} \times \cdots \times C_{p_r^{a_r}}$$

Writing each of the cyclic groups in Theorem 6.1 in this way gives the result. □

In fact when we prove Theorem 6.1 we will prove the following refinement:

Theorem 6.4. Let G be a finite abelian group. Then

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$$

for some $d_1 \mid D_2 \mid \cdots \mid d_t$.

Remark 6.5. The integers $n_1, \dots, n_k$ in Corollary 6.3 (up to ordering) and $d_1, \dots, d_t$ in Theorem 6.4 (assuming $d_1 > 1$) are uniquely determined by the group G.

(Proof omitted – but works by counting the number of elements of G of each prime power order).

Examples

(i) The abelian groups of order 8 are

$$C_8, \quad C_2 \times C_2 \quad \text{and} \quad C_2 \times C_2 \times C_2$$

(ii) The abelian groups of order 12 are

$$C_2 \times C_2 \times C_3 \cong C_2 \times C_6$$

and

$$C_4 \times C_3 \cong C_{12}$$

Definition (Exponent of a group)**.** The *exponent* of a group G is the least integer $n \geq 1$ such that $g^n = 1$ for all $g \in G$, i.e. the lowest common multiple of all the orders of the elements of G.

Example. A_4 has exponent 6.

Corollary 6.6. Every finite abelian group contains an element whose order is the exponent of the group.

Proof. If $G \cong C_{d_1} \times \cdots C_{d_t}$ with $d_1 \mid d_2 \mid \cdots \mid d_t$, then every $g \in G$ has order dividing d_t and if $h \in C_{d_t}$ is a generator then $(1, 1, 1, \dots, 1, h) \in G$ has order d_t. Thus G has exponent d_t. $\square$

Start of lecture 8

Chapter II

Rings

Contents

7. Definition and Examples

Definition (Ring)**.** A *ring* is a triple $(R, +, \cdot)$ consisting of a set R and two binary operators $+ : R \times R \to R$ and $\cdot : R \times R \to R$ satisfying:

(i) $(R, +)$ is an abelian group, with identity 0 (sometimes written 0_R).

(ii) Multiplication is associative and has an identity, i.e.

$$x \cdot (y \cdot z) = (c \cdot y) \cdot z \qquad \forall x, y, z \in R$$

and there exists $1 \in R$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in R$ (sometimes we will write 1_R).

(iii) Distributive laws

$$x \cdot (y + z) = x \cdot y + x \cdot z \qquad \forall x, y, z \in R$$
$$(x + y) \cdot z = x \cdot z + y \cdot z \qquad \forall x, y, z \in R$$

Definition (Commutative ring)**.** We say R is a commutative ring if $x \cdot y = y \cdot x$ for all $x, y \in R$.

Note. *In this course* we only consider *commutative rings*.

Remarks

(i) As in the case of groups, check closure!

(ii) For $x \in R$, write $-x$ for the inverse of x under $+$ and abbreviate $x + (-y)$ as $x - y$.

(iii) $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, so $0 \cdot x = 0$ for all $x \in R$.

(iv) $0 = 0 \cdot x = (1 - 1) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x$ hence $(-1) \cdot x = -x$ for all $x \in R$.

Definition (Subring)**.** A subset $S \subset R$ is a *subring* (written $S \leq R$) if it is a ring under $+$ and $\cdot$ with the same identity elements 0 and 1.

Examples

(i) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$ (ring of Gaussian integers)

(ii) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \leq \mathbb{R}$.

(iii) $\mathbb{Z}/n\mathbb{Z}$ = integers mod n.

(iv) R, S rings. The product $R \times S$ is a ring via

$$
\begin{aligned}
(r_1, s_1) + (r_2, s_2) &= (r_1 + r_2, s_1 + s_2) \\
(r_1, s_1) \cdot (r_2, s_2) &= (r_1 \cdot r_2, s_1 \cdot s_2) \\
0_{R\times S} &= (0_R, 0_S) \\
1_{R\times S} &= (1_R, 1_S)
\end{aligned}
$$

Note: $R \times \{0\}$ is *not* a subring of $R \times S$.

(v) Let R be a ring. A polynomial f over R is an expression $f = a_0 + a_1X + \cdots + a_nX^n$, $a_i \in \mathbb{R}$. (Note "X" is just a symbol, not a variable). The *degree* of f is the largest $n \in \mathbb{N}$ such that $a_n \neq 0$. We write $R[X]$ for the set of all polynomials over R. If $g = b_0 + b_1X + \cdots + b_mX^m$ is another polynomial, set

$$
\begin{aligned}
f + g &= \sum_i (a_i + b_i)X^i \\
f \cdot g &= \sum_i \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i
\end{aligned}
$$

Then $R[X]$ is a ring with identities 0 and 1. We identify R with the subring of $R[X]$ of constant polynomials (ie $\sum_i a_iX^i$ with $a_i = 0$ for all $i \geq 1$).

Definition (Unit)**.** An element $r \in R$ is a *unit* if it has an inverse under multiplication, i.e. $\exists s \in R$ such that $r \cdot s = 1$. The units in a ring R form a group $(R^\times, \cdot)$.

For example, $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

Definition (Field)**.** A *field* is a ring with $0 \neq 1$ such that every non zero element is a unit.

Remark. If R is a ring with $0 = 1$, then $x = x \cdot 1 = x \cdot 0 = 0$ for all $x \in R$, so $R = \{0\}$ the trivial ring.

Proposition 7.1. Let $f, g \in R[X]$. Suppose the leading coefficient of g is a unit. Then there exists $q, r \in R[X]$ such that

$$f(X) = q(X)g(X) + r(X)$$

where $\deg(r) < \deg(g)$.

Proof. By induction on $n = \deg f$. Write

$$\begin{aligned} f(X) &= a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \qquad a_n \neq 0 \\ g(X) &= b_m X^m b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 \qquad b_m \neq 0 \end{aligned}$$

If $n < m$, then put $q = 0$, $r = f$ and done. Otherwise we have $n \geq m$ and we set

$$f_1(X) = f(X) - a_n b_m^{-1} X^{n-m} X^{n-m} g(X)$$

Coefficient of X^n is $a_n - a_n b_m^{-1} b_m = 0$ therefore $\deg(f_1) < n$. By the induction hypothesis, there exists $q_1, r \in R[X]$ such that

$$\begin{aligned} f_1(X) &= q_1(X)g(X) + r(X) \qquad \deg(r) < \deg(g) \\ \implies f(X) &= \underbrace{(g_1(X) + a_n b_m^{-1} X^{n-m})}_{=g(X)} g(X) + r(X) \end{aligned}$$

□

Remark. If R is a field then we only need $g \neq 0$.

Further Examples

(i) If R is a ring and S is a set then the set of all functions $S \to \mathbb{R}$ is a ring under pointwise operations

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x) \end{aligned}$$

Further interesting examples appear as subrings, for example

$$\{\text{continuous functions } \mathbb{R} \to \mathbb{R}\}$$

has

$$\{\text{polynomial functions } \mathbb{R} \to \mathbb{R}\} = R[X]$$

as a subring.

(ii) Power series ring $R[X] = \{a_0 + a_1 X + \cdots \mid a_i \in R\}$.

(iii) Laurent polynomials

$$R[\![X, X^{-1}]\!] = \left\{ \sum_{i \in \mathbb{Z}} a \cdot X^i : a_i \in R, \text{only finitely many } a_i \neq 0 \right\}$$

Start of lecture 9

8. Homomorphisms, Ideals and Quotients

Definition. Let R and S be rings. A function $\phi : R \to S$ is a ring *homomorphism* if

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ for all $r_1, r_2 \in R$.

(ii) $\phi(r_1 r_2) = \phi(r_1) \cdot \phi(r_2)$ for all $r_1, r_2 \in R$.

(iii) $\phi(1_R) = 1_S$

A ring homomorphism that is also a bijection is called an *isomorphism*.

The kernel of ϕ is

$$\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}$$

Lemma 8.1. A ring homomorphism $\phi : R \to S$ is injective if and only if $\ker(\phi) = 0_R$.

Proof. $\phi : (R, +) \to (S, +)$ is a group homomorphism. □

Definition. A subset $I \in R$ is an ideal (written $I \trianglelefteq R$) if

(i) I is a subgroup of $(R, +)$

(ii) If $r \in R$ and $x \in I$, then $rx \in I$.

We say I is *proper* if $I \neq R$.

Lemma 8.2. If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R.

Proof. $\phi : (r, +) \to (S, +)$ is a group homomorphism, $\ker(\phi)$ is a subgroup of $(R, +)$. If $r \in R$ and $x \in \ker(\phi)$, then

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0_S = 0_S$$

hence $rx \in \ker(\phi)$. □

Remark. If I contains a unit, then $1_R \in I$ and hence $I = R$. Thus if I is a proper ideal, $1_R \notin I$, so I is not a subring.

Lemma 8.3. The ideals in $\mathbb{Z}$ are

$$n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$$

for $n = 0, 1, 2 \dots$.

Proof. Certainly $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Let $I \trianglelefteq \mathbb{Z}$ be a non-zero ideal, and n the smallest positive integer in I. Then $n\mathbb{Z} \subset I$. If $m \in I$, then write $m = qn + r$ with $q, r \in \mathbb{Z}$. Then $r = m - qn \in I$. Contradicts choice of n unless $r = 0$. But then $m \in n\mathbb{Z}$, i.e. $I \subset n\mathbb{Z}$. □

Definition. For $a \in R$, write $(a) = \{ra : r \in R\} \trianglelefteq R$. This is the *ideal generated by* a. More generally, if $a_1, a_2, \dots, a_n \in R$, we write

$$(a_1, \dots, a_n) = \{r_1 a_1 + \cdots r_n a_n \mid r_i \in R\} \trianglelefteq R.$$

Definition. Let $I \trianglelefteq R$. We say I is *principal* if $I = (a)$ for some $a \in R$.

Theorem 8.4. If $I \trianglelefteq R$ then the set R/I of cosets of I in $(R, +)$ forms a ring (called the quotient ring) with operations

$$\begin{aligned} (r_1 + I) + (r_2 + I) &= r_1 + r_2 + I \\ (r_1 + I)(r_2 + I) &= r_1 r_2 + I \end{aligned}$$

and $0_{R/I} = 0_R + I$, $1_{R/I} = 1_R + I$. Moreover, the map $R \to R/I$, $r \mapsto r + I$ is a ring homomorphism with kernel I.

Proof. Already know $(R/I, +)$ is a group. If $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$, then

$$r_1' = r_1 + a_1, \qquad r_2' = r_2 + a_2$$

for some $a_1, a_2 \in I$. Then

$$\begin{aligned} r_1' r_2' &= (r_1 + a_1)(r_2 + a_2) \\ &= r_1 r_2 + \underbrace{r_1 a_2}_{\in I} + \underbrace{r_2 a_1}_{\in I} + a_1 a_2 \end{aligned}$$

thus $r_1' r_2' + I = r_1 r_2 + I$. Remaining properties for R/I follow from those for R. □

Example. (i) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Quotient ring $\mathbb{Z}/n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$ has elements $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$. Addition and multiplication carried out $\mod n$.

(ii) Consider $(X) \subset \mathbb{C}[X]$ (polynomials with 0 constant term). If

$$f(X) = a_n X^n + r \cdots a_1 X + a_0, \qquad a_1 \in \mathbb{C}$$

then $f(X) + (X) = a_0 + (X)$. There is a bijection $\mathbb{C}[X]/(X) \to \mathbb{C}$, $f(X) + (X) \mapsto f(0)$, $a + (X) \leftarrow\!\shortmid a$. These maps are ring homomorphisms. Thus $\mathbb{C}[X]/(X) \cong \mathbb{C}$.

(iii) Consider $(X^2 + 1) \trianglelefteq \mathbb{R}[X]$

$$\mathbb{R}[X]/(X^2+1) = \{f(X) + (X^2+1) : f(X) \in \mathbb{R}[X]\}$$

By proposition 7.1, $f(X) = q(X)(X^2+1) + r(X)$ with $\deg r < 2$, i.e. $r(X) = a + bX$, $a, b \in \mathbb{R}$. Thus

$$\mathbb{R}[X]/(X^2+1) = \{a + bX + (X^2+1) : a, b \in \mathbb{R}\}$$

If $a + bX + (X^2+1) = a' + b'X + (X^2+1)$. Then $a = a' + (b - b')X = g(X)(X^2+1)$ for some $g(X) \in \mathbb{R}[X]$. Comparing degrees, we see $g(X) = 0$ and $a = a'$, $b = b'$. Consider the bijection

$$\mathbb{R}[X]/(X^2+1) \to \mathbb{C}, \qquad a + bX + (X^2+1) \mapsto a + bi$$

We show ϕ is a ring homomorphism It preserves additions and maps $1 + (X^2+1)$ to 1. Now we check that it respects multiplication:

$$\begin{aligned}
&\phi((a + bX + (X^2+1))(c + dX + (X^2+1))) \\
&= \phi((a+bX)(c+dX) + (X^2+1)) \\
&= \phi(ac + (ad+bc)X + \cancel{bd(X^2+1)} - bd + (X^2+1)) \\
&= ac - bd + (ad+bc)i \\
&= \phi(a + bX + (X^2+1))\phi(c + dX + (X^2+1))
\end{aligned}$$

Thus $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Start of lecture 10

Theorem (First Isomorphism Theorem for Rings)**.** Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \trianglelefteq R$, $\operatorname{Im}(\phi) \le S$ and there exists isomorphism

$$R/\ker(\phi) \cong \operatorname{Im}(\phi)$$

Proof. Already saw that $\ker(\phi) \trianglelefteq R$ (Lemma 8.2), and $\operatorname{Im}(\phi)$ is a subgroup of $(S, +)$.

Now

$$\phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \mathrm{Im}(\phi)$$
$$1_S = \phi(1_R) \in \mathrm{Im}(\phi)$$

Thus $\mathrm{Im}(\phi)$ is a subring of S. Let $K = \ker(\phi)$. Define

$$\Phi : R/K \to \mathrm{Im}(\phi)$$
$$r + K \mapsto \phi(r)$$

By the first isomorphism theorem for groups, this is well-defined, a bijection and a group homomorphism under $+$. Also $\Phi(1_R + K) = \phi(1_R) = 1_S$ and

$$\begin{aligned}\Phi((r_1 + K)(r_2 + K)) &= \Phi(r_1 r_2 + K) \\ &= \phi(r_1 r_2) \\ &= \phi(r_1)\Phi(r_2) \\ &= \Phi(r_1 + K)\Phi(r_2 + K)\end{aligned}$$

Thus Φ is a ring isomorphism. □

Theorem (Second Isomorphism Theorem for Rings)**.** Let $R \le S$ and $J \trianglelefteq S$. Then $R \cap J \trianglelefteq R$, $R + J = \{r + a \mid r \in R, a \in J\} \le S$, and

$$\frac{R}{R \cap J} \cong \frac{R + J}{J} \le \frac{S}{J}$$

Proof. By second isomorphism theorem for groups, $R + S$ is a subgroup of $(S, +)$, and we have

$$1_S = \underbrace{1_S}_{\in R} + \underbrace{0_S}_{\in J} \in R + J$$

If $r_1, r_2 \in R$ and $a_1, a_2 \in J$ then

$$(r_1 + a_1)(r_2 + a_2) = \underbrace{r_1 r_2}_{\in J} + \underbrace{r_1 a_2}_{\in J} + \underbrace{r_2 a_1}_{\in J} + \underbrace{a_1 a_2}_{\in J} \in R + J$$

Thus $R + J \le J$. Let $\phi : R \to S/J$, $r \mapsto r + J$. This is the composite of inclusion $R \subset S$ and the quotient map $S \to S/J$ hence ϕ is a ring homomorphism.

$$\ker(\phi) = \{r \in R \mid r + J = J\} = R \cap J \trianglelefteq R$$
$$\mathrm{Im}(\phi) = \{r + J \mid r \in R\} = \frac{R + J}{J} \le \frac{S}{J}$$

Apply first isomorphism theorem. □

Note. Let $I \trianglelefteq R$. There exists bijection

$$\begin{aligned}\{\text{ideals in } R/I\} &\leftrightarrow \{\text{ideals in } R \text{ containing } I\} \\ K &\mapsto \{r \in R \mid r + I \in K\} \\ J/I &\leftarrow\!\shortmid J\end{aligned}$$

Theorem (Third Isomorphism Theorem for Rings)**.** Let $I \trianglelefteq R$, $J \trianglelefteq R$ with $I \leq J$. Then $J/I \trianglelefteq R/I$ and

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

Proof. Consider

$$\begin{aligned}\phi : R/I &\to R/J \\ r + I &\mapsto r + J\end{aligned}$$

This is a surjective ring homomorphism (well-defined since $I \leq S$).

$$\ker(\phi) = \{r + I : r \in J\} = J/I \trianglelefteq R/I$$

Apply first isomorphism theorem. □

Example. There is a surjective ring homomorphism $\phi : \mathbb{R}[X] \to \mathbb{C}$

$$f(X) = \sum_{n=1}^{m} a_n X^n \mapsto f(i) = \sum_{n=1}^{m} a_n i^m$$

Proposition 7.1 implies $\ker(\phi) = (X^2 + 1)$. First isomorphism theorem implies $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

Example. R a ring. Then there exists a unique ring homomorphism $i : \mathbb{Z} \to R$ given by

$$\begin{aligned} 0 &\mapsto 0_R \\ 1 &\mapsto 1_R \\ n &\mapsto (\underbrace{1_R + \cdots + 1_R}_{n \text{ times}}) \\ -n &\mapsto -(1_r + \cdots + 1_R) \end{aligned}$$

Since $\ker(i) \trianglelefteq \mathbb{Z}$, have $\ker(i) = n\mathbb{Z}$ for $n \in \{0, 1, 2, \dots\}$. By first isomorphism theorem, $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Im}(i) \le R$.

Definition. We call n the characteristic of R. For example $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ have characteristic 0, and $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}[X]$ have characteristic p.

9. Integral domains, maximal ideals and prime ideals

Definition (Integral Domain and Zero-Divisor)**.** An integral domain is a ring with $0 \neq 1$ such that for $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$. A *zero-divisor* in a ring R is a non-zero element a such that $ab = 0$ for some $0 \neq b \in R$. So an integral domain is a ring with no zero-divisors.

Examples

(i) All fields are integral domains (if $ab = 0$ with $b \neq 0$, multiply by b^{-1} to get $a = 0$)

(ii) Any subring of an integral domain is an integral domain, for example $\mathbb{Z} \le \mathbb{Q}, \mathbb{Z}[i] \le \mathbb{C}$.

(iii) $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain since $(1, 0)(0, 1) = (0, 0)$.

Lemma 9.1. *R an integral domain $\implies$ $R[X]$ an integral domain.*

Proof. Write $f(X) = a_m x^m + \cdots + a_1 X + a_0$, $a_m \neq 0$, $g(X) = b_n X^n + \cdots + b_1 X + b_0$, $b_n \neq 0$. Then
$$f(X)g(X) = a_m b_n X^n + \cdots$$
where $a_m b_n \neq 0$ since R is an integral domain. Thus $\deg(fg) = m + n = \deg(f) + \deg(g)$ and $fg \neq 0$. □

Start of lecture 11

Definition. A polynomial
$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in R[X]$$
if *monic* if $a_n = 1_R$.

Lemma 9.2. *Let R be an integral domain and $0 \neq f \in R[X]$. Let*
$$\mathrm{Roots}(f) = \{a \in R \mid f(a) = 0\}$$
Then $|\mathrm{Roots}(f)| \le \deg(f)$.

Proof. Example Sheet 2. □

Theorem 9.3. Let F be a field. Then any finite subgroup $G \leq (F^\times, \bullet)$ is cyclic.

Proof. G is a finite abelian group. If G not cyclic, then by Theorem 6.4 (structure theorem for finite abelian groups) there exists $H \leq G$ such that $H \cong C_{d_1} \times C_{d_1}$ for some $d_1 \geq 2$. But then the polynomial $f(X) = X^{d_1} - 1 \in F[X]$ has degree d_1 and $\geq d_1^2$ roots, which contradicts Lemma 9.2. □

Example. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Proposition 9.4. Any finite integral domain is a field.

Proof. Let R be a finite integral domain. Let $0 \neq a \in R$. Consider map $\phi : R \to R$, $x \mapsto ax$. If $\phi(x) = \phi(y)$, then $a(x - y) = 0$ therefore $x - y = 0$ (since R is an integral domain and $a \neq 0$), hence $x = y$.

Thus ϕ is injective, and hence surjective since R is finite. Hence there exists $b \in R$ such that $ab = 1$, i.e. a is a unit. Thus R is a field. □

Theorem 9.5 (Field of Fractions Existence)**.** Let R be an integral domain. There exists a field F such that

(i) $R \leq F$.

(ii) Every element of F can be written in the form ab^{-1} where $a, b \in R$ with $b \neq 0$.

F is called the *field of fractions* of R.

Proof. Consider the set $S = \{(a, b) \mid a, b \in R, b \neq 0\}$ and the equivalence relation on S given by

$$(a, b) \sim (c, d) \iff ad - bc = 0$$

Clearly reflexive and symmetric. For transitivity, if $(a, b) \sim (c, d) \sim (e, f)$, then

$$(ad)f = (bc)f = b(cf) = b(de) \implies d(af - be) = 0$$

Since R an integral domain and $d \neq 0$, this gives $af - be = 0$, i.e. $(a, b) \sim (e, f)$. Let $F = S/\sim$ and write $\frac{a}{b}$ for $[(a, b)]$. Define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Can be checked that these operations are well defined and maps F into a ring with $0_F = \frac{0_R}{1_R}$ and $1_F = \frac{1_R}{1_R}$.

If $\frac{a}{b} \neq 0_F$, then $a \neq 0_R$ and $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1_R}{1_R} = 1_F$. So F is a field and

(i) Identify R with subring $\left\{\frac{r}{1_R} : r \in R\right\} \leq F$.

(ii) $\frac{a}{b} = a \cdot b^{-1}$.

□

Example. (i) $\mathbb{Z}$ is an integral domain with field of fractions $\mathbb{Q}$.

(ii) $\mathbb{C}[X]$ has field of fractions $\mathbb{C}(X)$ = field of rational functions in X.

Definition. An ideal $I \trianglelefteq R$ is maximal if $I \neq R$ and if $I \subseteq J \trianglelefteq R$ then $J = I$ or R.

Lemma 9.6. A (non-zero) ring R is a field if and only if its only ideals are $\{0\}$ and R.

Proof. ($\Rightarrow$) If $0 \neq I \trianglelefteq R$, then I contains a unit and hence $I = R$.

($\Leftarrow$) If $0 \neq x \in R$, then the (x) is non-zero hence $(x) = R$ and there exists $y \in R$ such that $xy = 1$, i.e. x is a unit. □

Proposition 9.7. Let $I \trianglelefteq R$ be an ideal. I is maximised if and only if R/I is a field.

Proof.

$$\begin{aligned} R/I \text{ is a field} &\iff I/I \text{ and } R/I \text{ are the only ideals in } R/I \\ &\iff I \text{ and } R \text{ are the only ideals in } R \text{ containing } I \\ &\iff I \trianglelefteq R \text{ is maximal} \end{aligned}$$

□

Definition. An ideal $I \trianglelefteq R$ is prime if $I \neq R$ and whenever $a, b \in R$ with $a, b \in I$, we have $a \in I$ or $b \in I$.

Example. The ideal $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is a prime ideal if and only if $n = 0$ or $n = p$ is a prime number. If $ab \in p\mathbb{Z}$, then $p \mid ab$ so $p \mid a$ or $p \mid b$, so $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. Conversely, if $n = uv$ with $u, v > 1$, then $uv \in n\mathbb{Z}$, but $u \notin n\mathbb{Z}$, $v \notin n\mathbb{Z}$.

Proposition 9.8. Let $I \trianglelefteq R$ be an ideal. Then I is prime if and only if R/I is an integral domain.

Proof.

$$\begin{aligned} I \text{ is prime} &\iff \text{whenever } a, b \in R \text{ with } ab \in I, \text{ we have } a \in I \text{ or } b \in I \\ &\iff \text{whenever } a + I, b + I \in R/I \text{ with } (a + I)(b + I) = 0 + I \\ & \text{ we have } a + I = 0 + I \text{ or } b = 0 + I \\ &\iff R/I \text{ is an integral domain.} \end{aligned}$$

□

Remark. Proposition 9.7 and 9.8 show that I maximal implies I is prime.

Start of lecture 12

Remark. If $\operatorname{char}(R) = n$, then $\mathbb{Z}/n\mathbb{Z} \leq R$. So if R is an integral domain, then $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. Therefore $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ a prime ideal, therefore $n = 0$ or p a prime. In particular, a field has characteristic 0 (and contains $\mathbb{Q}$) or has characteristic p (and contains $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$).

10. Factorisation in integral domains

This section: R is an integral romain.

Definition. (i) $a \in R$ is a unit if there exists $b \in R$ with $ab = 1$ (equivalently $(a) = R$). $R^\times :=$ units in R.

(ii) $a \in R$ divides $b \in R$ (written $a \mid b$) if there exists $c \in R$ such that $b = ac$ (equivalently $(b) \subseteq (a)$).

(iii) $a, b \in R$ are associate if $a = bc$ for some unit $c \in R^\times$ (equivalently $(a) = (b)$, or $a \mid b$ and $b \mid a$).

(iv) $r \in R$ is irreducible if $r \neq 0$, r is not a unit and

$$r = ab \implies a \text{ or } b \text{ is a unit}$$

(v) $r \in R$ is prime if $r \neq 0$, r is not a unit and

$$r \mid ab \implies r \mid a \text{ or } r \mid b$$

Note. These properties depend on ambient ring R. For example:

- 2 is prime and irreducible in $\mathbb{Z}$, but not in $\mathbb{Q}$.
- $2X$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{Z}[X]$.

Lemma 10.1. $(r) \trianglelefteq R$ is a prime ideal if and only if $r = 0$ or is a prime.

Proof. $\Rightarrow$ Suppose (r) is prime and $r \neq 0$. Since prime ideals are proper, $(r) \neq R$, so $r \notin R^\times$. If $r \mid ab$, then $ab \in (r)$ so $a \in (r)$ or $b \in (r)$ hence $r \mid a$ or $r \mid b$, i.e. r is prime.

$\Leftarrow$ $\{0\} \trianglelefteq R$ is a prime ideal since R an integral domain. Let $r \in R$ be a prime. If $ab \in (r)$, then $r \mid ab$ hence $r \mid a$ or $r \mid b$. Hence $a \in (r)$ or $b \in (r)$, i.e. (r) is a prime ideal.

□

Lemma 10.2. If $r \in R$ is prime, then it is irreducible.

Proof. Since r is prime, $r \neq 0$ and $r \notin \mathbb{R}^\times$. Suppose $r = ab$. Then $r \mid ab$ so $r \mid a$ or $r \mid b$. WLOG assume $r \mid a$, so $r = rc$ for some $c \in R$. Then $r = ab = rcb$, therefore $r(1 - bc) = 0$. Then since R is an integral domain and $r \neq 0$, $bc = 1$, i.e. b is a unit. □

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\} \leq \mathbb{C}$ (note $R \cong \mathbb{Z}[X]/(X^2+5)$). R a subring of $\mathbb{C}$, so an integral domain. Define a function $N : R \to \mathbb{Z}_{\geq 0}$, $a+b\sqrt{-5} \mapsto a^2 + 5b^2$ "the norm". Note that $N(z_1 z_2) = N(z_1)N(z_2)$.

Claim. $R^\times = \{\pm 1\}$.

Proof. If $r \in R^\times$, i.e. $rs = 1$ for some $s \in R$. Then $N(r)N(s) = N(1) = 1$ so $N(r) = 1$. But only integer solutions to $a^2 + 5b^2 = 1$ are $(a, b) = (0, 1), (-1, 0)$. □

Claim. $2 \in R$ is irreducible.

Proof. Suppose $2 = rs$, $r, s \in R$. Then $4 = N(2) = N(r)N(s)$. Since $a^2 + 5b^2 = 2$ has no integer solutions R has no elements of norm 2. Thus $N(r) = 1$ and $N(2) = 4$ (or vice versa). But $N(r) = 1$ implies r is a unit (for example $r\overline{r} = 1$). □

By similar reasoning, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are irreducible (as there are no elements of norm 3).

Now $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. Thus $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, but $2 \nmid 1 + \sqrt{-5}$ and $2 \nmid 1 - \sqrt{-5}$ (check by taking norms, $4 \nmid 6$). Thus 2 is *not* prime in R.

Takeaways

(i) Irreducible does not imply prime!

(ii) $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ gives two different factorisations into irreducibles.

Remark. Since $R^\times = \{\pm 1\}$, the irreducibles in (ii) are not associates.

Definition (Principal Ideal Domain)**.** An integral domain R is a principal ideal domain (PID) if every ideal $I \trianglelefteq R$ is principal, i.e. $I = (r)$ for some $r \in R$.

For example, $\mathbb{Z}$ is a PID by Lemma 8.3.

Proposition 10.3. Let R be a PID. Then every irreducible element of R is prime.

Proof. Let $r \in R$ be irreducible and $r \mid ab$, and assume $r \nmid a$. R a PID implies $(a, r) = (d)$ for some $d \in R$. In particular $r = cd$ for some $c \in R$. Since r is irreducible, either c or d is a unit. If c a unit, then $(a, r) = (r)$ so $r \mid a$, contradiction. If d a unit, then $(a, r) = R$. So there exists $s, t \in R$ such that $sa + tr = 1$. Then $b = sab + trb$, and since $r \mid ab$ we have $r \mid b$. Then r is prime. □

Start of lecture 13

Let R be an integral domain.

Lemma 10.4. Let R be a PID and $0 \neq r \in R$. Then r is irreducible $\iff$ (r) is a maximal ideal.

Proof. $\Rightarrow$ $r \notin R^\times$ so $(r) \neq R$. Suppose $(r) \subseteq J \subseteq R$. R a PID implies $J = (a)$ for some $a \in R$. Hence $r = ab$ for some $b \in R$. Since r is irreducible, either $a \in R^\times$ in which case $J = R$ or $b \in R^\times$ in which case $(r) = J$. Thus (r) is maximal.

$\Leftarrow$ $(r) \neq R$ so $r \notin R^\times$. Suppose $r = ab$. Then $(r) \subseteq (a) \subseteq R$. Since (r) is maximal, either $(a) = (r)$ in which case b is a unit, or $(a) = R$ in which case a is a unit. Thus r is irreducible.

□

Remark. (i) Backwards direction holds without assuming R a PID.

(ii) Let R a PID, $0 \neq rR$. Then

$$\begin{aligned}(r) \text{ maximal} &\iff r \text{ irreducible} \\ &\iff r \text{ prime} \\ &\iff (r) \text{ prime}\end{aligned}$$

Thus there exists a bijection

$$\{\text{non-zero prime ideals}\} \leftrightarrow \{\text{non-zero maximal ideals}\}$$

Definition (Euclidean domain)**.** An integral domain is a *Euclidean domain* (ED) if there is a function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ (a Euclidean function) such that:

(i) If $a \mid b$ then $\phi(a) \leq \phi(b)$.

(ii) If $a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ with $a = bq + r$ and either $r = 0$ or $\phi(r) < \phi(b)$.

Example. $\mathbb{Z}$ is an ED with Euclidean function $\phi(n) = |n|$.

Proposition 10.5. If R is a Euclidean domain, then it is a principal ideal doman (ie ED implies PID).

Proof. Let R have Euclidean function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. Let $I \trianglelefteq R$ non-zero. Choose $b \in I \setminus \{0\}$ with $\phi(b)$ minimal, then $(b) \subseteq I$. For $a \in I$, write $a = bq + r$ with $q, r \in R$ and either $r = 0$ or $\phi(r) < \phi(b)$. Since $r = a - bq \in I$, cannot have $\phi(r) < \phi(b)$ by choice of b. Thus $a = bq \in (b)$, and hence $(b) = I$. □

Remark. Only used (ii) here. Property (i) allows us to describe the units in R as

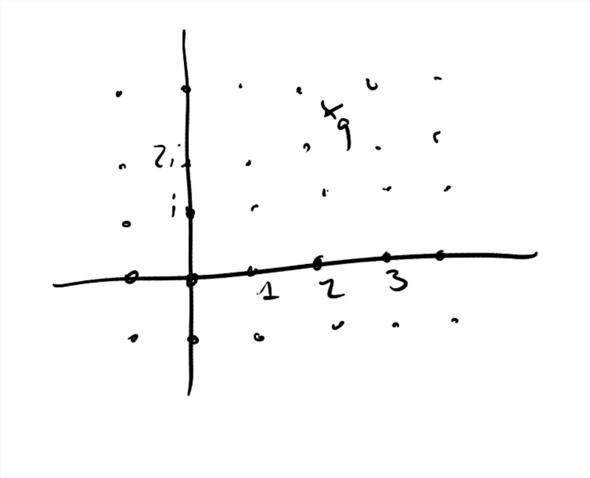
$$R^\times = \{u \in R \setminus \{0\} \mid \phi(u) = \phi(1)\}$$

Example. (i) F a field, $F[X]$ is an ED with Euclidean function $\phi(f) = \deg f$, $f \in F[X]$. (Proposition 7.1)

(ii) $R = \mathbb{Z}[i]$ is an ED with Euclidean function

$$\phi(a + ib) = N(a + ib) = |a + ib|^2 = a^2 + b^2$$

Since $N(z_1 z_2) = N(z_1)N(z_2)$, property (i) holds. For property (ii), let $z_1, z_2 \in \mathbb{Z}[i]$ with $z_2 \neq 0$. Consider $\frac{z_1}{z_2} \in \mathbb{C}$. This has distance less than 1 from the nearest element of $\mathbb{Z}[i]$, i.e. there exists $q \in \mathbb{Z}[i]$ such that $\left|\frac{z_1}{z_2} - q\right| < 1$ $(*)$.



Set $r = z_1 - z_2 q \in \mathbb{Z}[i]$. Then $z_1 = z_2 q + r$ and

$$\phi(r) = |r|^2 = |z_1 - z_2 q|^2 < |z_2|^2 = \phi(z_2)$$

Thus Proposition 10.5 implies that $\mathbb{Z}[i]$ and $F[X]$ for F a field are PIDs.

Example. Let A be an $n \times n$ matrix over a field F. Let $I = \{f \in F[X] : f(A) = 0\}$. If $f, g \in I$, then $(f - g)(A) = f(A) - g(A) = 0 \implies f - g \in I$. If $f \in F[X]$ and $g \in I$, then $(f \cdot g)(A) = f(A) \cdot g(A) = 0 \implies fg \in I$. Thus $I \subseteq F[X]$ is an ideal, and hence $I = (f)$ for some $f \in F[X]$ since $F[X]$ is a PID. May assume f is monic upon mlutiplying by a unit in F. Then for $g \in F[X]$, $g(A) = 0 \iff g \in I \iff g \in (f)$, i.e. $f \mid g$. Thus f is minimal polynomial of A.

Example (Field of order 8)**.** Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Let $f(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$. If $f(X) = g(X)h(X)$ with $g, h \in \mathbb{F}_2[X]$ and $\deg(g), \deg(h) > 0$, then either $\deg(g) = 1$ or $\deg(h) = 1$, and so f has a root. But $f(0) \neq 0$ and $f(1) \neq 0$ (in $\mathbb{F}_2$). Thus f is irreducible. Since $\mathbb{F}_2[X]$ a PID, Lemma 10.4 implies $(f) \trianglelefteq \mathbb{F}_2[X]$ is maximal, henec

$$\mathbb{F}_2[X]/(f) = \{aX^2 + bX + c + (f) \mid a, b, c \in \mathbb{F}_2\}$$

is a field of order 8.

Start of lecture 14

Example. $\mathbb{Z}[X]$ is not a PID. Consider $I = (2, X) \trianglelefteq \mathbb{Z}[X]$. Then

$$\begin{aligned} I &= \{2f_1(X) + Xf_2(X) : f_1, f_2 \in \mathbb{Z}[X]\} \\ &= \{f \in \mathbb{Z}[X] : f(0) \text{ if even}\} \end{aligned}$$

Suppose $I = (f)$ for some $f \in \mathbb{Z}[X]$. Then $2 = fg$ for some $g \in \mathbb{Z}[X]$. Thus $\deg(f) = \deg(g) = 0$ and $f \in \mathbb{Z}$. Hence $f = \pm 1$ or ± 2. Thus $I = \mathbb{Z}[X]$ or $2\mathbb{Z}[X]$. The first case is a contradiction since $1 \notin I$, and the second is a contradiction since $X \in I$.

Definition. An integral domain is a unique factorisation domain (UFD) if

(i) Every non-zero, non-unit is a product of irreducibles.

(ii) If $p_1 \cdots p_m = q_1 \cdots q_n$ where p_i, q_i are irreducibles, then $m = n$ and we can reorder so that p_i is an associate of q_i for all $i = 1, \ldots, n$.

Goal: PID $\implies$ UFD.

Proposition 10.6. Let R be an integral domain satisfying (i) in definition of UFD. Then R is a UFD if and only if every irreducible is prime.

Proof. $\Rightarrow$ Suppose $p \in R$ is irreducible and $p \mid ab$. Then $ab = pc$ for some $c \in R$. Writing a, b, c as products of irreducibles, it follows from (ii) that $p \mid a$ or $p \mid b$. Thus p is prime.

$\Leftarrow$ Suppose $p_1 \cdots p_m = q_1 \cdots q_n$ with each p_i and q_i irreducible. Since p_1 is prime and $p_1 \mid q_1 \cdots q_n$, we have $p_1 \mid q_i$ for some i. Upon reordering, we may assume $p_1 \mid q_1$, i.e. $q_1 = up_1$ for some $u \in R$. But q_1 is irreducible and p_1 not a unit, so u is a unit. Thus p_1 and q_1 are associates. Cancelling p_1 gives $p_2 \cdots p_m m = (uq_2) \cdots q_n$. Result then follows by induction. □

Lemma 10.7. Let R be a PID and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ a nested sequence of ideals. Then $\exists N \in \mathbb{N}$ such that $I_n = I_{n+1}$ for all $n \geq N$. (Rings satisfying the "ascending chain condition" are called Noetherian – more later).

Proof. Let $I = \bigcup_{i=1}^{\infty} I_i$. This is an ideal in R. (See Example Sheet 2). Since R is a PID, we have $I = (a)$ for some $a \in R$. Then $(a) = \bigcup_{i=1}^{\infty} I_i$, so $a \in I_N$ for some N. Then for any $n \geq N$ we have

$$(a) \subseteq I_N \subseteq I_n \subseteq I = (a)$$

and so $I_n = I$. □

Theorem 10.8. If R is a principal ideal domain, then it is a unique factorisation domain. (i.e. PID implies UFD).

Proof. (i) Let $0 \neq x \neq R$, not a unit. Suppose x is not a product of irreducibles. Then x not irreducible, so can write $x = x_1 y_1$ where x_1, y_1 are not units. Then either x_1 or y_1 is not a product of irreducibles, say x_1. We have $(x) \subseteq (x_1)$ and inclusion is strict since y_1 not a unit. Now write $x_1 = x_2 y_2$ where x_2, y_2 are not units. Repeat this procedure to get

$$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$$

contradicting Lemma 10.7.

(ii) By proposition 10.6, suffices to show irreducibles are prime. Conclude by Proposition 10.3. □

Examples

	ED	$\Longrightarrow$	PID	$\Longrightarrow$	UFD	$\Longrightarrow$	Integral Domain
$\mathbb{Z}/4\mathbb{Z}$	✗		✗		✗		✗
$\mathbb{Z}[\sqrt{-5}]$	✗		✗		✗		✓
$\mathbb{Z}[X]$	✗		✗		✓		✓
$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$	✗		✓		✓		✓
$\mathbb{Z}[i]$	✓		✓		✓		✓

Definition. R an integral domain.

(i) $d \in R$ is a greatest common divisor of $a_1, \ldots a_n \in R$ (written $d = \gcd(a_1, \ldots, a_n)$) if $d \mid a_i$ for all i and if $d' \mid a_i$ for all i, then $d' \mid d$.

(ii) $m \in R$ is a least common multiple of $a_1, \ldots, a_n \in R$ (written $m = \operatorname{lcm}(a_1, \ldots, a_n)$) if $a_i \mid m$ for all i and if $a_i \mid m'$ for all i, then $m \mid m'$.

Both gcd's and lcm's (when they exist) are unique up to associates.

Proposition 10.9. In a UFD, both lcm's and gcd's exist.

Proof. Write $a_i = u_i \prod_j p_j^{n_{ij}}$ for all $1 \le i \le n$, where u_i is a unit, the p_i are irreducible which are *not* associates of each other, and $n_{ij} \in \mathbb{Z}_{\ge 0}$.

We claim that $d = \prod_j p_j^{m_j}$ where $m_f = \min_{1 \le i \le n} n_{ij}$ is the gcd of $a_1, \dots, a_n$. Certainly $d \mid a_i$ for all i. If $d' \mid a_i$ for all i, then $d' = u \prod_j p_j^{t_j}$, we find $t_j \le n_{ij}$ for all j so $t_j \le m_j$. Therefore $d' \mid d$. The argument for lcm's is similar. $\square$

Start of lecture 15

11. Factorisation in Polynomial Rings

Goal of this lecture:

Theorem 11.1. If R is a UFD then $R[X]$ is a UFD.

In this section: R is a UFD with field of fractions F. We have $R[X] \leq F[X]$.

Moreover $F[X]$ is an ED hence a PID and a UFD.

Definition. The *content* of $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ is

$$c(f) = \gcd(a_0, a_1, \ldots, a_n)$$

(well-defined up to multiplication by a unit). We say f is *primitive* if $c(f)$ is a unit.

Lemma 11.2. (i) If $f, g \in R[X]$ are primitive, then fg is also primitive.

(ii) If $f, g \in R[X]$, then $c(fg) = c(f)c(g)$ (equality is up to units).

Proof. (i) Let $f = a_n X^n + \cdots + a_1 X + a_0$, $g = b_m X^m + \cdots + b_1 X + b_0$. If fg is not primitive, $c(fg)$ is not a unit, so there is some prime p such that $p \mid c(fg)$. Since f, g primitive, $p \nmid c(f)$ and $p \nmid c(g)$. Suppose $p \mid a_0$, $p \mid a_1$, …, $p \nmid a_k$, $p \mid b_0$, $p \mid b_1$, …, $p \nmid b_l$. Then the coefficient of X^{k_l} in fg is

$$\sum_{i+j=k+1} a_i b_j = \underbrace{\cdots + a_{k-1} b_{l-1}}_{\text{divisible by } p} + a_k b_l + \underbrace{a_{k-1} b_{l-1} + \cdots}_{\text{divisible by } p}$$

Note that the LHS is divisible by p, hence $p \mid a_k b_l$ so $p \mid a_k$ or $p \mid b_l$, contradiction.

(ii) Write $f = c(f) f_0$ and $c(g) g_0$ where $f_0, g_0 \in R[X]$ primitive. Then

$$fg = c(f)c(g) f_0 g_0$$

where $f_0 g_0$ is primitive by (i). Hence $c(fg) = c(f)c(g)$ (up to a unit).

□

Corollary 11.3. Let $p \in R$ be prime. Then p is prime in $R[X]$.

Proof. $R[X]^\times = R^\times$, so p is not a unit in $R[X]$. Let $f \in R[X]$. Then $p \mid f$ in $R[X]$ if and only if $p \mid c(f)$ in R. Thus if $p \mid gh$ in $R[X]$, we have

$$\begin{aligned} p \mid c(gh) = c(g)c(h) &\implies p \mid c(g) \text{ or } c(h) \text{ in } R \\ &\implies p \mid g \text{ or } p \mid h \text{ in } R[X], \text{ i.e. } p \text{ prime in } R[X]. \end{aligned}$$

□

Lemma 11.4. Let $f, g \in R[X]$ with g primitive. If $g \mid f$ in $F[X]$, then $g \mid f$ in $R[X]$.

Proof. Let $f = gh$, $h \in F[X]$. Let $a \in R$ such that $ah \in R[X]$ ("clear denominators"), and write $ah = c(ah)h_0$, $af = c(ah)h_0 g$ with h_0 primitive, and hence $h_0 g$ primitive. Taking contents, we find that $a \mid c(ah)$. Thus $h \in R[X]$ and $g \mid f$ in $R[X]$. □

Lemma (Gauss's Lemma)**.** Let $f \in R[X]$ be primitive. Then f irreducible in $R[X]$ implies f irreducible in $F[X]$.

Proof. Since $f \in R[X]$ is irreducible and primitive, we have $\deg(f) > 0$, and so f not a unit in $F[X]$. Suppose that f is *not* irreducible in $F[X]$, say $f = gh$, where $g, h \in F[X]$ with $\deg(g), \deg(h) > 0$. Let $\lambda \in F^\times$ such that $\lambda^{-1} g \in R[X]$ is primitive. (For example, let $0 \neq b \in R$ such that $bg \in R[X]$. Then $bg = c(bg)g_0$ with g_0 primitive. So can take $\lambda = \frac{c(bg)}{b} \in F^\times$).

Upon replacing g by $\lambda^{-1} g$ and h by λh, may assume $g \in R[X]$ primitive. Then Lemma 11.4 implies $h(X) \in R[X]$ and so $f = gh$ in $R[X]$, $\deg(g), \deg(h) > 0$, contradiction. □

Remark. We'll see "$\Leftarrow$" also holds.

Lemma 11.5. Let $g \in R[X]$ be primitive. Then g is prime in $F[X]$ implies g prime in $R[X]$.

Proof. Suppose $f_1, f_2 \in R[X]$ and $g \mid f_1 f_2$ in $R[X]$. g prime in $F[X]$ implies $g \mid f_1$ or $g \mid f_2$ in $F[X]$ hence by Lemma 11.4, $g \mid f_1$ or $g \mid f_2$ in $R[X]$, i.e. g prime in $R[X]$. □

Now we can finally prove Theorem 11.1:

Proof of Theorem 11.1. Let $f \in R[X]$. Write $f = c(f) f_0$ with $f_0 \in R[X]$ primitive. R a UFD implies $c(f)$ a product of irreducibles in R (which are irreducible in $R[X]$). If f_0 not irreducible, say $f_0 = gh$, then $\deg(g), \deg(h) > 0$ since f_0 primitive, and g, h primitive.

By induction on degree, f_0 a product of irreducibles in $R[X]$ – establishes (i) in definition of UFD. By Proposition 10.6, suffices to show that if $f \in R[X]$ is irreducible, then f is prime. Write $f = c(f) f_0$, $f_0 \in R[X]$ primitive. Then f irreducible implies f constant or primitive.

- Case f constant: f irreducible in $R[X]$ implies f irreducible in R, hence prime in R (since UFD), hence f prime in $R[X]$ by Corollary 11.3.
- Case f primitive: f irreducible in $R[X]$ implies f irreducible in $F[X]$ (Gauss's Lemma), hence f prime in $F[X]$ ($F[X]$ an ED hence UFD), hence f prime in $R[X]$ by Lemma 11.5. □

Remark. By Lemma 10.2, the three implications in the f primitive case are actually equivalences.

Start of lecture 16

Example. (i) Theorem 11.1 implies $\mathbb{Z}[X]$ is a UFD.

(ii) Let $R[X_1, \dots, X_n]$ be the polynomial ring in $X_1, \dots, X_n$ with coefficients in R. (Define inductively $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$). Applying Theorem 11.1 inductively implies $R[X_1, \dots, X_n]$ is a UFD if R is as UFD.

Theorem (Eisenstein's Criterion)**.** Let R be a UFD and $f(X) = a_nX^n + \cdots + a_1X + a_0 \in R[X]$ primitive. Suppose $\exists p \in R$ irreducible (= prime) such that

- $p \nmid a_n$
- $p \mid a_i \ \forall 0 \le i \le n-1$
- $p^2 \nmid a_0$

Then f is irreducible in $R[X]$.

Proof. Suppose $f = gh$, $g, h \in R[X]$ not units. f primitive implies $\deg(g), \deg(h) > 0$. Let $g = r_kX^k + \cdots + r_1X + r_0$, $h = s_lX^l + \cdots + s_1X + s_0$ with $k + l = m$. Then $p \nmid a_n = r_ks_l$ so $p \nmid r_k$ and $p \nmid s_l$, and $p \mid a_0 = r_0s_0$ so $p \mid r_0$ or $p \mid s_0$. WLOG $p \mid r_0$. Then there exists $j \le k$ such that $p \mid r_0$, $p \mid r_1$, …, $p \mid r_{j-1}$, $p \nmid r_j$. Then

$$a_j = \underbrace{r_0s_j + r_1s_{j-1} + \cdots + r_{j-1}s_1}_{\text{divisible by } p} + r_js_o$$

but p divides a_j since $j < n$, thus $p \mid r_js_0$, hence $p \mid s_0$. Then $p^2 \mid r_0s_0 = a_0$, contradicting the third assumption. □

Example. (i) $f(X) = X^3 + 2X + 5 \in \mathbb{Z}[X]$. If f irreducible in $\mathbb{Z}[X]$, then

$$f(X) = (x + a)(X^2 + bX + c)$$

for some $a, b, c \in \mathbb{Z}$. Thus $ac = 5$. But ± 1, ± 5 are not roots of f, contradiction. By Gauss's Lemma, f irreducible in $\mathbb{Q}[X]$. Thus $\mathbb{Q}[X]/(f)$ is a field (Lemma 10.4).

(ii) Let $p \in \mathbb{Z}$ be a prime. Eisenstein's criterion implies $x^n - p$ is irreducible in $\mathbb{Z}[X]$, have irreducible in $\mathbb{Q}[X]$ by Gauss's Lemma.

(iii) Let $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ where p is prime. Eisenstein does not apply directly to f. But note that $f(X) = \frac{X^p - 1}{X - 1}$. Substituting $Y = X - 1$ gives

$$f(Y + 1) = \frac{(Y + 1)^p - 1}{(Y + 1) - 1} = Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{p-2} Y + \binom{p}{p-1}$$

Now $p \mid \binom{p}{i}$ for all $1 \le i \le p-1$ and $p^2 \nmid \binom{p}{p-1} = p$. Thus $f(Y+1)$ is irreducible in $\mathbb{Z}[Y]$, so $f(X)$ is irreducible in $\mathbb{Z}[X]$ (because if it did have a factorisation then we could construct a factorisation of $f(Y + 1)$).

12. Algebraic Integers

Recall $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$ – ring of Gaussian integers. Norm $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$, $a + ib \mapsto a^2 + b^2$ with $N(z_1) = N(z_1)N(z_2)$ is a Euclidean function. Thus $\mathbb{Z}[i]$ is a Euclidean Domain, hence PID and UFD, and so $\boxed{\text{primes} = \text{irreducibles}}$ in $\mathbb{Z}[i]$. The units in $\mathbb{Z}[i]$ are ± 1, $\pm i$.

Example. (i) $2 = (1 + i)(1 - i)$ and $5 = (2 + i)(2 - i)$ are not primes in $\mathbb{Z}[i]$.

(ii) $N(3) = 9$ so if $3 = ab$ in $\mathbb{Z}[i]$ then $N(a)N(b) = 9$. But $\mathbb{Z}[i]$ has no elements of norm 3. Thus a or b is a unit, hence 3 is a prime in $\mathbb{Z}[i]$. Similarly 7 is prime.

Proposition 12.1. Let $p \in \mathbb{Z}$ be a prime number. Then the following are equivalent:

(i) p is not prime in $\mathbb{Z}[i]$.

(ii) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

(iii) $p = 2$ or $p \equiv 1 \pmod 4$.

Proof.

(i) $\implies$ (ii) Let $p = xy$, $x, y \in \mathbb{Z}[i]$ not units. Then $p^2 = N(p) = N(x)N(y)$, $N(x), N(y) > 1$. Thus $N(x) = N(y) = p$. Writing $x = a + ib$ gives $p = N(x) = a^2 + b^2$.

(ii) $\implies$ (iii) The squares modulo 4 are 0 and 1. Thus if $p = a^2 + b^2$, then $p \not\equiv 3 \pmod 4$.

(iii) $\implies$ (i) Already saw 2 not prime in $\mathbb{Z}[i]$. Assume $p \equiv 1 \pmod 4$. By Theorem 9.3, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4, i.e. there exists $x \in \mathbb{Z}$ with $x^a \equiv 1 \pmod p$ but $x^2 \not\equiv 1 \pmod p$. Thus $x^2 \equiv -1 \pmod p$. Now $p \mid x^2 + 1 = (x + i)(x - i)$ but $p \nmid x + i$ and $p \nmid x - i$. Thus p not prime. □

Theorem 12.2. The primes in $\mathbb{Z}[i]$ (up to associates) are

(i) $a + ib$, where $a, b \in \mathbb{Z}$ and $a^2 + b^2 = p$ a prime number with $p = 2$ or $p \equiv 1 \pmod 4$.

(ii) Prime numbers $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$.

Proof. First we check these are primes.

(i) $N(a+ib)=p$. If $a+ib=uv$ then either $N(u)=1$ or $N(v)=1$. Thus $a+ib$ is irreducible, hence prime.

(ii) Proposition 12.1, now let $z \in \mathbb{Z}[i]$ prime (= irreducible). Then $\overline{z} \in \mathbb{Z}[i]$ is also irreducible and $N(z) = z\overline{z}$ is a factorisation into irreducibles. Let $p \in \mathbb{Z}$ be a prime number dividing $N(z)$. If $p \equiv 3 \pmod 4$, then p is prime in $\mathbb{Z}[i]$. Thus $p \mid z$ or $p \mid \overline{z}$, so p is an associate of z or $\overline{z}$. Hence p is an associate of z. Otherwise, $p = 2$ or $p \equiv 1 \pmod 4$ and $P = a^2+b^2 = (a+ib)(a-ib)$, $a, b \in \mathbb{Z}$. Then $(a+ib)(a-ib) \mid z\overline{z}$. Thus z is an associate of $a+ib$ or $a-ib$ by uniqueness of factorisation. □

Start of lecture 17

Remark. In Theorem 12.2, if $p = a^2+b^2$, $a+bi$ and $a-bi$ are not associates unless $p = 2$ ($(1+i) = (1-i)i$).

Corollary 12.3. An integer $n \geq 1$ is the sum of 2 squares if and only if every prime factor p of n with $p \equiv 3 \pmod 4$ divides n to an even power.

Proof.

$$\begin{aligned} n = a^2+b^2 &\iff n = N(x) \text{ for some } x \in \mathbb{Z}[i] \\ &\iff n \text{ a product of norms of primes in } \mathbb{Z}[i] \end{aligned}$$

Theorem 12.2 implies that norms of primes in $\mathbb{Z}[i]$ are the primes $p \in \mathbb{Z}$ with $p \not\equiv 3 \pmod 4$ and squares of primes $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$. □

Example. $65 = 5 \cdot 13$. Factoring into primes in $\mathbb{Z}[i]$ gives

$$\begin{aligned} 5 &= (2+i)(2-i) \\ 13 &= (2+3i)(2-3i) \end{aligned}$$

Thus $65 = (2+i)(2+3i)\overline{(2+i)(2+3i)}$, i.e.

$$\begin{aligned} 65 &= N((2+i)(2+3i)) \\ &= N(1+8i) \\ &= 1^2+8^2 \end{aligned}$$

But also have

$$\begin{aligned} 65 &= N((2+i)(2-3i)) \\ &= N(7-4i) \\ &= 7^2+4^2 \end{aligned}$$

Definition. (i) $\alpha \in \mathbb{C}$ is an algebraic number if there exists non-zero $f \in \mathbb{Q}[X]$ with $f(\alpha) = 0$.

(ii) $\alpha \in \mathbb{C}$ is an algebraic integer if there exists monic $f \in \mathbb{Z}[X]$ with $f(\alpha) = 0$.

Notation. Let R be a subring of S, and $\alpha \in S$. We write $R[\alpha]$ for the smallest subring of S containing R and α, i.e. if

$$\phi : R[X] \to S, \qquad g(X) \mapsto g(\alpha)$$

then $R[\alpha] = \mathrm{Im}(\phi)$.

Let α be an algebraic number and let $\phi : \mathbb{Q}[X] \to \mathbb{C}$, $g(X) \mapsto g(\alpha)$. ($\mathrm{Im}(\phi) = \mathbb{Q}[\alpha]$). $\mathbb{Q}[X]$ is a PID hence $\ker(\phi) = (f)$ for some $f \in \mathbb{Q}[X]$. Then $f \neq 0$, since α an algebraic number. Upon multiplying f by a unit, may assume f is monic.

Definition. f is the *minimal polynomial* of α. By isomorphism theorem, $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha] \leq \mathbb{C}$. Thus $\mathbb{Q}[\alpha]$ an integral domain, hence f irreducible in $\mathbb{Q}[X]$ (hence $\mathbb{Q}[\alpha]$ is a field).

Proposition 12.4. Let α be an algebraic integer, and $f \in \mathbb{Q}[X]$ its minimal polynomial. Then $f \in \mathbb{Z}[X]$ and $(f) = \ker(\theta)$, where $\theta : \mathbb{Z}[X] \to \mathbb{C}$ is the map $g(X) \mapsto g(\alpha)$.

Proof. Let $\lambda \in \mathbb{Q}^\times$ such that $\lambda f \in \mathbb{Z}[X]$ is primitive. Then $\lambda f(\alpha) = 0$, so $\lambda f \in \ker(\theta)$. Let $g \in \ker(\theta) \trianglelefteq \mathbb{Z}[X]$. Then $g \in \ker(\phi)$ and hence $\lambda f \mid g$ in $\mathbb{Q}[X]$. Then by Lemma 11.4, $\lambda f \mid g$ in $\mathbb{Z}[X]$. Thus $\ker(\theta) = (\lambda f)$. Now α is an algebraic integer, hence there exists $g \in \ker(\theta)$ monic. Then $\lambda f \mid g$ in $\mathbb{Z}[X]$ hence $\lambda = \pm 1$. Hence $f \in \mathbb{Z}[X]$, and $(f) = \ker(\theta)$. $\square$

Let $\alpha \in \mathbb{C}$ an algebraic integer. Applying isomorphism theorem to θ gives $\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha]$. Examples: i, $\sqrt{2}$, $\frac{-1+\sqrt{3}}{2}$, $\sqrt[n]{p}$ have minimal polynomials X^2+1, X^2-2, X^2+X+1, $X^n - p$. Hence

$$\mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[i], \qquad \mathbb{Z}[X]/(X^2-2) \cong \mathbb{Z}[\sqrt{2}]$$

etc.

Corollary 12.5. If α is an algebraic integer and $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$.

Proof. Let α be an algebraic integer. Then minimal polynomial has coefficients in $\mathbb{Z}$. $\alpha \in \mathbb{Q}$ implies minimal polynomial is $X - \alpha$, and so $\alpha \in \mathbb{Z}$. $\square$

13. Noetherian Rings

We showed that any PID R satisfies the ascending chain condition (ACC): If $I_1 \subseteq I_2 \subseteq \cdots$ are ideals in R, then there exists $N \in \mathbb{N}$ such that $I_n = I_{n+1}$ for all $n \geq N$. More generally:

Lemma 13.1. Let R be a ring.

$$R \text{ satisfies ACC} \iff \text{All ideals in } R \text{ are finitely generated}$$

Proof. $\Leftarrow$ Let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals and $I = \bigcup_{n\geq 1} I_n$, which is again an ideal. By assumption $I = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_m \in R$. These elements belong to a nested union, so there exists $N \in \mathbb{N}$ such that $a_1, \ldots, a_m \in I_N$. Then for $n \geq N$,

$$(a_1, \ldots, a_m) \subseteq I_N \subseteq I_N \subseteq I = (a_1, \ldots, a_m)$$

so $I_n = I_N$.

$\Rightarrow$ Assume $J \trianglelefteq R$ not finitely generated. Choose $a_1 \in J$. Then $J \neq (a_1)$, so can choose $a_2 \in J \setminus (a_1)$. Then $J \neq (a_1, a_2)$, so choose $a_3 \in J \setminus (a_1, a_2)$. Continuing this process we obtain a chain of ideals

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots$$

with strict inclusions, which contradicts ACC.

□

Definition (Noetherian Ring)**.** A ring is called *Noetherian* if it satisfies the Ascending Chain Condition.

Start of lecture 18

Theorem (Hilbert's Basis Theorem)**.** If R is a Noetherian ring, then $R[X]$ is also Noetherian.

Proof. Assume $J \trianglelefteq R[X]$ is not finitely generated. Choose $f_1 \in J$ of minimal degree. Then $(f_1) \subsetneq J$. Choose $f_2 \in J \setminus (f_1)$ of minimal degree. Then $(f_1, f_2) \subsetneq J$. Choose $f_3 \in J \setminus (f_1, f_2)$ of minimal degree and so on. We obtain a sequence $f_1, f_2, \ldots$ with $\deg f_i \leq \deg f_{i+1}$. Set $a_i :=$ leading coefficient of f_i. We obtain $(a_1) \subseteq (a_1, a_2) \subseteq \cdots$, a chain of ideals in R. Since R is Noetherian, there exists $m \in \mathbb{N}$ such that $a_{m+1} \in (a_1, \ldots, a_m)$. Let $a_{m+1} = \sum_{i=1}^m \lambda_i a_i$, $\lambda_i \in R$ and set

$$g = \sum_{i=1}^{m} \lambda_i f_i X^{\deg f_{m-1} - \deg f_i} \in (f_1, \ldots, f_m)$$

Then $\deg f_{m+1} = \deg g$ and they have the same leading coefficient a_{m+1}. Then $f_{m+1} - g \in J$ and $\deg(f_{m+1} - g) < \deg f_{m+1}$. Hence by minimality of degree of f_{m+1}, we must have $f_{m+1} - g \in (f_1, \ldots, f_m)$. But $g \in (f_1, \ldots, f_m)$, hence $f_{m+1} \in (f_1, \ldots, f_m)$, contradiction. Thus J is finitely generated, so $R[X]$ is Noetherian by Lemma 13.1. □

Corollary.

- $\mathbb{Z}[X_1, \ldots, X_n]$ is Noetherian.
- $F[X_1, \ldots, X_n]$ Noetherian, F a field.

Examples

Let $R = \mathbb{C}[X_1, \ldots, X_n]$. Let $V \subseteq \mathbb{C}^n$ be a subset of the form

$$\{(a_1, \ldots, a_n) \mid f(a_1, \ldots, a_n) = 0, \forall f \in \mathcal{F}\}$$

where $\mathcal{F} \subset R$ is a possibly infinite set of polynomials. Let

$$I = \left\{ \sum_{i=1}^{m} \lambda_i f_i \mid m \in \mathbb{N}, \lambda_i \in R, f_i \in \mathcal{F} \right\}$$

Then $I \trianglelefteq R$, so $I = (g_1, \ldots, g_r)$, $g_i \in I$ (since R Noetherian). Thus

$$V = \{(a_1, \ldots, a_n) \mid g_i(a_1, \ldots, a_n) = 0, i = 1, \ldots, n\}$$

i.e. V is defined by finitely many polymonials.

Lemma 13.2. Let R be a Noetherian ring and $I \trianglelefteq R$. Then R/I is Noetherian.

Proof. Let $J_1' \subseteq J_2' \subseteq \cdots$ a chain of ideals in R/I. By the ideal correspondence we have $J_i' = J_i/I$ for some $J_1 \subseteq J_2 \subseteq \cdots$ a chain of ideals in R (containing I). R Noetherian implies there exists $N \in \mathbb{N}$ such that $J_n = J_{n+1}$ for all $n \geq N$, hence $J_n' = J_{n+1}$ for all $n \geq N$. Thus R/I is Noetherian. □

Examples

(i) $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2 + 1)$ is Noetherian.

(ii) $R[X]$ Noetherian implies $R[X]/X$ is Noetherian.

Examples of non-Noetherian Rings

(i) $R = \mathbb{Z}[X_1, X_2, \ldots] = \bigcup_{n \geq 1} \mathbb{Z}[X_1, \ldots, X_n]$. i.e. polynomials in countably many variables. But $(X_1) \subseteq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots$ is an infinite ascending chain, so R is not Noetherian.

(ii) $R = \{f \in \mathbb{Q}[X] : f(0) \in \mathbb{Z}\} \leq \mathbb{Q}[X]$. But:

$$(X) \subsetneq \left(\frac{1}{2}X\right) \subsetneq \left(\frac{1}{4}X\right) \subsetneq \left(\frac{1}{8}X\right) \subsetneq \cdots$$

(each inclusion is strict because $2 \in R$ is not a unit).

Chapter III

Modules

Contents

14. Modules

Definition (Module)**.** Let R be a ring. A module over R is a triple $(M, +, \cdot)$ consisting of a set M and two operations

$$+ : M \times M \to M, \qquad \cdot : R \times M \to M$$

such that

(i) $(M, +)$ is an abelian group, say with identity 0 $(=0_M)$.

(ii) The operation $\cdot$ satisfies:

$$\begin{aligned} (r_1 + r_2) \cdot m &= r_1 \cdot m + r_2 \cdot m && \forall r_1, r_2 \in R, m \in M \\ r \cdot (m_1 + m_2) &= r \cdot m_1 + r \cdot m_2 && \forall r \in R, m_1, m_2 \in M \\ r_1 \cdot (r_2 \cdot m) &= (r_1 \cdot r_2) \cdot m && \forall r_1, r_2 \in R, m \in M \\ 1_R \cdot m &= m && \forall m \in M \end{aligned}$$

Remark. Don't forget closure when checking $+, \cdot$ well-defined.

Example. (i) Let $R = F$ be a field. Then an F-module is *precisely the same* as a vector space over F.

(ii) $R = \mathbb{Z}$, a $\mathbb{Z}$-module is *precisely the same* as an abelian group, where $\cdot : \mathbb{Z} \times A \to A$ maps

$$(n, a) \mapsto \begin{cases} \overbrace{a + a + \cdots + a}^{n \text{ copies}} & n > 0 \\ 0 & n = 0 \\ -(\underbrace{a + a + \cdots + a}_{n \text{ copies}}) & n < 0 \end{cases}$$

(iii) F a field, V a vector space over F and $\alpha : U \to V$ a linear map. We can make V an $F[X]$-module via

$$\cdot : F[X] \times V \to V \qquad (fv) \mapsto (f(\alpha)(v))$$

for example $(X^2 +!) \cdot v = (\alpha^2 + 1_V)(v)$.

Note. Different choices of α make V into different $F[X]$-modules. Sometimes we'll write $V = V_\alpha$ to make this clear.

Examples

General construction.

(i) For any ring R, R^n is an R-module via $r \cdot (r_1, \dots, r_n) = (r_1, \dots, rr_n)$. In particular, taking $n = 1$, R is an R-module.

(ii) If $I \trianglelefteq R$, then I is an R-module (restrict the usual multiplication on R) and R/I is an R-module via

$$r \cdot (s + I) = rs + I$$

(iii) $\phi : R \to S$ a ring homomorphism, then any S-module M may be regarded as an R-module:

$$R \times M \to M \qquad (r, m) \mapsto \phi(r) \cdot m$$

In particular, if $R \leq S$ then any S-module may be viewed as an R-module.

Start of lecture 19

Definition. M an R-module. $N \subset M$ is an R-submodule (written $N \leq M$) if it is a subgroup of $(M, +)$ and $r \cdot n \in N$ for all $r \in R$, $n \in N$.

Examples

(i) A subset of R is an R-submodule *precisely* when it is an ideal.

(ii) When $R = F$ is a field, module $\equiv$ vector space, submodule $\equiv$ vector subspace.

Definition. If $N \leq M$ an R-submodule, the quotient M/N is the quotient of groups under $+$ with

$$r \cdot (m + N) = rm + N$$

This is well-defined, and makes M/N an R-module.

Definition. Let M, N be R-modules. A function $f : M \to N$ is an *R-module homomorphism* if it is a homomorphism of abelian groups and

$$f(r \cdot m) = r \cdot f(m) \qquad \forall r \in R, m \in M$$

Theorem (First isomorphism theorem)**.** Let $f : M \to N$ be an R-module homomorphism. Then

- $\ker(f) := \{m \in M \mid f(m) = 0\} \leq M$
- $\mathrm{Im}(f) := \{f(m) \in N \mid m \in M\} \leq N$

and $M/\ker(f) \cong \mathrm{Im}(f)$.

Proof. Similar to before. □

Theorem (Second isomorphism theorem)**.** Let $A, B \leq M$ be submodules. Then

$$A + B = \{a + b \mid a \in A, b \in B\} \leq M$$

$$A \cap B \leq M$$

and

$$A/(A \cap B) \cong (A + B)/B$$

Proof. Apply first isomorphism theorem to the composite $A \hookrightarrow M \hookrightarrow M/B$. □

For third isomorphism theorem, note that there exists bijection

$$\{\text{submodules of } M/N\} \leftrightarrow \{\text{submodules of } M \text{ containing } N\}$$

Theorem (Third isomorphism theorem)**.** If $N \leq L \leq M$ are R-submodules of M, then

$$\frac{M/N}{L/N} \cong M/L$$

In particular, these apply to vector spaces (compare with results from Linear Algebra).

Let M be an R-module. If $m \in M$, write $R_m = \{rm \in M \mid r \in R\}$ – submodule generated by m. If $A, B \leq M$, write

$$A + B = \{a + b \mid a \in A, b \in B\} \leq M$$

Definition.

- M is cyclic if there exists $m \in M$ such that $M = R_m$.
- M is finitely generated if there exists $m_1, \dots, m_n \in M$ such that

$$M = R_{m_1} + R_{m_2} + \cdots + R_{m_n}$$

Lemma 14.1. M is cyclic if and only if $M \cong R/I$ for some $I \trianglelefteq R$.

Proof. $\Rightarrow$ Suppose $M = R_m$. Then there is a surjective R-module homomorphism $R \to M$, $r \mapsto rm$. Its kernel is an R-submodule of R, i.e. an ideal. Then first isomorphism theorem gives $R/I \cong M$.

$\Leftarrow$ R/I is generated as an R-module by $1_R + I$. □

Lemma 14.2. M finitely generated if and only if there exists a surjective R-module homomorphism $f : R^n \to M$ for some n.

Proof. $\Rightarrow$ If $M = R_{m_1} + R_{m_2} + \cdots + R_{m_n}$ define $f : R^n \to M$, $(r_1, \ldots, r_n) \mapsto \sum_{i=1}^n r_i m_i$ a surjective R-module homomorphism.

$\Leftarrow$ Let $e_i = (0, \ldots, 1, \ldots, 0) \in R^n$. (1 is in the i-th place). Given f, let $m_i := f(e_i) \in M$. Then any $m \in M$ is of the form

$$\begin{aligned} f(r_1, \ldots, r_n) &= f\left(\sum_{i=1}^n r_i e_i\right) \\ &= \sum_{i=1}^n r_i f(e_i) \\ &= \sum_{i=1}^n r_i m_i \end{aligned}$$

Thus $M = Rm_1 + \cdots + Rm_n$. □

Corollary 14.3. Let $N \leq M$ be an R-submodule. If M is finitely generated, then M/N is finitely generated.

Proof. Let $f : R^n \to M$ be a surjective R-module homomorphism. Then $R^n \to M \to M/N$ is a surjective R-module homomorphism. □

Example (Counter-example)**.** A submodule of a finitely generated module need not be finitely generated. Let R be a non-Noetherian ring and $I \trianglelefteq R$ a non-finitely generated ideal. Then R is a finitely generated R-module and I is a submodule which is not finitely generated.

Remark. A submodule of a finitely generated module over a Noetherian ring is finitely generated (Examples Sheet 4).

Lemma 14.4. Let R be an integral domain. Then

$$\text{every submodule of a cyclic } R\text{-submodule is cyclic} \iff R \text{ is a PID}$$

Proof. $\Rightarrow$ R is a cyclic R-module. Saying its submodules are cyclic precisely means that every ideal is principal.

$\Leftarrow$ If M is a cyclic R-module, then $M \cong R/I$, $I \trianglelefteq R$ by Lemma 14.1. Any submodule of R/I is of the form J/I for some ideal $J \trianglelefteq R$ and $I \le J$. R a PID implies J principal hence J/I is cyclic.

□

Definition. Let M be an R-module.

(i) An element $m \in M$ is torsion if there exists $0 \neq r \in R$ with $rm = 0$.

(ii) M is a torsion module if every $m \in M$ is torsion.

(iii) M is torsion free if every $0 \neq m \in M$ is not torsion.

Example.
- The torsion elements in a $\mathbb{Z}$-module (= abelian group) are the elements of finite order.
- Any F-module (= vector space) is torsion free.

Start of lecture 20

15. Direct Sums and Free Module

Definition. Let $M_1, \ldots, M_n$ be R-modules. The direct sum

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n$$

is the set $M_1 \times \cdots \times M_n$ with operations

$$(m_1, \ldots, m_n) + (m'_1, \ldots, m'_n) = (m_1 + m'_1, \ldots, m_n + m'_n)$$
$$r(m_1, \ldots, m_n) = (rm_1, \ldots, rm_n) \qquad (r \in R)$$

Example. $R^n = R \oplus \cdots \oplus R$.

Lemma 15.1. If $M = \bigoplus_{i=1}^n M_i$ and $N_i \leq M_i$ for all i, then setting $N = \bigoplus_{i=1}^n N_i \leq M$, we have

$$M/N \cong \bigoplus_{i=1}^n M_i/N_i$$

Proof. Apply first isomorphism theorem to the surjective R-module homomorphism

$$M \to \bigoplus_{i=1}^n M_i/N_i$$
$$(m_1, \ldots, m_n) \mapsto (m_1 + N_1, \ldots, m_n + N_n)$$

with kernel $N = \bigoplus_{i=1}^n N_i$. □

Definition. Let $m_1, \ldots, m_n \in M$. The set $\{m_1, \ldots, m_n\}$ is independent if

$$\sum_{i=1}^n r_i m_i = 0 \implies r_1 = r_2 = \cdots = r_n = 0$$

Definition. A subset $S \subset M$ generates M freely if

(i) S generates M, i.e. $\forall m \in M$, $m = \sum_{i=1}^n r_i s_i$ for some $r_i \in R$, $s_i \in S$.

(ii) Any function $\psi : S \to N$ where N is an R-module, extends to an R-module homomorphism $\theta : M \to N$. (Such an extension is unique by (i)).

An R-module which is freely generated by some subset $S \subset M$ is called *free* and S is called a *free basis*.

Proposition 15.2. For a subset $S = \{m_1, \dots, m_n\} \subset M$, the following are equivalent:

(i) S generates M freely.

(ii) S generates M and S is independent.

(iii) Every element of M can be written uniquely as

$$r_1m_1 + \cdots r_nm_n$$

for some $r_1, \dots, r_n \in R$.

(iv) The R-module homomorphism

$$\begin{aligned} R^n &\to M \\ (r_1, \dots, r_n) &\mapsto \sum_{i=1}^{n} r_im_i \end{aligned}$$

is an isomorphism.

Proof. (i) $\Rightarrow$ (ii) Let S generate M freely. If S is not independent, then $\exists r_1, \dots, r_n \in R$ with $\sum r_im_i = 0$ and some $r_j \neq 0$. Define $\psi : S \to R$

$$m_i \mapsto \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

extends to R-module homomorphism $M \to R$. Then

$$\begin{aligned} 0 &= \theta(0) \\ &= \theta\left(\sum r_im_i\right) \\ &= \sum r_i\theta(m_i) \\ &= r_i \end{aligned}$$

Thus S is independent. The rest are exercises.

□

Example. A is non-trivial finite abelian group. Then A is not a free $\mathbb{Z}$-module.

Example. The set $\{2,3\}$ generates $\mathbb{Z}$ as a $\mathbb{Z}$-module, but they are not independent since

$$(3) \cdot 2 + (-2) \cdot 3 = 0$$

Furthermore, no subset of $\{2,3\}$ is a free basis, since $\{2\}$ and $\{3\}$ do not generate.

Proposition 15.3 (Invariance of dimension)**.** Let R be a non-zero ring. If $R^m \cong R^n$ as R-modules then $m = n$.

Proof. First, we introduce a general construction. Let $I \trianglelefteq R$ and M an R-module. Define

$$IM = \left\{ \sum a_i m_i : a_i \in I, m_i \in M \right\} \leq M$$

The quotient M/IM is an R/I-module via

$$(r + I)(m + IM) = rm + IM$$

Well-defined: if $b \in I$ then

$$b \cdot (m + IM) = bm + IM = 0 + IM$$

Suppose $R^m \cong R^n$. Choose $I \trianglelefteq R$ maximal ideal (user Zorn's Lemma and Example Sheet 2 Question 4). By the above, we get an isomorphism of R/i module

$$(R/I)^m \cong R^m/IR^m \cong R^n/IR^n \cong (R/I)^n$$

But $I \trianglelefteq R$ is maximal hence R/I is a field. So $m = n$ by invariance of dimension for vector spaces. □

16. The Structure Theorem and Applications

Until further notice: R is always a Euclidean domain, $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ Euclidean function. Let A be an $m \times n$ matrix with entries in R.

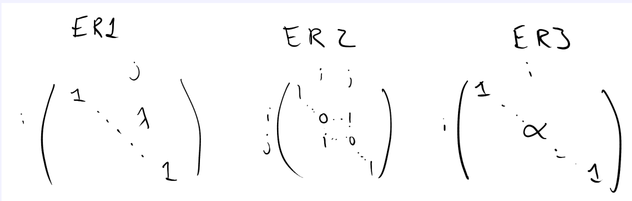
Definition. The elementary row operations are:

(ER1) Add λ times i-th row to j-th row ($\lambda \in R$, $i \neq j$).

(ER2) Swapping i-th and j-th rows.

(ER3) Multiply i-th row by $u \in R^\times$.

Each of these can be realised by left multiplication by an $m \times m$ invertible matrix:



In particular, these operations are reversible. Similarly, we can define elementary column operations (EC1-3) – realised b right multiplication by an invertible $n \times n$ matrix.

Definition (Equivalent matrices)**.** Two $m \times n$ matrices A and B are *equivalent* if there exists a sequence of elementary row and column operations taking A to B. If they are equivalent, then there exists (invertible) P, Q such that $B = QAP$.

Start of lecture 21

Let R be a Euclidean domain and $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ a Euclidean function.

Theorem 16.1 (Smith Normal-form)**.** An $m \times n$ matrix $A = (a_{ij})$ over a Euclidean Domain R is equivalent to a diagonal matrix

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_t & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

where $d_i \neq 0$ and $d_1 \mid d_2 \mid \cdots \mid d_t$. The d_i are called *invariant factors*. We will show they are unique up to associates.

Proof. If $A = 0$ then done. Otherwise upon swapping rows and columns, may assume $a_{11} \neq 0$. We will reduce $\phi(a_{11})$ as much as possible via the following algorithm.

(Step 1) If $a_{11} \mid a_{1j}$ for some $j \geq 2$, then write $a_{ij} = qa_{11} + r$, $q_1 r \in R$, $\phi(r) < \phi(a_{11})$. Subtracting q times column 1 from j, and swapping these columns makes the top left entry r.

(Step 2) If $a_{11} \nmid a_{i1}$ for some $i \geq 2$ then repeat above process with row operations.

Steps 1 and 2 decrease $\phi(a_{11})$, so can repeat finitely many times until $a_{11} \mid a_{1j}$ for all $j \geq 2$ and $a_{11} \mid a_{i1}$ for all $i \geq 2$. Subtracting multiples of first row / column from others gives

$$A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

where A' is a $(m-1) \times (n-1)$ matrix.

(Step 3) If $a_{11} \nmid a_{ij}$ for some $i, j \geq 2$, then add i-th row to first row, and perform column operations as in Step 1 to decrease $\phi(a_{11})$. Then restart algorithm. Hence after finitely many steps we get

$$A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

with $a_{11} = d_1$ say such that $d_1 \mid a_{ij}$ for all i, j.

Applying the same method to A' gives the result. □

For uniqueness of invariant factors – introduce minors of A.

Definition. A $k \times k$ minor of A is the determinant of a $k \times k$ submatrix of A (i.e. a matrix formed by deleting $m - k$ rows and $n - k$ columns).

Definition. The k-th Fitting ideal $\mathrm{Fit}_k(A) \trianglelefteq R$ is the ideal generated by the $k \times k$ minors of A.

Lemma 16.2. If A and B are equivalent matrices, then $\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)$ for all k.

Proof. We show that (ER1-3) don't change $\mathrm{Fit}_k(A)$. Same proof works for EC1-3.

(ER1) Add λ times j-th row to i-th row, so A becomes A'. Let C be a $k \times k$ submatrix of A and C' the corresponding submatrix of A'.

- If we did not choose the i-th row, then $C = C'$ so $\det C = \det C'$.
- If we choose both of the rows i and j, then C and C' differ by row operation, hence $\det C = \det C'$.
- If we chose the i-th row but not the j-th row, then by expanding along the i-th row,

$$\det(C') = \det(C) \pm \lambda \det(D)$$

  where D is another $R \times R$ submatrix of A (Choose j-th row instead of i-th row). Thus $\det(C') \in \mathrm{Fit}_k(A)$.

Hence $\mathrm{Fit}_k(A') \subset \mathrm{Fit}_k(A)$. Since (ER1) is reversible we get $\supset$ as well by same argument, hence equality. (ER2) and (ER3) are similar but easier.

□

Now if A has SNF $\mathrm{diag}(d_1, \ldots, d_t, 0, \ldots, 0)$, $d_1 \mid d_2 \mid \cdots \mid d_t$, then $\mathrm{Fit}_k(A) = (d_1 d_2 \cdots d_k) \trianglelefteq R$, $k = 1, \ldots, t$. Thus the products $d_1 \cdots d_k$ (up to associate) depends only on A.

Example. Consider the matrix

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$$

over $\mathbb{Z}$.

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \xrightarrow{c_1 \to c_1 + c_2} \begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix} \xrightarrow{c_2 \to c_1 + c_2} \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix} \xrightarrow{R_2 \to R_2 - 3R_1} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

But also $(d_1) = (2, -1, 1, 2) = (1)$ so $d_1 = \pm 1$, $(d_1 d_) = (\det A) = (5)$ so $d_2 = \pm 5$.

We will use SNF to prove the structure theorem. First some preparation.

Lemma 16.3. R a Euclidean Domain. Any submodule of R^m is generated by at most m elements.

Remark. $m = 1$ was Lemma 14.4.

Proof. Let $N \leq R^m$. Consider the ideal

$$I = \{r_1 \in R \mid \exists r_2, \dots, r_m \in R, (r_1, \dots, r_n) \in N\} \trianglelefteq R$$

Since ED implies PID, we have $I = (a)$ for some $a \in R$. Choose some $n = (a, a_2, \dots, a_m) \in N$. For $(r_1, \dots, r_m) \in N$, we have $r_1 = ra$ for some $r \in R$, so

$$(r_1, r_2, \dots, r_m) - rn = (0, r_2 - ra_2, \dots, r_m - ra_m)$$

which lies in $N' := N \cap (0 \oplus R^{m-1}) \leq R^{m-1}$, hence $N = Rn + N'$. By induction, N' is generated by $n_2, \dots, n_m$, hence $\{n, n_2, \dots, n_m\}$ generates N. □

Start of lecture 22

Lemma 16.4. R an PID. Any submodule of R^m is finitely generated.

Proof. Example Sheet 4. □

Theorem 16.5. Let R be a Euclidean Domain and $N \leq R^m$. There is a free basis $x_1, \dots, x_m$ for R^m such that N is generated by $d_1 x_1, \dots, d_t x_t$ for some $t \leq m$ and $d_1, \dots, d_t \in R$ with $d_1 \mid d_2 \mid \cdots \mid d_t$.

Proof. By Lemma 16.3 we have $N = Ry_1 + \cdots + Ry_n$ for some $n \leq m$. Each y_i belongs to R^m, so we can form an $m \times n$ matrix

$$A = (y_1 | y_2 | \cdots | y_n)$$

By Theorem 16.1, A is equivalent to

$$A' = \operatorname{diag}(d_1, \dots, d_t, 0, \dots, 0)$$

A' obtained from A by elementary row and column operations. Each row operation changes our choice of free basis for R^m and each column operation changes our set of generators for N. Thus, after changing free basis of R^m to $x_1, \dots, x_m$ (say), the submodule N is generated by $d_1 x_1, d_2 x_2, \dots, d_t x_t$ as claimed. □

Theorem (Structure Theorem)**.** Let R be a Euclidean Domain and M a finitely generated R-module. Then

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_t) \oplus \underbrace{R \oplus \cdots \oplus R}_{k \text{ copies}}$$

for some $0 \neq d_1 \in R$ with $d_1 \mid d_1 \mid \cdots \mid d_t$ and $k \geq 0$. The d_i are called *invariant factors*.

Proof. Since M is finitely generated, there exists a surjective R-module homomorphism $\phi : R^m \to M$ for some m (Lemma 14.1). By first isomorphism theorem, $M \cong R^m / \ker(\phi)$. By Theorem 16.4, there exists a free basis $x_1, \ldots, x_m$ for R^m such that $\ker(\phi)$ is generated by $d_1 x_1, \ldots, d_t x_t$ with $d_1 \mid d_2 \mid \cdots \mid d_t$. Then

$$\begin{aligned} M &\cong \frac{R \oplus R \oplus \cdots \oplus R \oplus R \oplus \cdots \oplus R}{d_1 R \oplus d_2 R \oplus \cdots \oplus d_t R \oplus 0 \oplus \cdots \oplus 0} \\ &\cong R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_t) \oplus R \oplus \cdots \oplus R \qquad \text{(by Lemma 15.1)} \end{aligned}$$

□

Remark. After deleting these d_i which are units, the module M uniquely determines the d_i (up to associates). Proof omitted.

Corollary 16.6. Let R be a Euclidean Domain. Then any finitely generated torsion-free R-module is free.

Proof. M torsion-free $\implies$ no submodules of the form $R/(d)$ with $d \neq 0$. Thus $M \cong R^m$ for some m. □

Example. $R = \mathbb{Z}$. Consider the abelian group G generated by a and b subject to the relations $2a + b = 0$, $-a + 2b = 0$. Then $G \cong \mathbb{Z}^2/N$, where N is generated by $(2,1)$, $(-1,2)$.

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \qquad \text{has SNF} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

Thus can change basis for $\mathbb{Z}^2$ such that N is generated by $(1,0)$ and $(0,5)$. Thus

$$G \cong \mathbb{Z}^2/N \cong \frac{\mathbb{Z} \oplus \mathbb{Z}}{\mathbb{Z} \oplus 5\mathbb{Z}} \cong \mathbb{Z}/5\mathbb{Z}$$

More generally:

Theorem (Structure theorem for finitely generated abelian groups)**.** Any finitely generate abelian group G is isomorphic to

$$\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

where $d_1 \mid d_2 \mid \cdots \mid d_t$ and $r \geq 0$.

Proof. Take $R = \mathbb{Z}$ in structure theorem. □

Remark. The special case G is finite (so $r = 0$) was quoted as Theorem 6.4.

In Section 6, we saw that any finite abelian group can be written as a product of C_{p^i}'s where p is prime. To generalise this we need:

Lemma 16.7. Let R be a PID and $a, b \in R$ with $\gcd(a, b) = 1$. Then

$$R/(ab) \cong R/(a) \oplus R/(b)$$

as R-modules. (Case $R = \mathbb{Z}$ was Lemma 6.2).

Proof. R a PID $\implies (a, b) = (d)$ for some $d \in R$. But $\gcd(a, b) = 1$ hence d a unit. So there exists $r, s \in R$ such that $ra + sb = 1$. Define an R-module homomorphism

$$\psi : R \to R/(a) \oplus R/(b) \qquad x \mapsto (x + (a), x + (b))$$

Then $\psi(sb) = (1 + (a), 0 + (b))$, $\psi(ra) = (0 + (a), 1 + (b))$. Thus

$$\psi(sbx + ray) = (x + (a), y + (b))$$

for any $x, y \in R$, so ψ is surjective. Clearly $(ab) \le \ker(\psi)$. Conversely, if $x \in \ker(\psi)$, then $x \in (a) \cap (b)$ and

$$\begin{aligned} x &= x(ra + sb) \\ &= \underbrace{r(ax)}_{\in (ab)} + \underbrace{s(xb)}_{\in (ab)} \\ &\in (ab) \end{aligned}$$

Thus $\ker(\psi) = (ab)$. Then by the First Isomorphism Theorem for rings, $R/(ab) \cong R/(a) \oplus R/(b)$. □

Start of lecture 23

Theorem (Primary decomposition theorem)**.** Let R be a Euclidean Domain and M a finitely generated R-module. Then

$$M \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k}) \oplus R^m$$

(as R-modules) where $p_1, \dots, p_k$ are primes (not necessarily distinct) and $m \ge 0$.

Proof. By the structure theorem

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_t) \oplus R^m$$

So it suffices to consider $M \cong R/(d_i)$, $d_i = up_1^{a_1} \cdots p_r^{a_r}$ where u is a unit and $p_1, \dots, p_r$ are distinct (non-associate) primes. Lemma 16.6 implies

$$R/(d_i) \cong R/(p_1^{a_1}) \oplus \cdots \oplus R/(p_r^{a_r})$$ □

Let V be a vector space over a field F. Let $\alpha : V \to V$ be a linear map and let V_α denote the $F[X]$-module V where $F[X] \times V \to V$ is given by $(f(X), v) \mapsto f(\alpha)(v)$.

Lemma 16.8. If V finite dimensional, then V_α is a finitely generated $F[X]$-module.

Proof. If $v_1, \ldots, v_n$ generate V as an F-vector space, then they generate V_α as an $F[X]$-module since $F \le F[X]$. □

Examples

(i) Suppose $V_\alpha \cong F[X]/(X^n)$ as $F[X]$-module. Then $1, X, X^2, \ldots, X^{n-1}$ is a basis for $F[X]/(X^n)$ as an F-vector space, and with respect to this basis α has matrix

$$(*) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

(ii) Suppose $V_\alpha \cong F[X]/(X-\lambda)^n$ as $F[X]$-modules. Then with respect to basis $1, (X-\lambda), (X-\lambda)^2, \ldots, (X-\lambda)^{n-1}$, $\alpha - \lambda\mathrm{id}$ has matrix $(*)$, thus α has matrix

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}$$

(iii) Suppose $V_\alpha \cong F[X]/(f(X))$ where $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, then with respect to basis $1, X, X^2, \ldots, X^{n-1}$, α has matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

This is called the companion matrix $C(f)$ of the monic polynomial f.

Theorem 16.9 (Rational canonical form)**.** Let $\alpha : V \to V$ be an endomorphism of a finite dimensional F-vector space, where F is a field. Then $F[X]$-module V_α decomposes as

$$V_\alpha \cong F[X]/(f_1) \oplus \cdots \oplus F[X]/(f_t)$$

where $f_i \in F[X]$ monic and $f_1 \mid f_2 \mid \cdots \mid f_t$. Moreover, with respect to a suitable basis for V (as an F vector space), α has matrix

$$\begin{pmatrix} C(f_1) & 0 & \cdots & 0 \\ 0 & C(f_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C(f_t) \end{pmatrix} \tag{$**$}$$

Proof. By Lemma 16.7, V_α is a finitely generated $F[X]$-module. Since $F[X]$ is a Euclidean Domain, structure theorem implies

$$V_\alpha \cong F[X]/(f_1) \oplus \cdots \oplus F[X]/(f_t) \oplus F[X]^m$$

with $f_1 \mid f_2 \mid \cdots \mid f_t$. Since V is finite dimensional as an F vector space, $m = 0$. Upon multiplying f_i by a unit we may assume f_i is monic. $\square$

Remark. (i) If α is represented by an $n \times n$ matrix A, then the theorem says that A is similar to $(**)$.

(ii) The minimal polynomial of α is f_t.

(iii) The characteristic polynomial of α is $\prod_{i=1}^t f_i$.

The last two properties show that the minimal polynomial divides the characteristic polynomial, which is the Cayley-Hamilton Theorem.

Example. If $\dim V = 2$, then $\sum \deg f_i = 2$. So

$$V_\alpha = F[X]/(X - \lambda) \oplus F[X]/(X - \lambda)$$

or

$$V_\alpha \cong F[X]/(f)$$

where f is the characteristic polynomial of α.

Corollary 16.10. Let $A, B \in \mathrm{GL}_2(F)$ non-scalar. Then

A and B are similar (= conjugate) $\iff$ they have the same characteristic polynomial

Proof. $\Rightarrow$ Linear algebra.

$\Leftarrow$ By the last example, A and B are similar to $C(f)$.

$\square$

Definition. The *annihilator* of an R module M is

$$\mathrm{Ann}_R(M) = \{r \in R \mid rm = 0 \forall m \in M\} \trianglelefteq R$$

Example. (i) $I \trianglelefteq R$, then $\mathrm{Ann}_R(R/I) = I$.

(ii) If A is a finite abelian group, then $\mathrm{Ann}_{\mathbb{Z}}(A) = (e)$ where e is the exponent of A.

(iii) If V_α as above, then $\mathrm{Ann}_{F[X]}(V_\alpha)$ is the ideal generated by the minimal polynomial of α.

Start of lecture 24

Lemma 16.11. The primes in $\mathbb{C}[X]$ (up to associates) are the polynomials $X - \lambda$, for some $\lambda \in \mathbb{C}$.

Proof. By the fundamental theorem of algebra, any non-constant polynomial in $\mathbb{C}[X]$ has a root in $\mathbb{C}$, so a factor $X - \lambda$. Hence, the irreducibles have degree 1. $\square$

Theorem 16.12 (Jordan Normal form)**.** Let $\alpha : V \to V$ be an endomorphism of a finite dimensional $\mathbb{C}$-vector space. Let V_α be V regarded as a $\mathbb{C}[X]$-module with X acting as α. There is an isomorphism of $\mathbb{C}[X]$-modules

$$V_\alpha \cong \mathbb{C}[X]/((X-\lambda_1)^{n_1}) \oplus \cdots \oplus \mathbb{C}[X]/((X-\lambda_t)^{n_t})$$

where $\lambda_1, \dots, \lambda_t \in \mathbb{C}$ (not necessarily distinct). In particular there exists a basis for V such that α has matrix

$$\begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \cdots & 0 \\ 0 & J_{n_2}(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

where

$$J_n(\lambda) = \begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}$$

Proof. $\mathbb{C}[X]$ is a Euclidean Domain and V_α is finitely generated by Lemma 16.7. We apply the primary decomposition, noting that the primes in $\mathbb{C}[X]$ are as in Lemma 16.10. V finite dimensional implies we get no copies of $\mathbb{C}[X]$. $J_n(\lambda)$ represents multiplying by X on $\mathbb{C}[X]/(X-\lambda)^n$ with respect to the basis $1, X-\lambda, (X-\lambda^2, \dots, (X-\lambda)^{n-1}$. □

Remark. (i) If α represented by matrix A, then the theorem says that A is similar to a matrix in JNF.

(ii) The Jordan blocks are uniquely determined up to reordering. Can be proved by considering the dimensions of the generalised eigenspace $\ker((\alpha - \lambda \mathrm{id})^m)$, $m = 1, 2, 3, \dots$ (omitted).

(iii) The minimal polynomial of α is $\prod_\lambda (X-\lambda)^{c_\lambda}$ where c_λ is the size of the largest λ-block.

(iv) The *characteristic polynomial* of α is $\prod_\lambda (X-\lambda)^{a_\lambda}$ where a_λ is the sum of the sizes of λ-blocks.

(v) The number of λ blocks is the dimension of the λ-eigenspace.

17. Modules over PID (non-examinable)

The *structure theorem* holds for PID's. We illustrate some ideas which go into the proof.

Theorem 17.1. Let R be a PID. Then any finitely generated torsion-free R-module is free. (For R a Euclidean Domain, this is Corollary 16.5).

Lemma 17.2. Let R be a PID and M an R-module. Let $r_1, r_2 \in R$ not both zero and let $d = \gcd(r_1, r_2)$.

(i) There exists $A \in \mathrm{SL}_2(R)$ such that

$$A \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}$$

(ii) If $x_1, x_2 \in M$ then there exists $x_1', x_2 \in M$ such that $Rx_1 + Rx_2 = Rx_1' + x_2'$ and $r_1x_1 + r_2x_2 = dx_1' + 0x_2'$.

Proof. R a PID implies $(r_1, r_2) = (d)$, hence there exists $\alpha, \beta \in R$ such that $\alpha r_1 + \beta r_2 = d$. Write $r_1 = s_1 d$, $r_2 = s_2 d$ for some $s_1, s_2 \in R$. Then $\alpha s_1 + \beta s_2 = 1$.

(i)

$$\underbrace{\begin{pmatrix} \alpha & \beta \\ -s_2 & s_1 \end{pmatrix}}_{\det = \alpha s_1 + \beta s_2 = 1} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

(ii) Let $x_1' = s_1x_1 + s_2x_2$, $x_2' = -\beta x_1 + \alpha x_2$. Then $Rx_1' + Rx_2' \subseteq Rx_1 + Rx_2$. To prove the reverse inclusion we solve for x_1 and x_2 in terms of x_1' and x_2'. This is possible since

$$\det \begin{pmatrix} s_1 & s_2 \\ -\beta & \alpha \end{pmatrix} = \alpha s_1 + \beta s_2 = 1$$

Finally

$$\begin{aligned} r_1x_1 + r_2x_2 &= d(s_1x_1 + s_2x_2) \\ &= dx_1' \end{aligned}$$

□

Proof of Theorem 17.1. Let $M = Rx_1 + Rx_n$ with n as small as possible. If $x_1, \dots, x_n$ are independent then M is free, and we're done. Otherwise, $\exists r_1, \dots, r_n \in R$ not all zero with $\sum_{r=1}^n r_ix_i = 0$. WLOG $r_1 \neq 0$. Lemma 17.2 (ii) shows that after replacing x_1 and x_2 by suitable x_1' and x_2', we may assume $r_1 \neq 0$ and $r_2 = 0$. Repeating this process (changing x_1 and x_3, then x_1 and x_4 and so on), we may assume $r_1 \neq 0$, $r_2 = 0, \dots, r_n = 0$. Now $r_1x_1 = 0 \implies x_1 = 0$ (since M is torsion free). Thus, $M = Rx_2 + \cdots + Rx_n$, which contradicts our choice of n. □