Groups, Rings and Modules

Hasan Baig

Lent 2021

Contents

0 Overview

0.1 Groups

Continuing from IA Groups. We pay particular attention to simple groups, p-groups and p-subgroups. The main highlight of this part of the course will be the Sylow theorems.

0.2 Ring

These are sets where we can add, subtract and multiply, for example $\mathbb{Z}$ or $\mathbb{C}[x]$. Important examples include "rings of integers" (e.g. $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$) studied further in Part II Number Fields, and polynomial rings which are central to Part II Algebraic Geometry. A ring where division is always possible is called a field for example $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}/p\mathbb{Z}$ for p a prime.

0.3 Modules

A module is the analogue of a vector space where the scalars belong to a ring instead of a field. We will attempt to classify modules over certain nice rings. This will allow us to prove the Jordan Normal Theorem for matrices and to classify finite abelian groups.

1 Groups

1.1 Revision and Basics

Definition. A **group** is a pair $(G, \cdot)$ consisting of a set G and binary operation $\cdot : G \times G \to G$ satisfying

- Associativity
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$$
- Identity
$$\exists e \in G \text{ s.t. } e \cdot g = g \cdot e = g \quad \forall g \in G$$
- Inverses
$$\forall g \in G \; \exists g^{-1} \in G \text{ s.t. } g \cdot g^{-1} = g^{-1} \cdot g = e$$

Remarks.

(i) In checking $\cdot$ is well defined, need to check closure. I.e.
$$a, b \in G \implies a \cdot b \in G$$

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

Definition. A subset $H \subseteq G$ is a **subgroup** (written $H \leq G$) s.t. it is a group w.r.t. $\cdot$ restricted to $H \times H$

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

Examples.

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

(ii) Cyclic & dihedral groups
$$C_n = \text{cyclic group of order } n$$
$$D_{2n} = \text{symmetries of a regular } n\text{-gon}$$

(iii) Symmetric & alternating groups
$$S_n = \text{all permutations of } \{1, 2, \ldots, n\}$$
$$A_n \leq S_n \text{ subgroup of even permutations}$$

(iv) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ $ij = k, ji = -k, i^2 = -1$ etc.

(v) Matrix groups. For F a field
$$GL_n(F) = \text{all } n \times n \text{ matrices over } F \text{ with } \det \neq 0$$
$$SL_n(F) \leq GL_n(F), \text{ subgroup of matrices with } \det = 1$$

(general and special linear groups)

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

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

Definition. For a subgroup $H \leq G$, the **left cosets** of H in G are sets

$$gH = \{gh : h \in H\} \text{ for } g \in G$$

Note. These partition G, and each has the same cardinality as H. We deduce Lagrange's Theorem.

Theorem 1.1. Let G be a finite group, H a subgroup. Then $|G| = |H| \cdot |G : H|$ where $|G : H|$ is the number of left cosets of H in G, and is called the index of H in G.

Note. There is a partial converse.

Claim. $|G| = p^a m$ p prime, $p \nmid m$ then $\exists H \leq G$ with $|H| = p^a$ (proof later) (1^{st} Sylow Theorem)

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

Remark. If g has order d then
(i) $g^n = 1 \iff d | n$
(ii) $\{1, g, g^2, \ldots, g^{d-1}\} \leq G$ and so if G is finite then by Lagrange $d \mid |G|$

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

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

Proof. We must check $\cdot$ is 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 $h_1, h_2 \in H$ so $g_1' g_2' H = g_1 h_1 g_2 h_2 H$. This is equal to $g_1 g_2 H$ iff

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

which is true since $H \trianglelefteq G$.
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

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

It has **kernel** $\ker(\phi) = \{g \in G : \phi(g) = 1\} \leq G$ and **image** $\mathrm{Im}(\phi) = \{\phi(g) : g \in G\} \leq H$. If $a \in \ker(\phi)$ and $g \in G$ then $\phi(g^{-1}ag) = \phi(g)^{-1}\phi(a)\phi(g) = 1$

$$\implies g^{-1}ag \in \ker(\phi) \text{ therefore } \ker(\phi) \trianglelefteq G$$

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 $\phi : G \to H$
(Exercise: check $\phi^{-1} : H \to G$ is a group homomorphism)

Theorem 1.3 (Isomorphism Theorem)**.** Let $\phi : G \to H$ be a group homomorphism.
Then $\ker(\phi) \trianglelefteq G$ and $G/\ker(\phi) \cong \mathrm{Im}(\phi)$

Proof. Let $K = \ker(\phi)$. We already checked that $K \trianglelefteq G$
Define $\Phi : G/K \to \mathrm{Im}(\phi)$
$gK \mapsto \phi(g)$
Φ is well defined and injective:

$$\begin{aligned} g_1K = g_2K &\iff g_2^{-1}g_1 \in K \\ &\iff \phi(g_2^{-1}g_1) = 1 \\ &\iff \phi(g_2)^{-1}\phi(g_1) = 1 \\ &\iff \phi(g_1) = \phi(g_2) \end{aligned}$$

Φ is a group homomorphism:

$$\begin{aligned} \Phi(g_1Kg_2K) &= \Phi(g_1g_2K) \\ &- \phi(g_1g_2) \\ &= \phi(g_1)\phi(g_2) \\ &\Phi(g_1K)\Phi(g_2K) \end{aligned}$$

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

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

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

$$\mathrm{Im}(\phi) = \mathbb{C}^* \text{(by existence of log)}$$

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

Note. Sometimes the Isomorphism Theorem is called the "First Isomorphism Theorem". It has the following corollaries:

Theorem 1.4 (2^{nd} Isomorphism Theorem)**.** Let $H \leq G$ and $K \leq G$. Then

$$HK = \{hk : h \in H,\, k \in K\} \leq G \text{ and } H \cap K \trianglelefteq H$$

Moreover

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

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

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1h_2^{-1}}_{\in H}\underbrace{h_2k_1k_2h_2^{-1}}_{\in K}$$

$$\therefore HK \leq G$$

Let $\phi : H \to G/K$
$h \mapsto hK$ (this is the composite of the inclusion $H \to G$ and the quotient map $G \to G/K$)
$\therefore \phi$ is a group homomorphism.

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

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

First isomorphism theorem $\implies H/H \cap J \cong HK/K$

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

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

$$X \mapsto \{g \in G : gK \in X\}$$

$$H/K \mapsfrom H$$

This restricts to a bijection

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

Theorem 1.5 (3^{rd} Isomorphism Theorem)**.** Let $K \leq H \leq G$ 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 $g_2^{-1}g_1 \in K \leq H \implies g_1H = g_2H \therefore \phi$ is well defind.
ϕ is a surjective group homomorphism with kernel H/K
Now apply the first isomorphism theorem

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

Definition. A group G is **simple** if $\{1\}$ and G are its only normal subgroups

Lemma 1.6. An abelian group is simple iff it is isomorphic to C_p for some prime number p

Proof. By Lagrange's Theorem, a subgroup $H \leq C_p$ has order $|C_p| = p$, hence order 1 or $p \therefore H = \{1\}$ or C_p. Thus C_p is simple.
Let G be an abelian simple group and $1 \neq g \in G$.
Any subgroup of an abelian group is normal.
G contains the subgroup $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}$
Since G is simple, this must be the whole group i.e. G is cyclic.
If G is infinite, then $G \cong (\mathbb{Z}, +)$, and $2\mathbb{Z} \trianglelefteq \mathbb{Z}$※
Otherwise $G \cong C_n$ for some n.
Let g be a generator. If $m|n$, then $g^{n/m}$ generates a subgroup of order m.
G simple $\implies$ only factors of n are 1 and $n \implies n$ is prime

Lemma 1.7. 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.

Proof. By induction on $|G|$. Case $|G| = 1$ ✓
If $|G| > 1$, then let G_{m-1} be a normal subgroup of largest possible order $\neq |G|$. Previous remark $\implies G/G_{m-1}$ is simple.
Apply induction hypothesis to G_{m-1}

2 Group Actions

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

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

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

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

(i)
$$e * x = x \ \forall x \in X$$

(ii)
$$(g_1 g_2) * x = g_1 * (g_x * x) \ \forall g_1, g_2 \in G \ \forall x \in X$$

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

Proof. For each $g \in G$ there is a function $\phi_g : \underset{x \mapsto g*x}{X \to X}$

We have
$$\phi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \phi_{g_1}(\phi_{g_2}(x))$$
$$\therefore \phi_{g_1 g_2} = \phi_{g_1} \cdot \phi_{g_2} \ (\dagger)$$

In particular
$$\phi \cdot \phi_{g^{-1}} = \phi_{g^{-1}} \cdot \phi_g = \phi_e = \mathrm{id} \therefore \phi_g \in \mathrm{Sym}(X)$$

We define
$$\phi : \underset{g \mapsto \phi_g}{G \to \mathrm{Sym}(X)}$$

(this is a group homomorphism by ($\dagger$))
Conversely, let $\phi : G \to \mathrm{Sym}(X)$ be a group homomorphism
Define
$$\underset{(g,x) \mapsto \phi(g)(x)}{G \times X \to X}$$

Then

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

(ii)
$$(g_1 g_2) * x = \phi(g_1 g_2)(x) = \phi(g_1)(\phi(g_2)(x)) = g_1 * (g_2 * x)$$

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

Definition. Let G act on a set X

(i) The **orbit** of $x \in X$ is $\mathrm{orb}_G(x) = \{g * x : g \in G\} \subseteq X$
(ii) The **stabiliser** of $x \in X$ is $G_x = \{g \in G | g * x = x\} \leq G$

Theorem 2.2. We recall from IA: Orbit-Stabiliser Theorem: there is a bijection $\mathrm{orb}_G(x) \leftrightarrow G/G_x$ (set of left cosets of G_x in G)
In particular, if G is finite then
$$|G| = |\mathrm{orb}_G(x)| \cdot |G_x|$$

Remarks.

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

(ii) The orbits partition X. If there is just one orbit, then we say that the action is transitive

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

Examples.

(i) Let G act on itself by left multiplication, i.e. $g * x = gx$
The kernel of the action is $\{g \in G | gx = x \ \forall x \in G\} = \{1\} \therefore G \hookrightarrow \text{Sym}(G)$ This proves theorem below

Theorem 2.3 (Cayley's Theorem)**.** Any finite group G is isomorphic to a subgroup of S_n for some n. (Indeed we may take $n = |G|$)

Examples (Continued)**.**

(ii) Let $H \leq G$. Then G acts on G/H by left multiplicationi.e. $g * xH = gxH$.
This is a transitive group action (since $x_2x^{-1} * x_1H = x_2H$) with

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

$$\ker(\phi) = \bigcap_{c \in G} xHx^{-1}$$

This is the largest normal subgroup of G that is contained in H.

(iii) Let G act on itself by conjugation, i.e. $g * x = gxg^{-1}$.
The orbits and stabilisers have special names:

$$\text{orb}_G(x) = \{gxg^{-1} : g \in G\} = \text{ccl}_G(x)$$

is the conjugacy class of x in G.

$$G_x = \{g \in G : gx = xg\}$$

is the centraliser of x in G.

$$\ker(\phi) = \{g \in G : gx = xg \ \forall x \in G\} = Z(G)$$

is the centre of G.

Note. G also acts by conjugation on any normal subgroup

(iv) 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 $\{g \in G : gHg^{-1} = H\} = N_G(H)$ - the normaliser of H in G.
This is the largest subgroup of G to contain H as a normal subgroup.
In particular $H \trianglelefteq G \iff N_G(H) = G$

Theorem 2.4. 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 $\phi : G \to \mathrm{Sym}(X) = S_n$ be the associated permutation representation. As G is simple $\ker(\phi) = 1$ or G.
If $\ker(\phi) = G$ then $\mathrm{Im}(\phi) = 1$, contradicting that G acts transitively on X (since $n > 1$)

$$\therefore \ker(\phi) = 1 \ \& \ G \cong \mathrm{Im}(\phi) \leq S_n$$

Since $G \leq S_n$ and $A_n \trianglelefteq S_n$, the second isomorphism theorem gives

$$G \cap A_n \trianglelefteq G \text{ and } \frac{G}{G \cap A_n} \cong \frac{GA_n}{A_n} \leq S_n/A_n \cong C_2$$

G simple $\implies G \cap A_n = 1$ or G
If $G \cap A_n = 1$, $G \hookrightarrow C_2$ ※ to G non-abelian so $G \cap A_n = G$
Hence $G \leq A_n$.
Finally if $n \leq 4$ then A_n has no non-abelian simple subgroups. (By listing them)

Example. Let G be the group of rotations of an icosahedron (20 faces, 12 vertices, 30 edges)

Order	# elements of G
1	1
2	15
3	20
5	24
Total	60

Then check for G acting on the set of vertices

$$|G| = |\text{orbit}| \cdot |\text{stabiliser}| = 12 \cdot 5 = 60$$

The elements of order 2 are all conjugate. As are those of order 3. The elements of order 5 split into 2 conjugacy classes of size 12 (rotation by $\pm\frac{2\pi}{5}$ & $\pm\frac{4\pi}{5}$)

If $H \trianglelefteq G$ then $|H| = 1 + 15a + 30b + 12c$ for $a, b \in \{0, 1\}$, $c \in \{0, 1, 2\}$, and $|H|$ divides 60 $\therefore |H| = 1$ or 60. This shows G is simple.

We claim that the sets $H\backslash\{1\}$ for $H \le G$ subgroup of order 4 ($|H| = 4$) partition the 15 elements of order 2 into 5 sets of 3.

(i)
$$|H| = 4 \implies H \cong C_2 \times C_2 \text{ or } C_4$$

Cannot be C_4 as G has no elements order 4. $C_2 \times C_2$ has 3 elements order 2.

(ii) If $g \in G$ has order 2 then

$$g \in C_G(g) \text{ \& } |C_G(g)| = \frac{|G|}{|\text{ccl}_G(g)|} = \frac{60}{15} = 4$$

(iii) Suppose $1 \ne g \in H \cap K$ where H and K are distinct subgroups of order 4.
Then $|C_G(g)| \ge |H \cup K| > 4$ (since H and K are abelian) ※

This proves the claim.

Let G act on $X = \{\text{Subgroups of } G \text{ of order } 4\}$ by conjugation.
We obtain a group homomorphism $G \xrightarrow{\phi} \text{Sym}(X) = S_5$

$$G \text{ simple} \implies \ker\phi = 1 \text{ or } G$$

If kernel is G then G has normal subgroup order 4 ※
So $G \cong \text{Im}(\phi) \le S_5$
Exactly as in proof of Thm 2.3, either $G \cong C_2$ or $G \le A_5$
But $|G| = |A_5| = 60 \therefore G \cong A_5$

3 Alternating Groups

As seen in IA, permutations in S_n are conjugate iff they have the same cycle type.

Example. In S_5 we have:

cycle type	# elements	sign
id	1	$+$
$(\cdot\cdot)$	10	$-$
$(\cdot\cdot)(\cdot\cdot)$	15	$+$
$(\cdot\cdot\cdot)$	20	$+$
$(\cdot\cdot)(\cdot\cdot\cdot)$	20	$-$
$(\cdot\cdot\cdot\cdot)$	30	$-$
$(\cdot\cdot\cdot\cdot\cdot)$	24	$+$
Total	120	

Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$.
If $\exists$ odd permutation commuting with g then

$$|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)| \ \&\ |\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|$$

Otherwise

$$|C_{A_n}(g)| = |C_{S_n}(g)| \ \&\ |\mathrm{ccl}_{A_n}(g)| = \frac{1}{2}|\mathrm{ccl}_{S_n}(g)|$$

e.g. Taking $n = 5$, $(1\,2)(3\,4)$ commutes with the odd permutation $(1\,2)$
$(1\,2\,3)$ commutes with the odd permutation $(4\,5)$
But if $h \in C_{S_5}(g)$ where $g = (1\,2\,3\,4\,5)$ then

$$(1\,2\,3\,4\,5) = h(1\,2\,3\,4\,5)h^{-1} = (h(1)\,h(2)\,h(3)\,h(4)\,h(5))$$

$$\implies h \in \langle g \rangle \leq A_5 \therefore |\mathrm{ccl}_{A_5}(g)| = \frac{1}{2}|\mathrm{ccl}_{S_5}(g)| = 12$$

$\therefore A_5$ has conjugacy classes of sizes 1, 15, 20, 12, 12.
Exactly as in earlier example, this shows A_5 simple.

Lemma 3.1. A_n is generated by 3-cycles

Proof. Each $\sigma \in A_n$ is a product of an even number of transpositions.
So it suffices to write the product of any two transpositions as a product of 3-cycles. For a, b, c, d distinct

$$(a\,b)(b\,c) = (a\,b\,c)$$

$$(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d)$$

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

Proof. We claim that every 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 σ by $\sigma(45)$

Theorem 3.3. The alternating group A_n is simple $\forall n \geq 5$

Proof. Let $1 \neq N \trianglelefteq A_n$. It suffices to show that N contains a 3-cycle.
Since then by Lemmas 3.1 and 3.2, we have $N = A_n$.
We take $1 \neq \sigma \in N$ and write it as a product of disjoint cycles.

- Case 1: σ contains a cycle of length $r \geq 4$ w.l.o.g.

$$\sigma = (1\,2\,3\,\ldots\,r)\tau$$

Let $\delta = (1\,2\,3)$

$$\underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} = (r\,\ldots\,2\,1)(1\,3\,2)(1\,2\,\ldots\,r)(1\,2\,3) = (2\,3\,r)$$

$\therefore$ N contains a 3-cycle.

- Case 2: σ contains two 3-cycles.
w.l.o.g.

$$\sigma = (1\,2\,3)(4\,5\,6)\tau$$

Let $\delta = (1\,2\,4)$

$$\sigma^{-1}\delta^{-1}\sigma\delta = (1\,3\,2)(4\,6\,5)(1\,4\,2)(1\,2\,3)(4\,5\,6)(1\,2\,4) = (1\,2\,4\,3\,6)$$

$\therefore$ we care done by case 1.

- Case 3: σ contains two 2-cycles w.l.o.g. $\sigma = (1\,2)(3\,4)\tau$
Let $\delta = (1\,2\,3)$

$$\underbrace{\sigma^{-1}\delta^{-1}\sigma\delta}_{\in N} = \overbrace{(1\,2)(3\,4)(1\,3\,2)(1\,2)(3\,4)}^{(2\,4\,1)}(1\,2\,3) = (1\,4)(2\,3) = \pi \text{ say}$$

Let $\varepsilon = (2\,3\,5)$
Then

$$\pi^{-1}\varepsilon^{-1}\pi\varepsilon = (1\,4)(2\,3)(2\,5\,3)(1\,4)(2\,3)(2\,3\,5) = (2\,3\,5)$$

Therefore N contains a 3-cycle

- Conclusion of proof: It remains to consider σ with cycle type

$$(\cdot\,\cdot) \implies \sigma \notin A_n ※$$

$$(\cdot\,\cdot\,\cdot) \implies \sigma \text{ is a 3-cycle}$$

$$(\cdot\,\cdot)(\cdot\,\cdot\,\cdot) \implies \sigma \notin A_n ※$$

Definition. An **automorphism** of a group G is an isomorphism $G \cong G$.
The automorphisms form a subgroup

$$\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$$

4 p-groups and p-subgroups

Definition. Let p be a prime. A finite group G is a **p-group** if $|G| = p^n$

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

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

$$\begin{aligned}|G| &\equiv \#(\text{conjugacy classes of size } 1)(\text{mod } p)\\ \implies 0 &\equiv |Z(G)|(\text{mod } p)\end{aligned}$$

Can check $g \in Z(G) \iff \text{ccl}_G(g) = \{g\}$
In particular $|Z(G)| > 1$

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
Nontrivial by 4.1 so G is abelian and apply lemma 1.3

Corollary 4.3. Let G be a p-group of order p^n.
Then G has a subgroup of order p^r for all $0 \leq p \leq n$

Proof. By Lemma 1.4, G has a composition series

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

with each quotient G_1/G_{i-1} simple. Also, G a p group so G_i/G_{i-1} a p-group

$$\implies G_i/G_{i-1} \cong C_p \therefore |G_i| = p^i \ \forall 0 \leq i \leq m \ \& \mu = n$$

Lemma 4.4. For G a group, if $G/Z(G)$ is cyclic then G is abelian

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

$$\therefore G = \{g^r z : r \in \mathbb{Z}, z \in Z(G)\}$$

$$\begin{aligned}(g^{r_1} z_1)(g^{r_2} z_2) &= g^{r_1+r_2} z_1 z_2 \text{ since } z_1 \text{ is central}\\ &= g^{r_1+r_2} z_2 z_1 \text{ since } z_1 \text{ is central}\\ &= (g^{r_2} z_2)(g^{r_1} z_1) \text{ since } z_2 \text{ is central}\end{aligned}$$

$\therefore G$ is abelian

Corollary 4.5. If $|G| = p^2$ then G is abelian

Proof. $|Z(G)| = \begin{cases} 1 \text{ ※to Thm 4.1} \\ p \implies |G/Z(G)| = p. \text{ Apply Lemma 4.4※} \\ p^2 \implies Z(G) = G, \text{ so done} \end{cases}$ See example sheet for case $|G| = p^3$

4.1 Sylow Theorems

Claim. Let G be a finite group of order $p^a m$ where p is a prime with $p \nmid m$. Then

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

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

(iii) The number $n_p = |\mathrm{Syl}_p(G)|$ of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod p$ & $n_p \mid |G|$ (and so in fact $n_p | m$

Proof.

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

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

For $0 \leq k < p^a$ the numbers $p^a m - k$ and $p^a - k$ are divisible by the same power of p

$$\therefore |\Omega| \text{ is coprime to } p \qquad (\dagger)$$

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

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

For any $X \in \Omega$ we have

$$|G_X| \cdot |\mathrm{orb}_G(X)| = |G| = p^a m$$

By ($\dagger$), we can pick X s.t. $|\mathrm{orb}_G(X)|$ is coprime to p.

$$\therefore p^a \mid |G_X| \qquad (1)$$

On the other hand, if $g \in G$ and $x \in X$ then $g \in (gx^{-1}) * X$

$$\therefore G = \bigcup_{g \in G} g * X$$

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

(1) and (2) $\implies |G_X| = p^a$, i.e. $G_X \leq G$ is a Sylow p-subgroup

(ii) We prove a bit more: see lemma 4.7

(iii) Let G act on $\mathrm{Syl}_p(G)$ by conjugation.
Sylow (ii) $\implies$ this action is transitive.
So by the orbit-stabiliser theorem $n_p = |\mathrm{Syl}_p(G)|$ divides $|G|$
Now let $P \in \mathrm{Syl}_p(G)$. Then P acts on $\mathrm{Syl}_p(G)$ by conjugation. Then the orbits have size dividing $|P|$, 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 size 1.
If $\{Q\}$ is an orbit size 1, then P normalises Q i.e. $P \leq N_G(Q)$.
Now P and Q are Sylow p-subgroups of $N_G(Q)$, hence by (ii) conjugate in $N_G(Q)$, hence equal since $Q \trianglelefteq N_G(Q)$
$\therefore \{P\}$ is the unique orbit of size 1.

Corollary 4.6. 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 $gPg^{-1} \leq G$ is another Sylow p-subgroup so we must have $gPg^{-1} = P \ \forall g \in G$, i.e. $P \trianglelefteq G$

Example. Let $|G| = 100 = 2^3 \cdot 5^3$
Then $n_5 \equiv 1 \pmod 5$ & $n_5 | 8$, so $n_5 = 1 \therefore$ the unique Sylow 5-subgroup is normal
$\therefore G$ is not simple

Example. Let $|G| = 132 = 2^2 \cdot 3 \cdot 11$
Then $n_{11} \equiv 1 \pmod{11}$ and $n_{11} | 12$
So $n_{11} = 1$ or 12. Suppose G is simple.
Then $n_{11} \neq 1$ (otherwise the 11-Sylow subgroup is normal)
$\therefore n_{11} = 12$ Now $n_3 \equiv 1 \pmod 3$ and $n_3 | 44$
So $n_3 = 4$ or 22 as G simple
Suppose $n_3 = 4$. Then letting G act on $\mathrm{Syl}_3(G)$ by conjugation gives a group homomorphism $\phi : G \to S_4$

$$\ker(\phi) \trianglelefteq \underset{G \text{ simple}}{\Longrightarrow} \underbrace{1}_{G \hookrightarrow S_4} \text{ or } \underbrace{G}_{※ \text{to Sylow (ii)}}$$

G can't inject into S_4 as then $132 \leq 24$
$\therefore n_3 = 22$ and $n_{11} = 12$
Hence, G has $22(3-1) = 44$ elements of order 3 and $12(11-1) = 120$ elements of order 11.
But

$$44 + 120 > 132 = |G| ※$$

$\therefore \nexists$ simple group of order 132.

Lemma 4.7. 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 set of left cosets G/P by left multiplication i.e.

$$q * gP = qgP$$

By the orbit stabiliser theorem, each orbit has size dividing $|Q|$, so either 1 or a multiple pf p. Since $|G/P| = m$ is coprime to p, $\exists$ orbit size 1. i.e. $\exists g \in G$ s.t.

$$qgP = gP \ \forall q \in Q$$

$$\Longrightarrow g^{-1}qg \in P \ \forall q \in Q$$

$$\Longrightarrow Q \leq gPg^{-1}$$

5 Some matrix groups

Let F be a fireld (e.g. $\mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$)

$$GL_n(F) = n \times n \text{ invertible matrices over } F$$

$$SL_n(F) = \ker(GL_n(F) \underset{\det}{\to} F*) \trianglelefteq GL_N(F)$$

Let $Z \trianglelefteq GL_n(F)$ be the subgroup of scalar matrices.

Definition.

$$PGL_n(F) = \frac{GL_n(F)}{Z}$$

$$PSL_n(F) = \frac{SL_n(F)}{Z \cap SL_n(F)} \cong \frac{ZSL_n(F)}{Z} \leq PGL_n(F)$$

Example. Let $G = GL_n(\mathbb{Z}/p\mathbb{Z})$. A list of n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ are the columns of some $A \in G$ iff they are linearly independent

$$\begin{aligned}\therefore |G| &= \underset{1^{\text{st}}\text{ col}}{(p^n - 1)}\underset{2^{\text{nd}}\text{ col}}{(p^n - p)}(p^n - p^2)\dots\underset{\text{last col}}{(p^n - p^{n-1})} \\ &= p^{1+2+\dots+(n-1)}(p^n - 1)(p^{n-1} - 1)\dots(p-1) \\ &= p^{\binom{n}{2}}\prod_{i=1}^{n}(p^i - 1)\end{aligned}$$

So the Sylow p-subgroups have order $p^{\binom{n}{2}}$
One such is the subgroup of upper triangular matrices with 1's on the diagonal

$$U = \{\begin{bmatrix}1 & * & * & \dots \\ 0 & 1 & & \\ 0 & 0 & \ddots & \\ 0 & 0 & \dots & 1\end{bmatrix}\} \leq G$$

Indeed there are $\binom{n}{2}$ entries *, each of which can take p values.

Remark. Just as $PGL_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ via Mobius maps, $PSL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$
Indeed $GL_2(\mathbb{Z}/p\mathbb{Z})$ acts as

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

and since scalar matrices act trivially, this is an action of $PGL_2(\mathbb{Z}/p\mathbb{Z})$

Lemma 5.1. The permutation representation $PGL_2(\mathbb{Z}/p\mathbb{Z}) \to S_{p+1}$ is injective (in fact isomorphism if $p = 2$ or 3)

Proof. Suppose

$$\frac{az+b}{cz+d} = z \; \forall z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$$

Putting $z = 0$ shows $b = 0$
Putting $z = \infty$ shows $c = 0$
Putting $z = 1$ shows $a = d$
Thus

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ is a scalar matrix (diagonal all same scalar) in } PGL_2(\mathbb{Z}/p\mathbb{Z})$$

Lemma 5.2. If p is an odd prime, then

$$|PSL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{p(p-1)(p+1)}{2}$$

Proof. By example earlier,

$$|GL_2(\mathbb{Z}/p\mathbb{Z})| = p(p-1)(p^2-1)$$

Then the group homomorphism $GL_2(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p\mathbb{Z})^*$ is surjective as we have

$$\begin{bmatrix} a & \\ & 1 \end{bmatrix} \mapsto a$$

$$\therefore |SL_2(\mathbb{Z}/pZ)| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{p-1} = p(p-1)(p+1)$$

If $\begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} \in SL_2(\mathbb{Z}/p\mathbb{Z})$ then $\lambda^2 \equiv 1 \pmod p \implies p|(\lambda-1)(\lambda+1) \implies \lambda \equiv \pm 1 \pmod p$
$\therefore$ the only scalar matrices in $SL_2(\mathbb{Z}/p\mathbb{Z})$ are $\pm I$, distinct as $p \neq 2$

$$\therefore |PSL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{1}{2}|SL_2(\mathbb{Z}/p\mathbb{Z}) = \frac{p(p-1)(p+1)}{2}$$

Example. Let $G = PSL_2(\mathbb{Z}/5\mathbb{Z})$. Then

$$|G| = \frac{4 \cdot 5 \cdot 6}{2} = 60 = 2^2 \cdot 3 \cdot 5$$

Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ via

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

By Lemma 5.1, there is an injective group homomorphism

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

Claim.

$$\mathrm{Im}(\phi) \le A_6$$

i.e. $\psi : G \underset{\phi}{\to} S_6 \xrightarrow{\text{sign}} \{\pm 1\}$ is trivial.

Proof. If m is odd, then

$$\psi(g) = 1 \iff \psi(g)^m = 1 \iff \psi(g^m) = 1$$

So suffices to consider $g \in G$ with order a power of 2. Lemma 4.7 $\implies$ every such element belongs to a Sylow 2-subgroup.
So it suffices to check $\psi(H) = 1$ for H a Sylow 2-subgroup. (Using here that any two Sylow 2-subgroups are conjugate and ψ maps to an abelian group)
We take

$$H = \left\langle \pm \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle \le G = \frac{SL_2(\mathbb{Z}/5\mathbb{Z})}{\{\pm I\}}$$

We compute

$$\phi \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = (1\,4)(2\,3) \;\; z \mapsto -z$$

$$\phi \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = (0\,\infty)(1\,4) \;\; z \mapsto -\frac{1}{2}$$

These are even permutations $\therefore \psi(H)$
This proves the claim.
The last part of ES1 Q14 shows that if $G \le A_6$ and $|G| = 60$ then $G \cong A_5$

Note. Facts (not proved in the course):

- $PSL_n(\mathbb{Z}/p\mathbb{Z})$ is a simple group $\forall n \ge 2$, p prime, except $(r, p) = (2, 2)$ or $(2, 3)$
- The smallest non-abelian simple groups are

$$A_5 \cong PSL_2(\mathbb{Z}/5\mathbb{Z}) \text{ order } 60$$

$$PSL_2(\mathbb{Z}/7\mathbb{Z}) \cong GL_3(\mathbb{Z}/2\mathbb{Z}) \text{ order } 168$$

6 Finite Abelian Groups

Later in this course, we prove:

Theorem 6.1. Every finite abelian group is isomorphic to a product of cyclic groups.
However, such a decomposition is not unique

Lemma 6.2. If m and n are coprime then $C_m \times C_n \cong C_{mn}$

Proof. Let g and h be generators of C_m and C_n.
We have $(g,h) \in C_m \times C_n$ and $(g,h)^r = (g^r, h^r)$
In particular

$$(g,h)^r = 1 \iff m|r \text{ and } n|r \quad (1)$$
$$\iff mn|r \quad (2)$$

$\therefore (g,h)$ 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 $n = p_1^{a_1} \dots p_r^{a_r}$ ($p_1, \dots, p_r$ distinct primes) then Lemma 6.2 shows

$$C_n \cong C_{p_1^{a_1}} \times C_{p_2^{a_1}} \times \cdots \times C_{p_r^{a_r}}$$

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

Note. In fact, we will prove the following refinement of Theorem 6.1:

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 $d_1|d_2|\dots|d_t$

Remark. The integers $n_1, \dots, n_k$ in Corollaryy 6.3 (up to order) nd the integers $d_1, \dots, d_t$ in Theorem 6.4 (assuming $d_1 > 1$) are uniquely determined by the group G.
The proof (which we omit) works by counting the number of elements of G of each prime power order.

Examples.
(i) The abelian groups of order 8 are

$$C_8, C_2 \times C_4 \text{ and } C_2 \times C_2 \times C_2$$

(ii) The abelian groups of order 12 are

$$C_2 \times C_2 \times C_3 \; C_4 \times C_3 \text{ using cor. 6.3}$$

$$C_2 \times C_6 \; C_12 \text{ using cor. 6.4}$$

Definition. The **exponent of a group** G is the least integer $n \geq 1$ s.t. $g^n = 1 \; \forall g \in G$ i.e. the $LCM$of all the orders of the elements of G

Example. A_4 has exponent 6.

Corollary 6.5. Every finite abelian group contains an element whose order is the exponent of the group.

Proof. If

$$G \cong C_{d_1} \times \cdots \times C_{d_t} \text{ with } d_1 | d_2 | \dots | d_t$$

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. $\therefore G$ has exponent d_t

7 Rings - Definition and Examples

Definition. A **ring** is a triple $(R, +, \cdot)$ consisting of set R and two binary opertations $+ : R \times R \to R$ and $\cdot : R \times R$ satisfying
(i) $(R, +)$ is an abelian group, with identity 0 $(= 0_R)$
(ii) Multiplication is associative and has an identity i.e.

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

and

$$\exists 1 \in R \text{ s.t. } x \cdot 1 = 1 \cdot x = x \; \forall x \in R$$

(can write $1 = 1_R$)
(iii) Ditributive laws

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

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

Remarks.

(i) As in the case of groups, don't forget to check closure

(ii) For $x \in R$ we write $-x$ for the its inverse under addition and abbreviate $x + (-y)$ as $x - y$

(iii)
$$0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x \implies 0 \cdot x = 0 \ \forall x \in R$$

(iv)
$$0 = 0 \cdot x = (1-1) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x \implies (-1) \cdot x = -x \ \forall x \in R$$

(v) Using (iv), it is possible to deduce $+$ is commutative from the other axioms

Definition. R is **commutative** if
$$x \cdot y = y \cdot x \ \forall x, y \in R$$
In this course, we only consider commutative rings

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

Examples.

(i) We have subrings
$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$$

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

(iii)
$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \leq \mathbb{R}$$

(iv)
$$\mathbb{Z}\left[\frac{1}{p}\right] = \{\frac{m}{p^n} : m \in \mathbb{Z}, n \geq 0\} \leq \mathbb{Q}$$

(v)
$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{ \text{ integers mod } n\}$$

7.1 New rings from old

Examples.

(i) If R and S are rings then their product $R\times$ is a ring via

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

We have

$$0_{R\times S} = (0_R, 0_S) \text{ and } 1_{R\times S} = (1_R, 1_S)$$

> **Note.** $R \times \{0\}$ is not a subring

(ii) If R is a ring, and X is a set then the set of all functions $X \to R$ is a ring under pointwise operations

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

further interesting examples appear as subgrings e.g. continuous functions $\{\mathbb{R} \to \mathbb{R}\}$

(iii) Let R be a ring and S the set of all sequences $(a_0, a_1, a_2, \dots)$ $a_i \in \mathbb{R}$ with $a_i = 0$ $\forall i$ sufficiently large.

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$$

where

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}$$

It may be checked that S is a ring

$$0_S = (0, 0, 0, \dots)$$

$$1_S = (1, 0, 0, \dots)$$

We identify R with the subring

$$\{(a, 0, 0, \dots) : a \in R\} \leq S$$

Define $X = (0, 1, 0, \dots)$. Then

$$X^m = (\underbrace{0, 0, \dots, 0}_{n \text{ zeros}}, 1, 0, \dots)$$

and

$$(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

$\therefore \underset{R[X]}{S}$ is the ring of polynomials with coefficients in R

> **Remark.** Let $R = \mathbb{Z}/p\mathbb{Z}$, p prime and $f(X) = X^p - X$. Then the function $\underset{R\to R}{x \mapsto f(x)}$ is identically zero but the polynomial f is non-zero

Examples (Further Examples)**.**

(i)
$$R[X_1, \ldots, X_n] = \text{ polynomials in } X_1 \ldots, X_n \text{ with coefficients in } R$$
(could define inductively $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$)

(ii) Power series ring
$$R[[X]] = \{a_0 + a_1 X + a_2 X^2 + \ldots | a_i \in R\}$$

(iii) Laurent polynomials
$$R[X, X^{-1}] = \left\{ \sum_{i \in \mathbb{Z}} a_i X^i | a_i \in R, \text{ and only finitely many } a_i \neq 0 \right\}$$

Definition. An element $r \in R$ is a **unit** if it has an inverse under multiplication, i.e. $\exists s \in R$ s.t. $r \cdot s = 1$

Note. 2 is a unit in $\mathbb{Q}$, but not in $\mathbb{Z}$

The units in a ring R form a group $(R^\times, \cdot)$ under multiplication, e.g.
$$\mathbb{Z}^\times = \{\pm 1\}$$
$$\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}$$

Definition. A **field** is a ring with $0 \neq 1$, such that every non-zero element is a unit.
(e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ p prime)

Remark. If R is a ring with $0 = 1$ then
$$x = 1 \cdot x = 0 \cdot x = 0 \ \forall x \in R$$
$$\implies R = \{0\}$$
is the trivial ring

Lemma 7.1. Let $f, g \in R[X]$. Suppose the leading coefficient of g is a unit. Then $\exists\ q, r \in R[X]$ s.t. $f(X) = q(X)g(X) + r(X)$ where $\deg(r) < \deg(g)$

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

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \ a_n \neq 0$$

$$g(X) = b_m X^m + b_{m-1}X^{m-1} + \cdots + b_1 X + b_0 \ b_m \in R^\times$$

If $n < m$, then put $q = 0,\ r = f$✓
Otherwise we have $n \geq m$ and we put $f_1(X) = f(X) - a_n b_m^{-1} X^{n-m} g(X)$
Coeff of X_n is $a_n - a_n b_m^{-1} b_m = 0$

$$\therefore \deg(f_1) < n$$

By induction hypothesis,

$$f_1(X) = q_1(X)g(X) + r(X) \ \deg(r) < \deg(g)$$

$$\implies f(X) = \underbrace{q(X)}_{(q_1(X) + a_n b_n^{-1} X^{n-m})} g(X) + r(X)$$

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

8 Ideals and Quotients

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

(i)
$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \ \forall r_1, r_2 \in R$$

(ii)
$$\phi(r_1 r_2) = \phi(r_1)\phi(r_2) \ \forall r_1, r_2 \in R$$

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

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

Definition. The **kernel** of ϕ is

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

Lemma 8.1. A ring homomorphism is injective if

$$\ker(\phi) = \{0_R\}$$

Proof.

$$\phi : (R, +) \to (S, +)$$

is a group homomorphism, so lemma follows from corresponding result for groups

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

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

(ii) $r \in R$ and $x \in I \implies rx \in I$

Remark. If I contains 1 (or more generally if I contains a unit) then by (ii), we have $I = R$. Hence if R is a field then the only ideals are $\{0\}$ and R.

Definition. 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 in R

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

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0 = 0 \implies rx \in \ker(\phi)$$

Lemma 8.3. The ideals in $\mathbb{Z}$ are $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$

Proof. Certainly $n\mathbb{Z} \trianglelefteq \mathbb{Z}$
Let $I \trianglelefteq \mathbb{Z}$ be a non-zero ideal, so a subgroup of $(\mathbb{Z}, +)$
Let n be the least positive integer in I.
Then $n\mathbb{Z} \subseteq I$
If $m \in I$ then write $m = qn + r$ with $q, r \in \mathbb{Z},\ 0 \leq r < n$
Then

$$r = m - qn \in I$$

This contradicts the choice of n unless $r = 0$

$$\therefore I = n\mathbb{Z}$$

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

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_i \in \mathbb{R}\} \trianglelefteq R$$

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

Note. Lemma 8.3 shows that every ideal in $\mathbb{Z}$ is principal

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

$$(r_1 + I) + (r_2 + I) = r_1 + r_2 + I$$

$$(r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I$$

and

$$0_{R/I} = 0_R + I$$

$$1_{R/I} = 1_R + I$$

Moreover the map $r \underset{R \to R/I}{\mapsto} r + I$ is a ring homomorphism (called the quotient map) with kernel I

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

$$r_1' = r_1 + a_1 \text{ and } r_2' = r_2 + a_2 \; a_1, a_2 \in I$$

Then

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

$$\therefore r_1' r_2' + I = r_! r_2 + I$$

The remaining properties to show R/I is a ring follow from those of R

Examples.

(i) We have $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ with quotient ring $\mathbb{Z}/n\mathbb{Z}$
This ring has elements
$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}.$$
Addition and multiplication are carried out mod n

(ii) Consider $(X) \trianglelefteq \mathbb{C}[X]$
This is the ideal of polynomials whose constant term is 0. If
$$f(X) = a_n X^n + \cdots + a_1 X + a_0 \ a_i \in \mathbb{C}$$
Then
$$f(X) + (X) = a_0 + (X)$$
There is a bijection
$$\frac{\mathbb{C}[X]}{(X)} \leftrightarrow \mathbb{C}$$
$$f(X) + (X) \mapsto f(0)$$
$$a + (X) \mapsfrom a$$
These maps are ring homomorphisms
$$\therefore \frac{\mathbb{C}[X]}{(X)} \cong \mathbb{C}$$

(iii)
$$\frac{\mathbb{R}[X]}{(X^2+1)} = \{f(X) + (X^2+1) : f(X) \in \mathbb{R}[X]\}$$
By Lemma 7.1
$$f(X) = q(X)(X^2+1) + r(X)$$
with deg $r < 2$, i.e.
$$r(X) + a + bX \ a \in \mathbb{R}$$
$$\therefore \frac{\mathbb{R}[X]}{X^2+1} = \{a + bX + (X^2+1) : a, b \in \mathbb{R}\}$$
If
$$a + bX + X^2 + 1 = a' + b'X + X^2 + 1$$
then
$$a - a' + (b - b') = q(X)(X^2+1) \text{ for some } q \in \mathbb{R}[x]$$
Comparing degrees we see $q(X) = 0$ and $a = a', \ b = b'$

Examples.

(iii) (continued) $\therefore$ There is a bijection

$$\frac{\mathbb{R}[X]}{(X^2+1)} \overset{\phi}{\leftrightarrow} \mathbb{C}$$

$$a + bX + (X^2+1) \mapsto a + bi$$

We show ϕ is a ring homomorphism. It preserves addition and maps $1 + (X^2+1)$ to 1

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

$$\therefore \frac{\mathbb{R}[X]}{(X^2+1)} \cong \mathbb{C}$$

8.1 First Isomorphism Theorem

Theorem 8.5 (First Isomorphism Theorem)**.** let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \trianglelefteq R$ and

$$R/\ker(\phi) \cong \mathrm{Im}(\phi) \leq S$$

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

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

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

$\therefore$ $\mathrm{Im}(\phi)$ is a subgring of S.
Let $K = \ker(\phi)$
We define

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

$$r + K \mapsto \phi(r)$$

this is well defined, a bijection and a group homomorphism under $+$, by the first isomorphism theorem for groups.
Also

$$\Phi(1_R + K) = \phi(1_r) = 1_s$$

and

$$\Phi((r_1+K)(r_2+K)) = \Phi(r_1 r_2 + K) = \phi(r_1 r_2) = \phi(r_1)\phi(r_2) = \Phi(r_1+K)\Phi(r_2+K)$$

$\therefore$ Φ is an isomorphism of rings

8.2 Second Isomorphism Theorem

Theorem 8.6 (Second Isomorphism Theorem)**.** Let $R \leq S$ and $J \trianglelefteq S$. Then

$$R \cap J \trianglelefteq R$$

$$R + J \leq S$$

and

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

Proof. Clearly $R + j$ is a subgroup of $(S, +)$
It contains 1 (since $1 \in R$ and $0 \in J$) and if $r_1 r_2 \in R,\ x_1 x_2 \in J$

$$(r_1 + x_1)(r_2 + x_2) = \underbrace{r_1 r_2}_{\in R} + \underbrace{r_1 x_2 + r_2 x_2 + x_1 x_2}_{\in J} \in R + J$$

$$\therefore R + J \leq S$$

Let $\phi : R \to S/J$, $r \mapsto r + J$
This is the composite of the inclusion $R \subseteq S$ and the quotient map $S \to S/J$, therefore a ring homomorphism

$$\ker(\phi) = \{r \in R | r + J = J\} = R \cap J \trianglelefteq R$$

$$\mathrm{Im}(\phi) = \{r + J | r \in R\} = \frac{R+J}{J} \leq \frac{S}{J}$$

Apple the first isomorphism theorem.

Remark. To motivate the 3^{rd} isomorphism theorem, we note there is a bijection

$$\{\text{ ideals in } R/I\} \leftrightarrow \{\text{ideals of } R \text{ containing } I\}$$

$$K \mapsto \{r \in R | r + I \in K\}$$

$$J/I \hookleftarrow J$$

8.3 Third Isomorphism Theorem

Theorem 8.7 (Third Isomorphism Theorem)**.** Let $I \trianglelefteq R,\ J \trianglelefteq R$ with $I \subseteq J$
Then

$$J/I \trianglelefteq R/I$$

and

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

Proof. Consider $\phi : R/I \to R/J$

$$r + I \mapsto r + J$$

This is a ring homomorphism (well-defined since $I \subseteq J$)

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

$$\mathrm{Im}(\phi) = R/J$$

Apply the first isomorphism theorem.

Example. There is a surjective ring homomorphism

$$\mathbb{R}[X] \to \mathbb{C}$$

$$f(X) = \sum a_n X^n \mapsto f(i) = \sum a_n i^n$$

Using Lemma 7.1, we find

$$\ker(\phi) = (X^2 + 1)$$

$$\text{First isomorphism thm} \implies \frac{\mathbb{R}[X]}{(X^2+1)} \cong \mathbb{C}$$

Example. For any ring R, there is a unique ring homomorphism $\iota : \mathbb{Z} \to R$
It is given by:

$$0 \mapsto 0_R$$

$$1 \mapsto 1_R$$

$$n \mapsto 1_R + \cdots + 1_R$$

$$-n \mapsto -(1_R + \cdots + 1_R)$$

Since $\ker(\iota) \trianglelefteq \mathbb{Z}$, we have $\ker(\iota) = n\mathbb{Z}$ for some $n \in \{0, 1, 2, \dots\}$
By the first isomophism theorem

$$\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Im}(\iota) \leq R$$

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

Remark. If $\mathrm{char}(R) = n > 0$, then n is the order of 1 in $(R, +)$

9 Integral Domains, Maximal Ideals and Prime Ideals

Definition. An **integral domain** is a ring R with $0 \neq 1$ such that for $a, b \in R$

$$ab = 0 \implies a = 0 \text{ or } b = 0$$

A zerodivisor 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 without zero divisors.

Examples.

(i) All fields are integral domains (if $ab = 0$ with $b \neq 0$ then multiplying by b^{-1} shows that $a = 0$)

(ii) Any subring of an integral domain is an integral domain, e.g. $\mathbb{Z}[i] \leq \mathbb{C}$

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

Lemma 9.1. R an integral domain $\implies$ $R[X]$ an integral domain.
Moreover if $f, g \in R[X]$ non-zero then

$$\deg(fg) = \deg(f) + \deg(g)$$

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

$$f(X)g(X) = \underbrace{a_m b_n}_{\neq 0} X^{m+n} + \ldots$$

non-zero as R is an integral domain
$\therefore fg \neq 0$ and $\deg(fg) = m + n = \deg(f) + \deg(g)$

Lemma 9.2. Let R be an integral domain, and $0 \neq f \in R[X]$
Let

$$\text{Roots}(f) = \{a \in R : f(a) = 0\}$$

Then $\#\text{Root}(f) \leq \deg(f)$

Proof. See example sheet

Theorem 9.3. Any finite subgroup of the multiplicative group of a field is cyclic

Proof. Let F be a field and $A \leq F^*$ a finite subgroup.
A is a finite abelian group. If it is not cyclic then by Theorem 6.4 (= structure theorem for finite abelian groups) it contains a subgroup isomorphic to $C_m \times C_m$ for some $m \geq 2$. But then the polynomial

$$f(X) = X^m - 1 \in F[X] \text{ has degree } m \text{ and } \geq m^2 \text{ roots}$$

Contradicting lemma 9.2

Examples.

$$(\mathbb{Z}/p\mathbb{Z})^* \text{ is cyclic}$$

$$\mu_m = \{z \in \mathbb{C} : z^m = 1\} \leq \mathbb{C}^k \text{ is cyclic}$$

Prop 9.4. Any finite integral domain is a field

Proof. Let R be a finite integral domain.
Let $0 \neq a \in R$. Consider the map $\phi : R \to R$

$$x \mapsto ax$$

If $\phi(x) = \phi(y)$ then

$$a(x-y) = 0 \implies x - y = 0 \implies x = y$$

(as R an integral domain and $a \neq 0$)
$\therefore \phi$ is injective
R finite $\implies$ ϕ is surjective
$\implies \exists b \in R$ s.t. $ab = 1$, i.e. a is a unit
$\therefore R$ is a field

Theorem 9.5. Let R be an integral domain. There is a field F such that

(i) $R \leq F$, and

(ii) Every element of F may 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

$$S = \{(a, b) : a, b \in R,\ b \neq 0\}$$

and the equivalence relation $\sim$ on S given by

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

This is 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 is 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 a/b for $[(a, b)]$.
Define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

It may be checked that these operations are well-defined, and make F into a ring with

$$0_F = \frac{0_R}{1_R} \text{ and } 1_F = \frac{1_R}{1_R}$$

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

(i) We identify R with

$$\left\{\frac{r}{1} : r \in R\right\}$$

(ii)

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

Examples.

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

(ii) $\mathbb{Z}[i]$ has field of fractions

$$F = \{ab^{-1} : ab \in \mathbb{Z}[i],\ b \neq 0\} \leq \mathbb{C}$$

In fact

$$F = \{x + iy : x, y \in \mathbb{Q}\}$$

(iii) $\mathbb{C}[X]$ has field of fractions

$$\mathbb{C}(X) = \text{field of rational functions in } X$$

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

Proof. "$\implies$" If $0 \neq I \trianglelefteq R$ then I contains a unit and hence $I = R$
"$\impliedby$" If $0 \neq x \in R$ then the principal ideal (x) is non-zero. Hence,

$$(x) = R$$

So $\exists y \in R$ s.t. $xy = 1$ i.e. x is a unit

Definition.
(i) Let S be a collection of subsets of a set X.
$A \in S$ is **maximimal** if $\nexists B \in S$ s.t. $A \subsetneq B$
(ii) An ideal $I \trianglelefteq R$ is **maximal** if it is maximal among all proper ideals of R
(i.e. $I \neq R$ and $\nexists J \trianglelefteq R$ with $I \subsetneq J \subsetneq R$)

Prop 9.7. Let $I \trianglelefteq R$ be an ideal

$$I \text{ is maximal} \iff R/I \text{ is a field}$$

Proof. R/I is a field $\iff$ I/I and R/I are the only ideals in R/I
$\iff$ I and R are the only ideals in R containing I
$\iff$ $I \trianglelefteq R$ is maximal

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

Example. The ideal $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is a prime ideal iff $n = 0$ or $n = p$ is a prime number.
Indeed if $ab \in p\mathbb{Z}$ then $p|ab$, so $p|a$ or $p|b$ so $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.
Conversely, if $n = uv$ is composite (so $u, v > 1$) then $uv \in n\mathbb{Z}$, yet $u \notin n\mathbb{Z},\ v \notin n\mathbb{Z}$

Prop 9.8. Let $I \trianglelefteq R$ be an ideal

$$I \text{ is prime} \iff R/I \text{ is an integral domain}$$

Proof. I is prime
$\iff$ whenever $a, b \in R$ with $ab \in I$, we have $a \in I$ or $b \in I$
$\iff$ whenever $a + I, b + I \in R/I$ with $(a + I)(b + I) = 0 + I$ we have $a + I = 0 + I$ or $b + I = 0 + I$
$\iff$ R/I is an integral domain

Remark. Proposition 9.7 and 9.9 show that

$$I \text{ maximal} \implies I \text{ prime}$$

Remark. If $\text{char}(R) = n$ 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

$$\implies n\mathbb{Z} \trianglelefteq \mathbb{Z} \text{ is a prime ideal}$$

$$\implies n = 0 \text{ or } n = p \text{ is a prime}$$

In particular any field either has characteristic 0 (and so contains $\mathbb{Q}$ as a subfield) or else has characteristic p (and so contains $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ as a subfield)

10 Factorisation in Integral Domains

Note. In this section R is always an integral domain

Definition.

(i) $a \in R$ is a **unit** if $\exists b \in R$ with $ab = 1$, equivalently $(a) = R$

(ii) $a \in R$ divides $b \in R$ (written $a|b$) if $\exists c \in R$ s.t. $b = ac$, equivalently,

$$(b) \subseteq (a)$$

(iii) $a, b \in R$ are **associates** if $a = bc$ for some unit $c \in R$, equivalently

$$(a) = (b)$$

(iv) $r \in R$ is **irreducible** if it is not zero not a unit and

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

(v) $r \in R$ is **prime** if it is not zero, not a unit and

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

Remark. These properties depend on the ambient ring R
e.g. 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) is a prime ideal in $R \iff r = 0$ or r is a prime

Proof. "$\implies$" Suppose (r) is prime and $r \neq 0$.
As prime ideals are proper, $(r) \neq R$, so r is not a unit
If $r|ab$ then $ab \in (r)$ so $a \in (r)$ or $b \in (r)$
so $r|a$ or $r|b$
$\therefore r$ is prime
"$\impliedby$" $\{0\} \trianglelefteq R$ is a prime ideal since R is an integral domain.
Let $r \in R$ be prime. If $ab \in (r)$ then $r|ab$ so $r|a$ or $r|b$, so $a \in (r)$ or $b \in (r)$
$\therefore (r)$ is a prime ideal

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

Proof. Since r is prime, it is not zero and not a unit
Suppose $r = ab$. Then $r|ab$, so $r|a$ or $r|b$
Let's suppose $r|a$, say $a = rc$ some $c \in R$.
Then
$$r = ab = rcb \implies r(1 - bc) = 0$$
as $r \neq 0$ and R is an integral domain
$$1 - bc = 0$$
so b is a unit
Likewise if $r|b$ then a is a unit

Warning. The converse does NOT hold in general

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

Claim. The units in R are ± 1.

Proof. If $r \in R$ is a unit i.e. $rs = 1$ for some $s \in R$ then
$$N(r)N(s) = N(rs) = N(1) = 1 \implies N(r) = 1$$
But the only integer solutions to $a^2 + 5b^2 = 1$ are $(a, b) = (\pm 1, 0)$

Claim. $2 \in R$ is irreducible

Proof. Suppose $2 = rs$ some $r, s \in R$. taking norms we get
$$N(r)N(s) = 4$$
Since $a^2 + 5b^2 = 2$ has no solutions with $a, b \in \mathbb{Z}$, there are no elements of norm 2.
$\therefore N(r) = 1$ and $N(s) = 4$ or vice versa. But $N(r) = 1 \implies r$ is a unit

Note. Similarly, $3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible, as there are no elements of norm 3.
We have $(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$
yet $2 \nmid 1+\sqrt{-5}$ and $2 \nmid 1-\sqrt{-5}$
Seen by taking norm or by noting that $\frac{1 \pm \sqrt{-5}}{2} \notin R$
2 lessons:

(i) irreducible $\not\Longrightarrow$ prime
(ii) $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ gives two factorisations into irreducibles

Remark. Since the only units in R are ± 1, it is clear that the irreducibles in (ii) are not associates.

Definition. An integral domain R is called a **principal ideal domain (PID)** if every ideal of R is principle, i.e. is of the form (a) for some $a \in R$
e.g. $\mathbb{Z}$ is a PID by Lemma 8.3
We will show that $\mathbb{Z}[i]$ and $\mathbb{F}[X]$ for $\mathbb{F}$ a field are PIDs

Lemma 10.3. Let $0 \neq r \in R$. If (r) is a maximal ideal then r is irreducible and the converse holds if R is a PID.

Proof. we have $r \neq 0$ (by assumption) and r is not a unit (since maximal ideals are proper).
Suppose $r = ab$ with $a, b \in R$.
Then
$$(r) \subseteq (a) \subseteq R$$
$$(r) \text{ maximal} \implies \text{either } (r) = (a) \text{ or } (a) = R$$
$$(r) = (a) \implies b \text{ is a unit}$$
$$(a) = R \implies a \text{ is a unit}$$
$\therefore r$ is irreducible.
Conversely, suppose r is irreducible and $(r) \subseteq J \subseteq R$
$$\begin{aligned} R \text{ is PID} &\implies J = (a) \text{ for some } a \in R \\ &\implies r = ab \text{ for some } b \in R \end{aligned}$$
Since r is irreducible either:
$$a \text{ is a unit} \implies J = R$$
or
$$b \text{ is a unit} \implies (r) = J$$
$\therefore (r)$ is maximal

Prop 10.4. Let R be a PID. Then every irreducible element of R is prime.

Proof (Version 1)**.** Let $p \in R$ be irreducible and $p|ab$ and $\nmid a$.
R is a PID $\implies (a,p) = (d)$ for some $d \in R$
In particular $p = cd$ for some $c \in R$
Since p is irreducible either c or d is a unit.
If c is a unit then

$$(a,b) = (p), \text{ so } p|a ※$$

If d is a unit then $(a,p) = R$

$$\text{so } \exists r, s \in R \text{s.t.} ra + sp = 1$$

Then $b = rab + spb$ and since $p|ab$ we get $p|b$
$\therefore p$ is prime

Proof (Version 2)**.** p irreducible $\implies (p)$ is maximal (lemma 10.3)
$\implies R/(p)$ is a field
$\implies R/(p)$ is an integral domain
$\implies (p)$ is prime
$\implies p$ is prime

Definition. An integral domain R is a **Euclidean domain (ED)** if there is a function

$$\phi : R\backslash\{0\} \to \mathbb{Z}_{\geq 0} \text{ (a Euclidean function)}$$

such that
(i) if $a|b$ then $\phi(a) \leq \phi(b)$
(ii) if $a, b \in R$ with $b \neq 0$ then $\exists q, r \in R$ with $a = qb + r$ and either $r = 0$ or $\phi(r) < \phi(b)$

Prop 10.5. If R is a Euclidean domain then it is a principal ideal domain
(i.e. ED $\implies$ PID)

Proof. Let R have Euclidean function

$$\phi : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$$

Let $I \trianglelefteq R$ be a non-zero ideal choose $b \in I\backslash\{0\}$ with $\phi(b)$ minimal
We have $(b) \subseteq I$.
For $a \in I$ we write

$$a = qb + r$$

with $q, r \in R$ and either $r = 0$ or $\phi(r) \leq \phi(b)$
Since $r = a - qb \in I$, this contradicts the choice of b, unless $r = 0$
But then $a = qb \in (b)$.
Hence

$$I = (b)$$

Remark. We only used (ii) here. The reason for including (i) in the definition of ED is that it allows us to describe the units as

$$R^\times = \{u \in R\backslash\{0\} | \phi(u) = \phi(1)$$

Examples.

(i) $\mathbb{Z}$ is a Euclidean domain with $\phi(n) = |n|$

(ii) If F is a field, then $F[X]$ is a Euclidean domain with

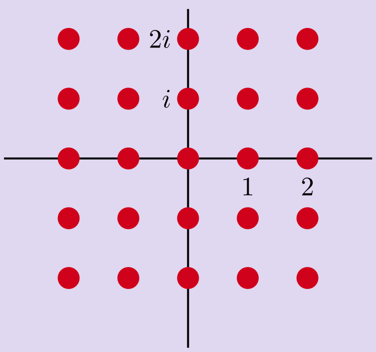
$$\phi(f) = \deg(f)$$

(see Lemma 7.1 and 9.1)

(iii) $R = \mathbb{Z}[i] \leq \mathbb{C}$ is a Euclidean domain with

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

Since $N(z_1 z_2) = N(z_1)N(z_2)$ property under (i) is clear
For property (ii), let $z_1, z_2 \in \mathbb{Z}[i]$ with $z_2 \neq 0$
Consider $z_1/z_2 \in \mathbb{C}$. This has distance les than 1 from the nearest element of $\mathbb{Z}[i]$



So we can write

$$\frac{z_1}{z_2} = q + \varepsilon$$

where $q \in \mathbb{Z}[i],\ \varepsilon \in \mathbb{C},\ |\varepsilon| < 1$

$$\implies z_1 = qz_2 + \underbrace{\varepsilon z_r}_{r}$$

$$r = z_1 - qz_2 \in \mathbb{Z}[i]$$

and

$$\phi(r) = |\varepsilon z_2|^2 < |z_2|^2 = \phi(z_2)$$

It follows from prop 10.5 that $F[X]$ for F a field nd $\mathbb{Z}[i]$ are PID's.

Example. Let A be a $n \times n$ matrix over a field F. Let

$$I = \{f \in F[X] : f(A) = 0\}$$

If $f, g \in I$ then $(f + g)(A) = f(A) + g(A) = 0$, so $f + g \in I$
If $f \in F[X], g \in I$ then $(fg)(A) = f(A)g(A) = 0$
So I is an ideal in $F[X]$
$F[X]$ is a PID $\implies I = (f)$ for some $f \in F[X]$, which we may suppose monic by multiplying by a unit.
Note that for $g \in F[X]$

$$g(A) = 0 \iff g \in I \iff g \in (G) \iff f|g$$

We say f is the minimal polynomial of A

Example. Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ be the field with 2 elements
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 one of these factors is linear, and so f has a root. But $f(0 \neq 0$ and $f(1) \neq 0$
$\therefore g$ is irreducible.
Since $\mathbb{F}_2[X]$ is a PID, it follows from Lemma 10.3 that $(f) \trianglelefteq \mathbb{F}_2[X]$ is maximal, hence

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

is a field of order 8

Example. The ring $\mathbb{Z}[X]$ is not a PID
Indeed consider $(2, X) \trianglelefteq \mathbb{Z}[X]$
Then

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

Suppose $I = (f)$ for some $f \in \mathbb{Z}[X]$
Then $2 = fg$ for some $g \in \mathbb{Z}[X]$

$$\therefore \deg(f) = \deg(g) = 0$$

$$\therefore f = \pm 1 \text{ or } \pm 2$$

$$\therefore I = \mathbb{Z}[X] \text{ or } 2\mathbb{Z}[X]$$

$I = \mathbb{Z}[X]$ is impossible as $1 \notin I$, $2\mathbb{Z}[X]$ impossible as $X \in E$

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

(i) every non-zero, non unit is a product of irreducibles
(ii) if $p_1 \dots p_m = q_1 \dots q_n$ where p_1 and q_i are irreducibles then $m = n$ and e may reorder s.t.p_i is an associate of q_i $\forall 1 \leq i \leq n$

Prop 10.6. Let R be an integral domain satisfying (i) in the definition of UFD. Then R is a UFD $\iff$ every irreducible in R is prime

Proof. " $\implies$ " suppose $p \in R$ is irreducible, and $p|ab$, say

$$ab = pc$$

for some $c \in R$
Writing a, b, c as products of irreducibles, it follows from (ii) that $p|a$ or $p|b$.

$$\therefore p \text{ is prime}$$

" $\impliedby$ " suppose $p_1 \dots p_m = q_1 \dots q_n$ with each p_1 and q_i irreducible.
Since p_1 is prime and $p_1|q_1 \dots q_n$ we have $p_1|q_i$ for some i. After some reordering, we may assume $p_1|q_1$ i.e.

$$q_1 = up_1$$

for some $u \in R$. But q_1 is irreducible and p_1 is not a unit, so u is a unit

$$\therefore p_1 \text{ and } q_1 \text{ are associates}$$

Cancelling p_1 gives $p_2 \dots p_m = (uq_2) \dots q_n$
The result then follows by induction

Lemma 10.7. Let R be a PID and

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

a nested sequence of ideals. Then $\exists N \in \mathbb{N}$ s.t. $I_n = I_{n+1}$ $\forall n \geq N$.
(Rings satisfying this "ascending chain condition" are called Noetherian - more on this later)

Proof. Let

$$I = \bigcup_1^\infty I_i$$

This is an ideal in R.
As R is a PID, we have

$$I = (a) \text{ for some } a \in R$$

Then

$$a \in \bigcup_{i=1}^\infty I_i$$

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. We must check (i) and (ii) in the definition of UFD

(i) Let $0 \neq x \in R$, not a unit. Suppose it is not a product of irreducibles. Then x is not irreducible, so can write

$$x = x_1 y_1$$

where x_1, y_1 are not units.
One or other of x_1 and y_1 is not a product of irreducibles. Let's say it's x_1.
we have $(x) \subseteq (x_1)$ and this inclusion is strict since y_1 is not a unit.
Now write

$$x_1 = x_2 y_2$$

where x_2, y_2 are not units. Repeating in this way we obtain

$$(x) \subset (x_1) \subset (x_2) \subset \dots \text{※}$$

(contradicts lemma 10.7)

(ii) By proposition 10.6, it suffices to show that irreducibles are prime, which we proved in proposition 10.4.

Examples.

	ED $\implies$	PID $\implies$	UFD $\implies$	integral domain
$\mathbb{Z}/4\mathbb{Z}$	X	X	X	X
$\mathbb{Z}[\sqrt{-5}]$	X	X	X	✓
$\mathbb{Z}[X]$	X	X	✓	✓
$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$	X	✓	✓	✓

See next section and part II number fields for 3^{rd} and 4^{th}

Definition. Let R be an integral domain

(i) $d \in R$ is a **greatest divisor** of $a_1, \dots, a_n \in R$ written

$$d = \gcd(a_1, \dots, a_n)$$

if $d | a_i \ \forall i$ and if $d' | a_i \forall i \implies d' \mid d$

(ii) $m \in R$ is a **least common multiple** written

$$m = \text{lcm}(a_1, \dots, a_n)$$

if $a_i | m \ \forall i$ and $a_i | m' \ \forall i \implies m | m'$

Both gcd's and lcm's (when they exist) are unique up to multiplying by a unit

Prop 10.9. In a UFD, both lcm's and gcd's exists

Proof. Write

$$a_i = u_i \prod_j p_j^{n_{ij}} \ \forall 1 \leq i \leq n$$

where u_i is a unit, the p_j are irreducibles which are not associates of each other and $n_{ij} \in \mathbb{Z}_{\geq 0}$ we claim that

$$d = \prod_j p_j^{m_j}$$

where

$$m_j = \min_{1 \leq i \leq n} n_{ij}$$

is the gcd of $a_1, \ldots, a_n$.
Certianly $d | a_i \ \forall i$. If $d' | a_i \ \forall i$ then writing

$$d' = u \prod_j p_j^{t_j}$$

we find $t_k \leq n_{ij} \ \forall i$ and so $t_j \leq m_j$. therefore $d' | d$.
The argument for lcm's is similar.

11 Factorisation in Polynomial Rings

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

Proof. Comes a bit later.

Remark. Repeatedly applying this result shows that if R is a UFD then $R[X_1, \ldots, X_n]$ is a UFD. In particular, the theorem shows that $\mathbb{Z}[X]$ and $\mathbb{C}[X_1, \ldots, X_n]$ are UFD's.

Note. In this section R is a UFD with field of fractions F. We have $R[X] \leq F[X]$.
Moreover, $F[X]$ is a ED, hence a PID & UFD.

Definition. The **content** of

$$f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$$

is

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

We say f is **primitive** if $c(f)$ is a unit, i.e. all a_i are coprime

Lemma 11.2.

(i) Any prime in R is also prime in $R[X]$

(ii) If $f, g \in R[X]$ are primitive, then fg are primitive

(iii) If $f, g \in R[X]$ then $c(fg) = c(f)c(g)$

Proof.

(i) Let $p \in R$ be a prime, so $R/(p)$ is an integral domain.
For $a \in R$, we write $\tilde{a} \in R/(p)$ for its image under the quotient map.
We define a ring homomorphism $\theta : R[X] \to R/(p)[X]$

$$a_n X^n + \cdots + a_1 X + a_0 \mapsto \tilde{a_n} X^n + \cdots + \tilde{a_1} X + \tilde{a_0}$$

If $f, g \in R[X]$ with $p|fg$ then $\theta(fg) = 0$

$$\implies \theta(f)\theta(g) = 0$$

and as $R/(p)[X]$ is an integral domain, by Lemma 9.1.

$$\theta(f) = 0 \text{ or } \theta(g) = 0$$

$$\implies p|f \text{ or } p|g \therefore p \text{ is prime in } R[X]$$

(ii) If fg is not primitive then $\exists p \in R$ irreducible with $p|fg$.
Since R is a UFD, p is prime. By (i) we have $p|f$ or $p|g$, contradicting f & g primitive

(iii) We write $f = c(f)f_0$ and $g = c(g)g_0$ where $f_0 g_0 \in R[X]$ primitive.
Then

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

and we have $f_0 g_0$ primitive by (ii)

$$\therefore c(fg) = c(f)c(g)$$

(up to multiplication by units)

Remark. If $f \in F[X]$ then we can write

$$f = \frac{a}{b} f_0 \text{ where } a, b \in R,\ b \neq 0 \text{ and } f_0 \in R[X] \text{ primitive}$$

Indeed, by clearing denominators we may find $0 \neq b \in R$ s.t. $bf \in R[X]$.
Then $bf = \underbrace{c(bf)}_{a} f_0$ for some $f_0 \in R[X]$ primitive.

Lemma 11.3. Let $f, g \in R[X]$ with g primitive.
If $g|f$ in $F[X]$ then $g|f$ in $R[X]$.

Proof. Write $f = gh$ with $h \in F[X]$.
By the remark,

$$h = \frac{a}{b}h_0 \ a, b \in R, \ b \neq 0, \ h_0 \in R[X] \text{ primitive}$$

Then

$$f = g\frac{a}{b}h_0 \implies bf = agh_0$$

and gh_0 primitive by Lemma 11.2
Taking contents shows $b|a$, hence $h \in R[X]$, hence $g|f$ in $R[X]$

Lemma 11.4 (Gauss' Lemma)**.** Let R be a UFD with field of fractions F.
Let $f \in R[X]$ be primitive. Then

$$f \text{ irred in } R[X] \implies f \text{ irred in } F[X]$$

Proof. Since $f \in R$ is irreducible and primitive we have $\deg(f) > 0$, and so f is not a unit in $F[X]$.
Suppose for a contradiction that f is not irreducible in $F[X]$, say $f = gh$ where $g, h \in F[X]$ with $\deg(g)$, $\deg(h) > 0$.
Replacing g & h by λg and $\lambda^{-1}h$ for some $\lambda \in F^*$, we may assume $g \in R[X]$ is primitive.
Then Lemma 11.3 shows $h \in R[X]$.
Now $f = gh$ where $g, h \in R[X]$, with $\deg(g)$, $\deg(h) > 0$.
This contradicts that f is irred in $R[X]$

Lemma 11.5. Let $g \in R[X]$ be primitive. Then

$$g \text{ prime in } F[X] \implies g \text{ is prime in } R[X]$$

Proof. Suppose $f_1, f_2 \in R[X]$ and $g \mid f_1f_2$ in $R[X]$

$$\begin{aligned} g \text{ is prime in } F[X] &\implies g|f_1 \text{ or } g|f_2 \text{ in } F[X] \\ &\implies g|f_1 \text{ or } g|f_2 \text{ in } R[X] \end{aligned}$$

$\therefore g$ is prime in $R[X]$

Proof (of Theorem 11.1)**.** Let $f \in R[X]$
Write $f = c(f) f_0$ where $f_0 \in R[X]$ is primitive.
R a UFD $\implies c(f)$ is a product of irreducibles in R (which are also irreducibles in $R[X]$)
If f_0 i not irreducible, say $f_0 = gh$ then the factors g and h have smaller degree (using that f_0 is primitive) and are again primitive.
By induction on the degree, f_0 is a product of irreducibles in $R[X]$
It remains to show (see Prop 10.6) that if $f \in R[X]$ is irreducible then it is prime.
Again write $f = c(f) f_0$ where $f_0 \in R[X]$ primitive.

$$f \text{ irred} \implies f \text{ is either constant or primitive}$$

Case f constant:

$$\begin{aligned} f \text{ irred in } R[X] &\implies f \text{ irred in } R \\ &\implies f \text{ prime in } R \text{ as } R \text{ is a UFD} \\ &\implies f \text{ prime in } R[X] \text{ (Lemma 11.2(i))} \end{aligned}$$

Case f primitive:

$$\begin{aligned} f \text{ irred in } R[X] &\implies f \text{ irred in } F[X] \text{ (Gauss' Lemma)} \\ &\implies f \text{ prime in } F[X] \text{ } (F[X] \text{ a UFD}) \\ &\implies f \text{ prime in } R[X] \text{ (Lemma 11.5)} \end{aligned}$$

Remark. In view of Lemma 10.2, the last three " $\implies$ " are " $\iff$ "

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

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

11.1 Eisenstein's Criterion

Claim. 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

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

Then f irreducible in $R[X]$

Proof. Suppose $f = gh, \; g, h \in R[X]$ not units. f primitive $\implies \deg(g), \deg(h) > 0$.
Let $g = r_kX^k + \cdots + r_1X + r_0$ and $h = s_lX^l + \cdots + s_1X + s_0$ with $k + l = n$ then $p \nmid a_n = r_ks_l \implies p \nmid r_k$ and $p \nmid s_l$.
$p \mid a_0 = r_0s_0 \implies p \mid r_0$ or $p \mid s_0$, wlog $p \mid r_0$.
Then $\exists j \leq k$ s.t. $p \mid r_0, \; p \mid r_1, \ldots, p \mid r_{j-1}, p \nmid r_j$

$$\underbrace{a_j}_{\text{div. by } p} = \underbrace{r_0s_j + r_1s_{j-1} + \cdots + r_{j-1}s_1}_{\text{div. by } p} + r_js_0$$

Thus $p \mid r_js_0 \implies p \mid s_0 \implies p^2 \mid r_0s_0 = a_0$※

Example. (i) $X^3 + 2X + 5 \in \mathbb{Z}[X]$ If f not irreducible in $\mathbb{Z}[X]$ then

$$f(X) = (X + a)(X^2 + bX + x) \text{ some } a, b, c \in \mathbb{Z}$$

Thus $ac = 5$. But $\pm 1, \; \pm 5$ are not roots of f ※.
By Gauss' Lemma, f irreducible in $\mathbb{Q}[X]$. Thus $\mathbb{Q}[X]/(f)$ is a field (Lemma 10.4)

(ii) Let $p \in \mathbb{Z}$ prime. eisenstein's criterion $\implies X^n - p$ irreducible in $\mathbb{Z}[X]$, hence irreducible in $\mathbb{Q}[X]$ by Gauss' Lemma

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

$$f(Y+1) = \frac{(Y+1)^p - 1}{Y + 1 - 1} = Y^{p-1} + \binom{p}{1}Y^{p-2} + \cdots + \binom{p}{p-2}Y + \binom{p}{p-1} \in \mathbb{Z}[Y]$$

Now $p \mid \binom{p}{i} \; \forall 1 \leq i \leq p-1$ and $p^2 \nmid \binom{p}{p-1} = p$. Thus $f(Y+1)$ irreducible in $\mathbb{Z}[Y]$ so $f(X)$ irreducible in $\mathbb{Z}[X]$ (if $f(X) = g(X)h(X)$ then $f(Y+1) = g(Y+1)h(y+1)$)

12 Algebraic Integers

Recall $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{C}\} \leq \mathbb{C}$ - ring of Gaussian integers.
Norm $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0},\ a + bi \mapsto a^2 + b^2$ iwth $N(z_1 z_2) = N(z_1)N(z_2)$ is a Euclidean function Thus $\mathbb{Z}[i]$ is a ED, hence a PID and UFG and so primes = irreducibles in $\mathbb{Z}[i]$
The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ (only elements of Norm 1)

Example. (i) $2 = (1_i)(1 - i)$ and $5 = (2 + i)(2 - i)$ are not primes in $\mathbb{Z}[i]$
(ii) $N(3) = 0$ so if $3 = ab$ in $\mathbb{Z}[i]$, $N(a)N(b) = 9$. But $\mathbb{Z}[i]$ has no elements of norm r. thus either a or b is a unit $\implies$ 3 is prime in $\mathbb{Z}[i]$. Similarly 7 is prime in $\mathbb{Z}[i]$

Prop 12.1. Let $p \in \mathbb{Z}$ be a prime number. 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 $p = 1 \bmod 4$

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 $x = a + bi$ gives $p = N(x) = a^2 + b^2$
(ii) $\implies$ (iii): the squares mod 4 are 0 and 1. Thus if $p = a^2 + b^2$, then $p \not\equiv 3 \bmod 4$
(iii) $\implies$ (i): Already saw 2 is not prime in $\mathbb{Z}[i]$. By theorem 9.3, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$. so if $p = 1 \bmod 4$, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$. So if $p = 1 \bmod 4$, then $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4, i.e. $\exists x \in \mathbb{Z}$ with $x^4 \equiv 1 \bmod p$, but $x^2 \not\equiv 1 \bmod p$. Then $x^2 \equiv -1 \bmod p$. Now $p \mid x^2 + 1 = (x + i)(x - i)$ but $p \nmid x + i$ and $p \nmid x - i$, thus p not prime in $\mathbb{Z}[i]$

Theorem 12.2. The primes in $\mathbb{Z}[i]$ are (up to associates)
(i) $a + bi$, where $a, b \in \mathbb{Z}$ and $a^2 + b^2 = p$ is a prime number with $p \equiv 2$ or $p \equiv 1 \bmod 4$.
(ii) Prime numbers $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$

Proof. First we check these are primes:
(i) $N(a + bi) = p$. If $a + bi = uv$, then either $N(u) = 1$ or $N(v) = 1$. Thus $a + bi$ is irreducible, hence prime
(ii) Prop 12.1

Now let $z \in \mathbb{Z}[i]$ be a prime (irreducible). Then $\bar{z} \in \mathbb{Z}[i]$ is also irreducible and $N(z) = z\bar{z}$ is a factorization into irreducibles.
Let $p \in \mathbb{Z}$ be a prime number dividing $N(z)$. If $p \equiv 3 \bmod 4$, then p is prime in $\mathbb{Z}[i]$. Thus $p \mid z$ or $\overline{z}$, so p is an associate of z or $\overline{z}$

$$\implies p \text{ is an associate of } z$$

Otherwise, $p \equiv 2$ or $p \equiv 1 \bmod 4$ and

$$p = a^2 + b^2 = (a + bi)(a - bi) \text{ some } a, b \in \mathbb{Z}$$

Then $(a+bi)(a-bi) \mid z\overline{z}$. Thus z is an associate of $a+bi$ or $a-bi$ by uniqueness of factorization

Remark. In theorem 12.2 (i), 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 iff every prime factor p of n with $p \equiv 3 \mod 4$ divides n to an even power

Proof. $n = a^2 + b^2 \iff n = N(x)$ some $x \in \mathbb{Z}[i] \iff n$ is a product of norms of primes in $\mathbb{Z}[i]$.
Theorem 12.2 implies that the norms of primes in $\mathbb{Z}[i]$ are the primes $p \in \mathbb{Z}$ with $p \not\equiv 3 \mod 4$, and squares of primes $p \in \mathbb{Z}$ with $p \equiv 3 \mod 4$

Example. $65 = 5 \cdot 13$
Factoring into primes in $\mathbb{Z}[i]$ gives $5 = (2 + i)(2 - i)$, $13 = (2 + 3i)(2 - 3i)$.
Thus $65 = (2 + 3i)(2 + i)(2 + 3i)(2 + i)$ i.e.

$$65 = N((2 + 3i)(2 + i)) = N(1 + 8i) \implies 65 = 1^2 + 8^2$$

But also

$$65 = N((2 + i)(2 - 3i)) = N(7 - 4i) \implies 65 = 7^2 + 4^2$$

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

$$R[\alpha] = \mathrm{Im}(\underset{R[X] \to S}{g(X) \mapsto g(\alpha)})$$

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

Definition. f above is the **minimal polynomial** of α. By isomorphism theorem

$$\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha] \leq \mathbb{C}$$

Thus $\mathbb{Q}[\alpha]$ is an integral domain $\implies f$ irreducible in $\mathbb{Q}[X] \implies \mathbb{Q}[\alpha]$ is a field

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

Proof. Let $\lambda \in \mathbb{Q}^\times$ s.t. $\lambda f \in \mathbb{Z}[X]$ 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 $\mathbb{Q}[X]$. Lemma 11.4 $\implies$ $\lambda f \mid g$ in $\mathbb{Z}[X]$. Thus $\ker(\theta) = (\lambda f)$.
Now α is an algebraic integer, hence $\exists g \in \ker(\theta)$ monic. Then $\lambda f \mid g$ in $\mathbb{Z}[X]$ $\implies$ $\lambda = \pm 1$. Hence $f \in \mathbb{Z}[X]$, and $(f) = \ker(\theta)$.

Let $\alpha \in \mathbb{C}$ an algebraic integer. applying isomorphism theorem θ gives

$$\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha]$$

Example. $i, \sqrt{2}, \frac{-1+\sqrt{3}}{2}, \sqrt[n]{p}$ have minimal polynomials

$$X^2+1, X^2-2, X^2+X+1, X^n-p$$

Thus

$$\frac{\mathbb{Z}[X]}{(X^2+1)} \cong \mathbb{Z}[i], \quad \frac{\mathbb{Z}[X]}{(X^2-2)} \cong \mathbb{Z}[\sqrt{2}] \text{ etc.}$$

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 prop 12.4 $\implies$ min poly has coefficients in $\mathbb{Z}$.
$\alpha \in \mathbb{Q}$ $\implies$ min poly is $X - \alpha$ and so $\alpha \in \mathbb{Z}$

13 Noetherian Rings

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

Lemma 13.1. Let R be a ring. R satisfies ACC $\iff$ All ideals in R are finitely generated

Proof. "$\Longleftarrow$": let $I_1 \subseteq I_2 \subseteq \dots$ be a chain of ideals and $I = \bigcup_{n\geq 1} I_n$, which is again an ideal.
By assumption, $I = (a_1, \dots, a_m)$ for some $a_1, \dots, a_n \in R$. These elements belong to a neted union so $\exists N \in \mathbb{N}$ s.t. $a_1, \dots, a_m \in I_N$. Then for $n \geq N$

$$(a_1, \dots, a_m) \subseteq I_N \subseteq I_n \subseteq I = (a_1, \dots, a_m)$$

so $I_n = I_N = I$.
"$\implies$": Assume $J \trianglelefteq R$ not finitely generated. choose $a_1 \in J$. Then $J \neq (a_1)$, so we can choose $a_2 \in J \backslash (a_1)$.
Then $J \neq (a_1, a_2)$, so we can choose $(a_3) \in J \backslash (a_1, a_2)$. Continuing this process, we obtain a chain of ideals

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

with dtrict inclusions ※ to ACC

Definition. A ring satisfying ACC is called **Noetherian**

13.1 Hilbert's Basis Theorem

Theorem 13.2 (Hilbert's Basis Theorem)**.** If R is a Noetherian ring, then $R[X]$ is Noetherian

Proof. Assume $J \trianglelefteq R[X]$ is not finitely generated. Choose $f_1 \in J$ of minimal degree. Then $(f_1) \neq J$. Choose $f_2 \in J \backslash (f_1)$ of minimal degree. Then $(f_1, f_2) \neq J$ and so on.
Obtain a sequence $f_1, f_2, f_3, \dots \in R[X]$ with $\deg f_i \leq \deg f_{i+1}$.
Set $a_i :=$ leading coefficient of f_i. We obtain

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \dots$$

a chain of ideals in R. Since R is Noetherian, $\exists m \in \mathbb{N}$ s.t. $a_{m+1} \in (a_1, \dots, a_m)$.
Let $a_{m+1} = \sum_{i=1}^m \lambda_i a_i$, and set

$$g = \sum_{i=1}^m \lambda_i X^{\deg f_{m+1} - \deg f_i} f_i$$

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 $\deg(f_{m+1} - g) < \deg f_{m+1} \implies f_{m+1} - g \in (f_1, \dots, f_m)$ by minimality of $\deg f_{m+1} \implies f_{m+1} \in (f_1, \dots, f_m)$ ※.
Thus J finitely generated $\implies R[X]$ Noetherian by Lemma 13.1

Corollary 13.3.
- $\mathbb{Z}[X_1, \dots, X_n]$ Noetherian
- $F[X_1, \dots, X_n]$ Noetherian for F a field

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

$$\{(a_1, \dots, a_n) \in \mathbb{C}^n : f(a_1, \dots, a_n) = 0, \ \forall f \in F\}$$

where $F \subseteq R$ is a possibly infinite set of polynomials.
Let $I = \{\sum_{i=1}^m \lambda_i f_i : m \in \mathbb{N}, \lambda_i \in R, f_i \in F\}$. Then $I \trianglelefteq R$. R Noetherian $\implies$

$$I = (g_1, \dots, g_r), \ g_i \in I$$

Thus

$$V = \{(a_1, \dots, a_n) \in \mathbb{C}^n : g_i(a_1, \dots, a_n) = 0, i = 1, \dots, r\}$$

Lemma 13.4. Let R be a Noetherian ring and $I \trianglelefteq R$. Then R/I is Noetherian

Proof. Let $J'_1 \subseteq J'_2 \subseteq \dots$ a chain of ideals in R/I. By ideal correspondence we have $J'_i = J_i/I$ fir sine $J_1 \subseteq J_2 \subseteq \dots$ a chain of ideals in R (containing I)
R Noetherian $\implies \exists N \in \mathbb{N}$ s.t. $J_n = J_{n+1}$ $\forall n \geq N \implies \exists N \in \mathbb{N}$ s.t. $J'_n = J'_{n+1}$ $\forall n \geq N$.
Thus R/I is Noetherian

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

Examples (of non-Noetherian rings).
(i) $R = \mathbb{Z}[X_1, X_2, \dots] = \bigcup_{n \geq 1} \mathbb{Z}[X_1, \dots, X_n]$ i.e. polynomials in countably many variables

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \dots$$

an infinite ascending chain
(ii) $R = \{f \in \mathbb{Q}[X] : f(0) \in \mathbb{Z}\} \leq \mathbb{Q}[X]$

$$(X) \subsetneq (\frac{1}{2}X) \subsetneq (\frac{1}{4}X) \subsetneq (\frac{1}{8}X) \subsetneq \dots$$

Since $2 \in R$ is not a unit

14 Modules - Definitions and Examples

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

$$+ : M \times M \to M \quad \cdot : R \times M \to M$$

such that

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

(ii) The operation $\cdot$ satisfies

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

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

$$\cdot : \mathbb{Z} \times A \to A$$

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

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

$$\cdot : F[X] \times V \to V$$

$$(f, v) \mapsto (f(\alpha))(v)$$

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

Example. General constructions

(i) For any ring R, R^n is an R-module via

$$r \cdot (r_1, \dots, r_n) = (rr_1, \dots, rr_n)$$

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 an S-module M may be regarded as an R module via $R \times M \to M$, $(r, m) \mapsto \phi(r)m$. In particular, if $R \leq S$ then any S-module may be viewed as an R-module

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

Example. (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

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

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

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

Example. If $R = F$ is a field, an F-module homomorphism is just a linear map

Theorem 14.1 (First isomorphism theorem)**.** Let $f : M \to N$ be an R-module homomorphism. Then

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

and

$$M/\ker(f) \cong \text{Im }(f)$$

Proof. Similar to before

Theorem 14.2 (Second isomorphism theorem)**.** Let $A, B \leq M$ be R-submodules. Then

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

$$A \cap B \leq M$$

and

$$\frac{A}{A \cap B} \cong \frac{A+B}{B}$$

Proof. Apply first isomorphism theorem to the composite $A \to M \to M/B$, $m \mapsto m + B$

For third isomorphism theorem, note $\exists$ bijection $\{$submodules of $M/N\} \leftrightarrow \{$submodules of M containing $N\}$

Theorem 14.3 (Third isomorphism theorem)**.** If $N \leq L \leq M$ are R-submodules, then

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

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

Notation. Let M be an R-module. If $m \in M$, write

$$Rm = \{rm \in M : r \in R\}$$

the submodule generated by m.
If $A, B \leq M$ then $A + B = \{a + b : a \in A, b \in B\} \leq M$

Definition. M is **finitely generated** if $\exists m_1, \dots, m_n \in M$ such that $M = Rm_1 + Rm_2 + \cdots + Rm_n$

Lemma 14.4. *M finitely generated $\iff$ $\exists$ a surjective R-module homomorphism $f : R^n \to M$ for some $n \in \mathbb{N}$*

Proof. " $\implies$ ": If $M = Rm_1 + \cdots + Rm_n$, define $f : R^n \to M$, $(r_1, \dots, r_n) \mapsto \sum r_i m_i$ a surjective R-module homomorphism.
" $\impliedby$ ":Let $e_i = (0, \dots, 0, 1, 0, \dots, 0) \in R^n$. Given $f : R^n \to M$ surjective, set $m_i : f(e_i)$. Then any $m \in M$ is of the form

$$f(r_1, \dots, r_m) = f(\sum r_i e_i) = \sum r_i f(e_i) = \sum r_i m_i$$

Thus $M = Rm_1 + \cdots + Rm_n$

Corollary 14.5. 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 $R^n \to M \to M/N$, $m \mapsto m + N$ is a surjective R-module homomorphism

Example. A submodule of a finitely generated module need not be finitelygenerated.
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 finitely generated module over a Noetherian ring is finitely generated

Definition. Let M be an R-module

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

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

(iii) M is **torsion-free** if $0 \neq m \in M$ is not tortion

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

15 Direct Sums and Free Modules

Definition. Let $M_1, \dots M_n$ be R-modules. The **direct sum** $M_1 \oplus \cdots \oplus M_n$ is the set $M_1 \times \cdots \times M_n$ with operations

$$(m_1, \dots, m_n) + (m'_1, \dots, m'_n) = (m_1 + m'_1, \dots, m_n + m'_n)$$

$$r \cdot (m_1, \dots, m_n) = (rm_1, \dots, rm_n)$$

$M_1 \oplus \cdots \oplus M_n$ is R-module

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

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

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

Proof. Apply 1st iso. theorem to the surjective R-module homomorphism

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

$$(m_1, \dots, m_n) \mapsto (m_1 + N_1, \dots, m_n + N_n)$$

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

Definition. Let $m_1, \dots, m_n \in M$. The set $\{m_1, \dots, m_n\}$ is **independent** if $\sum_{i=1}^n r_i m_i = 0 \implies r_1 = r_2 = \cdots = r_n = 0$

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

(i) S generates M, i.e. $\forall m \in M,\ m = \sum r_i s_i,\ r_i \in R,\ s_i \in S$

(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 $S \subseteq M$ is called **free** and S is called a **free basis**

Prop 15.2. For a subset $S = \{m_1, \dots, m_n\} \subseteq M$, the following are equivalent:
(i) S generates M freely
(ii) S generates M and S is independent
(iii) Every element can be written uniquely as $r_1 m_1 + \cdots + r_n m_n$ for some $r_1, \dots, r_n \in R$
(iv) The R-module homomorphism $R^n \to M$, $(r_1, \dots, r_n) \mapsto \sum r_i m_i$ is an isomorphism

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

$$m_i \mapsto \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

This extends to R-module homomorphism $\Theta : M \to R$. We then have

$$0 = \Theta(0) = \Theta(\sum r_i m_i) = \sum r_i \Theta(m_i) = r_j \text{ ※}$$

Thus S is indepnedent.
(ii) $\implies$ (iii) $\implies$ (i) and (iii) $\iff$ (iv) are exercises

Example. A non-trivial finite abelian group 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 $\{2\}, \{3\}$ do not generate

Prop 15.3 (Invariance of dimension)**.** R 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 $IM = \{\sum a_i m_i : a_i \in I,\ m_i \in M\} \leq M$. The quotient M/IM is an R/I-module via

$$(R + I) \cdot (m + IM) = rm + IM$$

(well-defined: if $b \in I$, $b \cdot (m + IM) = bm + IM = 0 + IM$)
Suppose $R^m \cong R^n$. Choose $I \trianglelefteq R$ a maximal ideal (Use Zorn's Lemma + ES2 Q4). By the above, get an isomorphism of R/I-modules

$$\left(\frac{R}{I}\right)^m \cong \frac{R^m}{IR^m} \cong \frac{R^n}{IR^n} \cong \left(\frac{R}{I}\right)^n$$

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

16 The Structure Theorem and applications

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

Definition. The **elementary row operations** are

- (ER1) Add λ times jth row to ith row ($\lambda \in R,\ i \neq j$)
- (ER2) Swap ith and jth rows
- (ER3) Multiply ith row by $u \in R^X$

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

- (ER1)
$$\begin{bmatrix} 1 & & & \\ & \ddots & \lambda & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$
- (ER2)
$$\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & & 1 & \\ & & \ddots & & & \\ & & 1 & & 0 & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}$$
- (ER3)
$$\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & u & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

  In particular, these operations are reversible

Note. Similarly, we can define elementary column operations (EC1 to EC3), realised by right multiplication by $n \times n$ invertible matrix

Definition. Two $m \times n$ matrices A and B are **equivalent** if $\exists$ sequence of elementary row and column operations taking A to B. If they are equivalent, then $\exists P, Q$ s.t. $B = QAP$

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

$$\begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_t & & \\ & & & 0 & \\ & & & & \ddots \end{bmatrix}$$

The d_i are called invariant factors - will show they are unique up to associates

Proof. If $A = 0$, 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

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

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

Steps (i) and (ii) decrease $\phi(a_{11})$, so can repeat finitely many times until $a_{11} | a_{1j}$ $\forall j \geq 2$, $a_{11} \mid a_{i1}$ $\forall i \geq 2$.

Subtracting multiples of the first row/ column from the others gives

$$A = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & A^1 & & \\ 0 & & & \end{bmatrix}$$

where A^1 is an $(m-1) \times (n-1)$ matrix.

(iii) If $a_{11} \nmid a_{ij}$ for some $i, j \geq 2$, then add ith row to first row and perform column operations as before to decrease $\phi(a_{11})$. Then restart algorithm.

After finitely many steps obtain:

$$A = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & A^1 & & \\ 0 & & & \end{bmatrix}$$

with $a_{11} = d_1$ say s.t. $d_1 \mid a_{ij}$ $\forall i, j$.

Applying same method to A^1 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 (i.e. a matrix formed by deleting $n - k$ rows and $n - k$ columns)

Definition. The kth fitting ideal $\text{Fit}_k(A) \trianglelefteq R$ is the ideal generated by the $k \times k$ minors of A

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

Proof. We show that (ER1 - ER3) don't change $\text{Fit}_k(A)$ (same proof works for EC1 - EC3)
(ER1) add λ times jth row to ith row, so A becomes A'

$$A' = \begin{bmatrix} a_{i1} + \lambda a_{j1} \dots a_{in} + \lambda a_{jn} & & \\ & & \\ a_{j1} & \dots & a_{jn} \\ & & \end{bmatrix}$$

Let C be a $k \times k$ submatrix of A and C' the corresponding submatrix of A':

- If we did not choose ith row, then $C = C'$

$$\implies \det C = \det C'$$

- If we choose both of the rows i and j, then C and C' differ by a row operation

$$\implies \det C = \det C'$$

- If we chose ith row but not the jth row, then by expanding along the ith row

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

where D is another $k \times k$ submatrix of A (in D we choose jth row instead of ith row).

Thus $\det(C') \in \text{Fit}_k(A)$ Hence $\text{Fit}_k(A') \subseteq \text{Fit}_k(A)$.
Since (ER1) is reversible, we get "$\supseteq$" and hence equality.
(ER2) and (ER3) are similar but easier.

Now if A has SNF

$$\begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_t & & \\ & & & 0 & \\ & & & & \ddots \end{bmatrix}$$

$d_1 \mid d_2 \mid \cdots \mid d_t$. Then $\text{Fit}_k(A) = (d_1 d_2 \dots d_k) \trianglelefteq R$. Thus the products $d_1 \dots d_k$ (up to associates) depend only on A.
Cancelling out, shows that each d_i (up to assiciate) depends only on A.

Example. Consider the matrix $A = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$ over $\mathbb{Z}$.

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

But also $(d_1) = (2, -1, 1, 2) = (1) \implies d_1 = \pm 1$

$$(d_1 d_2) = (\det A) = (5) \implies d_1 = \pm 5$$

Moral. 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

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

$$I = \{r \in R : \exists r_2, \ldots, r_m \in R \text{ s.t. } (r, r_2, \ldots, r_m) \in N\} \trianglelefteq R$$

Since ED $\implies$ PID, we have $I = (a)$, some $a \in R$. Choose some $n = (a, a_2, \ldots, a_m) \in N$. For $(r_1, \ldots, r_m) \in N$, we have $r_1 = ra$ for some r, so $(r_1, r_2, \ldots, r_m) - rn = (0, r_2 - ra_2, \ldots, r_m - ra_m)$ which lies in $N' := N \cap \{0\} \times R^{m-1} \leq R^{m-1}$ hence $N = Rn + N'$.
By induction, N' is generated by $n_2, \ldots, n_m$ hence $\{n, n_2, \ldots, n_m\}$ generates N

Theorem 16.4. Let R be a ED and $N \leq R^m$. There is a free basis $x_1, \ldots, x_m$ for R^m s.t. N is generated by $d_1x_1, \ldots, d_tx_t$ for some $r \leq m$ and $d_1, d_2, \ldots, d_t \in R$ with $d_1 \mid d_2 \mid d_t$.

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

$$A = \begin{bmatrix} y_1 & y_2 & \ldots & y_n \end{bmatrix}$$

By theorem 16.1, A is equivalent to

$$A' = \begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_t & & \\ & & & 0 & \\ & & & & \ddots \end{bmatrix}$$

with $d_1 \mid d_2 \mid \cdots \mid d_t$.
A' obtained from A by elementary row and column operations. Each row operation changes our choice of free basis for R^m. Each column operation changes our set of generators for N. Thus after changing free basis of R^m to $x_1, \ldots, x_m$, say, the submodule N is generated by $d_1x_1, \ldots d_tx_t$ as claimed

16.1 Structure Theorem

Theorem 16.5 (Structure Theorem)**.** Let R be a ED and M a finitely generated R-module. Then

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

for some $0 \neq d_i \in R$ with $d_1 \mid d_2 \mid \cdots \mid d_t$ and $k \geq 0$. The d_i are called invariant factors

Proof. Since M is finitely generated, $\exists$ 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, $\exists$ free basis $x_1, \ldots, x_m$ for R^m s.t. $\ker(\phi)$is generated by $d_1x_1, d_2x_2, \ldots, d_tx_t$ with $d_1 \mid d_2 \mid \cdots \mid d_t$. Then

$$\begin{aligned} M &\cong \frac{R \oplus R \oplus \cdots \oplus R \oplus R \oplus \cdots \oplus R}{d_1R_2 \oplus d_2R \oplus \cdots \oplus R_tR \oplus 0 \oplus \cdots \oplus 0} \\ &\cong \frac{R}{(d_1)} \oplus \frac{R}{(d_2)} \oplus \cdots \oplus \frac{R}{(d_t)} \oplus \underbrace{R \oplus \cdots \oplus R}_{m-t \text{ copies}} \end{aligned}$$

by Lemma 15.1

Remark. After deleting those d_i which are units, the module M uniquely determined (up to associated) - proof omitted

Corollary 16.6. Let R be a ED. Then any finitely generated torsion-free 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

$$2a + b = 0 \qquad -a + 2b = 0$$

Then $G \cong \mathbb{Z}^2/N$, where N is generated by $\begin{bmatrix} 2 & 1 \end{bmatrix}$, $\begin{bmatrix} -1 & 2 \end{bmatrix}$.
$A = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$ has SNF $\begin{bmatrix} 1 & 0 \\ 0 & 5 \end{bmatrix}$. Thus can change basis for $\mathbb{Z}^2$ s.t. N is generated by $(1, 0)$ and $(0, 5)$. Thus

$$G \cong \frac{\mathbb{Z} \oplus \mathbb{Z}}{\mathbb{Z} \oplus 5\mathbb{Z}} \cong \frac{\mathbb{Z}}{5\mathbb{Z}}$$

More generally

Theorem 16.7 (Structure Theorem for Finitely Generated Abelian Groups)**.** Any finitely generated abelian groups G is isomorphic to $\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z} \oplus \mathbb{Z}^r$ 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 finite ($r = 0$) 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 a prime number. To generalise this we need

Lemma 16.8. Let R be a PID and $a, b \in R$ with $\gcd(a, b) = 1$. Then

$$\frac{R}{(ab)} \cong \frac{R}{(a)} \oplus \frac{R}{(b)} \text{ as } R\text{-modules}$$

(case $R = \mathbb{Z}$ was Lemma 6.2)

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

$$\psi : R \to \frac{R}{(a)} \oplus \frac{R}{(b)}$$

$$x \mapsto (x + (a), x + (b))$$

Then $\psi(sb) = (1+(a), 0+(b))$, $\psi(ra) = (0+(a), 1+(b))$, thus $\psi(sbx+ray) = (x+(a), y+(b))$ for any $x, y \in R$ hence ψ is surjective.
Clearly $(ab) \subset \ker(\psi)$. Converselt if $x \in \ker(\psi), x \in (a) \cap (b)$ and $x = x(ra + sb) = r(ax) + s(xb) \in (ab)$. Then $\ker(\psi) = (Ab)$. First isomorphism theorem $\implies$

$$\frac{R}{(ab)} \cong \frac{R}{(a)} \oplus \frac{R}{(b)}$$

as modules

Theorem 16.9 (Primary decomposition theorem)**.** Let R be a ED and M a finitely generated R-module. Then

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

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

Proof. By the structure theorem

$$M \cong \frac{R}{(d_1)} \oplus \frac{R}{(d_2)} \oplus \cdots \oplus \frac{R}{(d_t)} \oplus R^m$$

So it suffices to consider $M \cong \frac{R}{(d_i)}$. $d_i = up_1^{\alpha_1} \dots p_r^{\alpha_r}$ where u is a unit and $p_1, \dots, p_r$ are distinct (non-associate) primes.
Lemma 16.6 $\implies$

$$M \cong \frac{R}{(p_1^{\alpha_1})} \oplus \cdots \oplus \frac{R}{p_r^{\alpha_r}}$$

Notation. 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, $(f(X), v) \mapsto f(\alpha)(v)$

Lemma 16.10. If V finite dimensional, then V_α is a finitely generated $F[X]$-module

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

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

$$\begin{bmatrix} 0 & & & & 0 \\ 1 & 0 & & & \vdots \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & & 1 & 0 \end{bmatrix} \tag{*}$$

since α acts as "multiplication by X"

(ii) Suppose $V_\alpha \cong \frac{F[X]}{((X-\lambda)^n)}$ as $F[X]$-modules. Then w.r.t. basis $1, X-\lambda, (X-\lambda)^2, \dots, (X-\lambda)^{n-1}$, $\alpha - \lambda \,\mathrm{Id}$ has matrix $(*)$, thus α has matrix

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

(iii) Suppose $V_\alpha \cong \frac{F[X]}{(f)}$ where

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

Then w.r.t. basis $1, X, \dots, X^{n-1}$, α has matrix

$$\begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & \vdots \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & \ddots & -a_{n-2} \\ 0 & 0 & & 1 & -a_{n-1} \end{bmatrix}$$

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

Theorem 16.11 (Rational canonical form)**.** Let $\alpha : V \to V$ be an endomorphism of a finite dimensional vector space, where F is any field. The $F[X]$-module V_α decomposes as

$$V_\alpha \cong \frac{F[X]}{(f_1)} \oplus \cdots \oplus \frac{F[X]}{(f_t)}$$

where $f_i \in F[X]$ monic and $f_1 \mid f_2 \mid \cdots \mid f_t$. Moreover, w.r.t. a suitable basis or V (as an F-vector space) α has matrix

$$\begin{bmatrix} C(f_1) & & \\ & \ddots & \\ & & C(f_t) \end{bmatrix} \qquad (**)$$

Proof. By Lemma 16.7, V_α is finitely generated as an $F[X]$-module. Since $F[X]$ is a ED, the structure theorem implies

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

where $f_1 \mid f_2 \mid \cdots \mid f_t$.
Since V is finite dimensional, $m = 0$. Upon multiplying each f_i by a unit, we may assume f_i are monic

Remarks.

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

(ii) The min. poly. of α is f_t. The char. poly. of α is $\prod_{i=1}^t f_i$ ($\implies$ Cayley-Hamilton theorem)

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

$$V_\alpha \cong \frac{F[X]}{(X-\lambda)} \oplus \frac{F[X]}{(X-\lambda)} \text{ or } \frac{F[X]}{(f)}$$

where f is char. poly of α

Corollary 16.12. Let $A, B \in GL_2(F)$ non-scalar matrices. Then A and B are similar $\iff$ they have the same char. poly.

Example. " $\implies$ ": Linear Algebra
" $\impliedby$ ": By the last example, A and B are both similar $C(f)$, where f is the char. poly. of A and B

Definition. The annihilator of an R-module M is

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

Examples. (i) $I \trianglelefteq R$, then $\text{Ann}_R(R/I) = I$
(ii) If A is a finite abelian group, then $\text{Ann}_{\mathbb{Z}}(A) = (e)$, where e is the exponent of A
(iii) If V_α as above, $\text{Ann}_{F[X]}(V_\alpha) = (\text{min.poly. of } \alpha)$

Lemma 16.13. The primes in $\mathbb{C}[X]$ are the polynomials $X - \lambda$, for $\lambda \in \mathbb{C}$

Proof. By the fundamental theorem of algebra, any non-constant polynoial in $\mathbb{C}[X]$ has a root in $\mathbb{C}$, so a factor $X - \lambda$. Hence the irreducibles have degree 1

Theorem 16.14 (Jordan Normal Form)**.** Let $\alpha : V \to V$ be an endomorphism of a finite dimensional $\mathbb{C}$-vector space. Let V_α be V as regarded as a $\mathbb{C}[X]$-module with X acting as α. There is an isomorphism of $\mathbb{C}[X]$-modules

$$V_\alpha \cong \frac{\mathbb{C}[X]}{((X-\lambda_1)^{n_1})} \oplus \cdots \oplus \frac{\mathbb{C}[X]}{((X-\lambda_t)^{n_t})}$$

where $\lambda_1, \ldots, \lambda_t \in \mathbb{C}$ (not nec. distinct) . In particular, $\exists$ basis for V s.t. α has matrix

$$\begin{bmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_t}(\lambda_t)) \end{bmatrix}$$

where

$$J_n(\lambda) = \begin{bmatrix} \lambda & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{bmatrix}$$

$n \times n$ matrix.

Proof. $\mathbb{C}[X]$ is a ED, and V_α is finitely generated as a $\mathbb{C}[X]$-module by Lemma 16.7. we apply the primary decomposition theorem 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 multiplication by X on $\frac{\mathbb{C}[X]}{((X-\lambda)^n)}$ w.r.t $1, (X-\lambda), (X-\lambda)^2, \ldots, (X-\lambda)^{n-1}$.

Remarks.
(i) If α is represented by matrix A, then theorem says 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 eigenspaces $\ker((\alpha - \lambda \text{ id})^m)$ $m = 1, 2, 3, \ldots$ (omit details)
(iii) The min. poly. of α is $\prod_\lambda (X-\lambda)^{c_\lambda}$ where c_λ is the size of the largest λ-block
(iv) The char. poly. of α is $\prod_\lambda (X-\lambda)^{a_\lambda}$ where a_λ is the sum of the sizes of the λ-blocks
(v) The number of λ-blocks is the dimension of the λ-eigenspace

17 Modules over PID's

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 ED, this was Corollary 16.5)

Proof. Let $M = Rx_1 + \cdots + Rx_n$ with n as small as possible. If $x_1, \ldots, x_n$ aer independent then M is free and we are done. Otherwise, $\exists r_1, \ldots, r_n \in R$ s.r. $\sum_{i=1}^n r_i x_i = 0$.
Wlog. $r_1 \neq 0$. Lemma 17.2 (ii) shows that after replacing x_1 and x_2 with suitable x_1' and x_2', we may assume that $r_1 \neq 0$ 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

$$r_1 \neq 0, \; r_2 = r_3 = \cdots = r_n = 0$$

Thus $M = Rx_2 + \cdots + Rx_n$ ※ choice of n

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) $\exists A \in SL_2(R)$ s.t.

$$A \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$$

(ii) If $x_1, x_2 \in M$, then $\exists x_1', x_2' \in M$ s.t. $Rx_1 + Rx_2 = Rx_1' + Rx_2'$ and

$$r_1 x_1 + r_2 x_2 = d x_1' + 0 \cdot x_2'$$

Proof. R a PID $\implies (r_1, r_2) = (d) \implies \exists \alpha, \beta \in R$ s.t. $\alpha r_1 + \beta r_2 = d$. Write $r_1 = s_1 d$ and $r_2 = s_2 d$, some $s_1, s_2 \in R$. Then $\alpha s_1 + \beta s_2 = 1$

(i)

$$\begin{bmatrix} \alpha & \beta \\ -s_2 & s_1 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$$

note $\det = \alpha s_1 + \beta s_2 = 1$

(ii) Let

$$x_1' = s_1 x_2 + s_2 x_2$$

$$x_2' = -\beta x_1 + \alpha x_2$$

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

$$\det \begin{bmatrix} s_1 & s_2 \\ -\beta & \alpha \end{bmatrix} = \alpha s_1 + \beta s_2 = 1$$

Finally, $r_1 x_1 + r_2 x_2 = d(s_1 x_1 + s_2 x_2) = d x_1' + 0 \cdot x_2'$