GRM

Groups Continuing from IA Groups, paying attention to simple groups, p-groups & p-subgroups. Main highlight will be Sylow theorems.

Rings Sets with addition, subtraction and multiplication like $\mathbb{Z}$ or $\mathbb{C}[X]$. Important examples include "rings of integers" ($\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$) studied further in Part II Number Fields, & polynomials which are basic to Part II Algebraic Geometry.

A ring where division is always possible is called a field, e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for p prime.

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

§1 Groups – revision & basics

Def^n: A group is a pair $(G,\cdot)$ consisting of a set G and a binary operation $\cdot : G\times G \to G$ satisfying associativity, identity, and inverses.

Remarks (i) In checking $\cdot$ is well-defined need to check closure
(ii) If using additive (or multiplicative) notation then we often write 0 (or 1) for the identity.

Def^n A subset $H \subseteq G$ is a subgroup (written $H \leq G$) if it is a group with $\cdot$ 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 = cyclic of order n
D_{2n} = symmetries of regular n-gon

L1.2 (iii) Symmetric & alternating groups

S_n = all permutations of $\{1, \dots, n\}$ i.e. bijections of this set to itself

$A_n \leq S_n$ subgroup of even ~~transpositions~~ permuta

Recall: Every $\sigma \in S_n$ can be written as a product of transpositions. As seen in IA Groups, the parity of the number of transpositions depends only on σ – we say σ is even or odd accordingly

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

$i^2 = j^2 = k^2 = ijk = -1, \dots$

(v) Matrix groups over F a field

general linear $GL_n(F)$ = $n \times n$ matrices over F with $\det \neq 0$

special linear $SL_n(F) \leq GL_n(F)$ subgroup of matrices with determinant 1

Def^n The (direct) product of groups G & H is $G \times H$ with operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$

For a subgroup $H \leq G$ the left cosets of H in G are the sets $gH = \{gh : h \in H\}$. These partition G, and each has the same cardinality as H.

We deduce

Lagrange's Theorem Let G be a finite group & H a subgroup. Then $|G| = |H||G:H|$ where $|G:H|$ is the number of left cosets of H in G, and is called the index of H in G.

Partial Converse $|G| = p^a m$, p prime, $p \nmid m$

Then $\exists$ subgroup $H \leq G$ with $|H| = p^a$ (proof later)

Def^n: 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.

Remarks Let $g \in G$ have order d

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

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

L1.3 **Def^n:** a subgroup $H \leq G$ is *normal* if $g^{-1}Hg = H \ \forall g \in G$ which we write $H \triangleleft G$.

Proposition 1.1 If $H \triangleleft G$ then the set G/H of left cosets of H in G is a group (called the *quotient group*) with operation $g_1H \cdot g_2H = g_1g_2H$.

Proof: we must check $\cdot$ is well-defined. Suppose $g_1H = g_1'H$ and $g_2H = g_2'H$. Then $g_1' = g_1h_1$, $g_2' = g_2h_2$ for some $h_1, h_2 \in H$.

$g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1g_2H$

This is equal to g_1g_2H iff $g_2^{-1}h_1g_2 \in H$ which is true since $H \triangleleft G$.

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

Def^n: If G, H groups, a function $\phi : G \to H$ is a *group homomorphism* if $\phi(g_1g_2) = \phi(g_1)\phi(g_2) \ \forall g_1, g_2 \in G$.

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

It is easy to check $\ker(\phi) \leq G$ & $\mathrm{Im}(\phi) \leq H$. If $a \in \ker(\phi)$ and $g \in G$, $\phi(g^{-1}ag) = \phi(g^{-1})\phi(a)\phi(g) = 1$, and hence $\ker(\phi) \triangleleft G$.

Def²: An isomorphism of groups is a group homomorphism that is also a bijection. Groups G and H are isomorphic (written $G \cong H$) if $\exists$ isomorphism $\phi: G \to H$.

(Ex: check ϕ^{-1} is a group isomorphism)

Isomorphism Theorem

Let $\phi: G \to H$ be a group homomorphism.

Then $\ker(\phi) \triangleleft G$ and $G/\ker(\phi) \cong \operatorname{Im}(\phi)$.

Proof: Let $K = \ker(\phi)$. We checked already $K \triangleleft G$.

Define $\Phi: G/\ker(\phi) \longrightarrow \operatorname{Im}(\phi)$

$$gK \longrightarrow \phi(g).$$

Φ is well defined & injective

$$g_1K = g_2K \iff g_2^{-1}g_1 \in K$$
$$\iff \phi(g_2^{-1}g_1) = e$$
$$\iff \phi(g_2)^{-1}\phi(g_1) = e$$
$$\iff \phi(g_1) = \phi(g_2)$$

Φ is a group homomorphism

$$\Phi(g_1K \cdot g_2K) = \Phi(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2)$$
$$= \Phi(g_1K)\,\Phi(g_2K)$$

Φ is surjective Let $x \in \operatorname{Im}(\phi)$

$\Rightarrow x = \phi(g)$ for some $g \in G$

$\Rightarrow x = \Phi(gK) \in \operatorname{Im}(\Phi)$. □

Example Let $\phi: \mathbb{C} \to \mathbb{C}^* = \{x \in \mathbb{C} : x \neq 0\}$

$$z \longrightarrow e^z$$

As $e^{z+w} = e^z e^w$ this is a group homomorphism from $(\mathbb{C}, +)$ to $(\mathbb{C}^*, \times)$.

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

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

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

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

Second Isomorphism Theorem

Let $H \leq G$ and $K \lhd G$. Then $HK = \{hk : h \in H, k \in K\} \leq G$ and $H \cap K \lhd H$.

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

Proof: Let $h_1k_1, h_2k_2 \in HK$ (so $h_1h_2 \in H$ & $k_1k_2 \in K$)

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1h_2^{-1}}_{\in H} h_2k_1k_2^{-1}h_2^{-1} = \underbrace{h_1h_2^{-1}}_{\in H} \underbrace{h_2(k_1k_2^{-1})h_2^{-1}}_{\in K} \in HK$$

$\therefore HK \leq G$

Let $\phi: H \to G/K$

$h \to hK$.

This is the composite of inclusion $H \hookrightarrow G$ and the quotient map $G \to G/K$.

$\therefore \phi$ is a group homomorphism

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

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

First isomorphism thm. $\Rightarrow H/H\cap K \cong HK/K$ □

Remark 1.2 Suppose $K \lhd G$.

Then there is a bijection between {subgroups of G/K} and {subgroups of G containing K} given by $X \to \{g \in G : gK \in X\}$ [1] in the forward direction and $H \to H/K$ in the other.

This restricts to a bijection

{normal subgroups of G/K} $\longleftrightarrow$ {normal subgroups of G containing K}

.....

① $g_1k_1g_2k_2 \in g_1g_2K \in X$

Third Isomorphism Theorem

Let $K \leq H \leq G$ be normal subgroups of G.

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

Proof: Let $\phi : G/K \longrightarrow G/H$

$$gK \longrightarrow gH.$$

If $g_1K = g_2K$ then $g_2^{-1}g_1 \in K \leq H$

$$\Rightarrow g_1H = g_2H.$$

$\therefore \phi$ is well-defined

ϕ is a surjective group hom with

$\ker(\phi) = H/K$

Now apply the First Isomorphism Theorem. □

If $K \lhd G$ then studying the groups K and G/K can help in studying G.

However, sometimes this is useless.

Def^n: A group G is simple if $\{1\}$ and G are its only normal subgroups.

Lemma 1.3 An abelian group is simple iff it is isomorphic to C_p for some prime p.

Proof: By Lagrange's Theorem, a subgroup $H \leq C_p$ has order dividing $|C_p| = p$, hence 1 or p.

$\therefore |H| = 1$ or C_p. Thus C_p is simple.

Let G be an abelian (simple) group, & pick $1 \neq g \in G$.

Any subgroup of an abelian group is normal.

G contains the subgroup $\langle g \rangle = \{\ldots, g^{-1}, 1, g, \ldots\}$

Since G is simple this must be the whole group, i.e. G is cyclic.

If G infinite then $G \cong (\mathbb{Z}, +)$ and $2\mathbb{Z} \lhd \mathbb{Z}$ ⚔

Else $G \cong C_n$ for some n.

Let g be a generator.

If m/n then $g^{n/m}$ generates a subgroup of order m.

G simple $\Rightarrow$ only factors of n are 1 and n

$\Rightarrow \not\leftarrow$ n is prime. □

<u>Theorem 1.4</u> If G is a finite group then G has a <u>composition series</u>

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

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

[Warning: G_i need not be normal in G]

<u>Proof</u> By induction on $|G|$. Case $|G| = 1$ ✓

If $|G| > 1$ then take G_{m-1} to be a normal subgroup of G of largest possible order $\neq |G|$.

By Remark 1.2, G/G_{m-1} is simple.

Repeat for G_{m-1}. This process terminates since $|G| < \infty$ and $|G_{m-1}| < |G|$. □

So in a sense the finite simple groups are the building blocks for all finite groups.

§ 2 Group actions

Def^n: For X a set we let $\mathrm{Sym}(X)$ be the group of all bijections $X \to X$. (identity element $id = id_X$)

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

Ex: $S_n = \mathrm{Sym}(\{1, \dots, n\})$ is a perm. group of degree n, as is $A_n \leq S_n$

D_{2n} (= symmetry group of a regular n-gon) is a subgroup of $\mathrm{Sym}(\{\text{vertices of the } n\text{-gon}\})$

Def^n: An action of a group G on a set X is a function $* : G \times X \to X$ such that

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

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

Proposition 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 $X \to X$ call it ϕ_g sending $x \mapsto g * x$.

We have $\phi_{g_1 g_2}(x) = (g_1 g_2) * x \overset{\text{by (ii)}}{=} g_1 * (g_2 * x)$

$= \phi_{g_1}(\phi_{g_2}(x)) \quad \forall\ x \in X$

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

In particular $\phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \phi_e \overset{\text{by (i)}}{=} id$

$\therefore \phi_g \in \mathrm{Sym}(X)$

We define $\phi : G \to \mathrm{Sym}(X)$

$g \to \phi_g$.

This is a group hom. by (†).

Conversely let $\phi : G \to \mathrm{Sym}(X)$ be a group hom. We define

$* : G \times X \to X$

$(g, x) \to \phi(g)(x)$

Then (i) $e * x = \phi(e)(x) = id(x) = x$

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

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

$= g_1 * (g_2 * x)$. □

Def^n: We say $\phi : G \to Sym(X)$ is a permutation representation, of the group G.

Def^n: Let G act on X.

(i) The orbit of $x \in X$ is $orb_G(x) = \{g * x : g \in G\}$

(ii) The stabiliser of $x \in X$ is $G_x = \{g \in G : g * x = x\}$

We recall from IA

Orbit-Stabiliser Theorem There is a bijection

$orb_G(x) \longleftrightarrow G/G_x$ (set of left cosets of G_x in G).

In particular if G is finite then

$|G| = |orb_G(x)||G_x|$.

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

(ii) The orbits partition the set X

If there is only one orbit we say the action is transitive.

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

Ex: (i) Let G act on itself by left multiplication, i.e. $g * x = gx$. The kernel of this action is $\{g \in G : gx = x \ \forall x \in G\} = \{1\}$. $\therefore G \hookrightarrow Sym(G)$

Theorem 3.2 (Cayley) Any finite group is isomorphic to a subgroup of S_n for some n.

(ii) Let $H \leq G$. Then G acts on G/H by left multiplication, i.e.

$g * xH = gxH$.

This is a transitive action with

$$\begin{aligned} G_{xH} &= \{g \in G : gxH = xH\} \\ &= \{g \in G : x^{-1}gx \in H\} \\ &= \{g \in G : g \in xHx^{-1}\} \\ &= xHx^{-1}. \end{aligned}$$

$\ker(\phi) = \bigcap_{g \in G} gHg^{-1}$ This is the largest normal subgroup of G contained in H.

(iii) Let G act on itself by conjugation, i.e.

$g * x = gxg^{-1}$

The orbits & stabilisers have special names

$\text{orb}_G(x) = \{gxg^{-1} : g \in G\} = \text{cl}_G(x)$ "conjugacy class of x"

$G_x(x) = \{g \in G : gx = xg\} = C_G(x)$ "centraliser of x in G"

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

N.B. G also acts by conjugation on any normal subgroup

(iv) Let X be the set of all subgroups of G. Then G acts by conjugation on X: $g * H = gHg^{-1}$

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.

Theorem 3.3 Let G be a non-abelian simple group and $H \leq G$ be 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 G/H by left multiplication, and let $\phi: G \to \text{Sym}(G/H) \cong S_n$ be the associated permutation representation.

L3.4

As G is simple, $\ker(\phi) = 1$ or G.

If $\ker(\phi) = G$ then $\mathrm{Im}(\phi) = 1$, a contradiction as $n > 1$.

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

Since $A_n \triangleleft S_n$ we have $G \cap A_n \triangleleft G$.

But G is simple, so $G \cap A_n = 1$ or G.

In the first case, the second isomorphism theorem gives

$$G \cong \frac{G}{G \cap A_n} \cong \frac{G A_n}{A_n} \leq \frac{S_n}{A_n} \cong C_2$$

$\Rightarrow$ G abelian ⨳

$\therefore G \cap A_n = G$, i.e. $G \leq A_n$

Finally, for $n \leq 4$, A_n has no non-abelian simple subgroups (by looking at them). □

Example 2.4 Let G be the group of rotations of an icosahedron.

(20 faces, 12 vertices, 30 edges)

order	# elements in G
1	1
2	15
3	20
5	24
TOTAL	60

(If G acts on the set of vertices
$|G| = |\text{orbit}|\,|\text{stabiliser}| = 12 \cdot 5 = 60$)

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

If $H \lhd G$ then $|H| = 1 + 15a + 20b + 12c$
for some $a,b \in \{0,1\}$ & $c \in \{0,1,2\}$ and $|H|$ divides 60
$\therefore |H| = 1$ or 60. This shows G is simple.

We claim that the sets $H \setminus \{1\}$ for $H \leq G$ a subgroup of order 4 partition the 15 elements of order 2 into 5 sets of 3.

(i) $|H| = 4 \Rightarrow H \cong C_2 \times C_2$ or ~~C_4~~ ← since G has no element order 4

has 3 elements of order 2

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

$$|C_G(g)| = \frac{|G|}{|\text{cl}_G(g)|} = 60/15 = 4$$

(iii) Suppose $1 \neq g \in H \cap K$ where H & K are distinct groups of order 4. Then $|C_G(g)| \geq |HUK| > 4$. ※

since H and K are abelian

Let G act on $X = \{\text{subgroups of } G \text{ of order } 4\}$ by conjugation.
Obtain group hom. $\phi: G \longrightarrow \text{Sym}(X) \cong S_5$.

L 4.2 G simple $\Rightarrow \ker\phi = 1$ or G

$\therefore\ G \cong \mathrm{Im}\,\phi \leq S_5$ (so)

impossible else subgroups normal ⚠

Exactly as in the proof of Thm 2.3, $G \leq A_5$. But $|G| = |A_5|$. Hence $G \cong A_5$.

§3 Some simple 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
+	id	(1)
−	$(\cdot\cdot)$	10
+	$(\cdot\cdot\cdot)$	(20)
−	$(\cdot\cdot\cdot)(\cdot\cdot)$	20
+	$(\cdot\cdot)(\cdot\cdot)$	(15)
−	$(\cdot\cdot\cdot\cdot)$	30
+	$(\cdot\cdot\cdot\cdot\cdot)$	(24) → 12, 12
	TOTAL	120

Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$.

If $\exists$ odd permutation in $C_{S_n}(g)$ then $|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)|$ and hence $|\mathrm{cl}_{A_n}(g)| = |\mathrm{cl}_{S_n}(g)|$.

Otherwise $|C_{A_n}(g)| = |C_{S_n}(g)|$ and $|\mathrm{cl}_{A_n}(g)| = \frac{1}{2}|\mathrm{cl}_{S_n}(g)|$.

Example Taking $n=5$, (123) commutes with (45).

$(12)(34)$ commutes with (12).

If $h \in C_{S_n}(g)$ where $g = (12345)$ then

$(12345) = h(12345)h^{-1}$

$= h(1) \to h(2) \to h(3) \to h(4) \to h(5)$

$\Rightarrow h \in \langle g \rangle \leq A_5$, so $|\mathrm{cl}_{A_5}(g)| = \frac{1}{2}|\mathrm{cl}_{S_5}(g)| = 12$.

Exactly as in Ex 2.4 this shows A_5 is simple.

Lemma 3.1 A_n is generated by 3-cycles

Proof Each $\sigma \in A_n$ is a product of evenly many transpositions, so it suffices to show the product of any two transpositions can be written with 3-cycles. For a, b, c, d distinct

$(ab)(bc) = (abc)$ $\qquad$ $(ab)(cd) = (acb)(acd)$

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 (123). Indeed if (abc) is a 3-cycle, then $(abc) = \sigma(123)\sigma^{-1}$ 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 Suppose $1 \neq N \triangleleft G = A_n$. It suffices to show that N contains a 3-cycle, since then by Lemmas 3.1, 3.2 $N = A_n$.

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

Case 1 σ contains a cycle of length r for $r \geq 4$

w.l.o.g. $\sigma = (1 \dots r)\tau$ $\qquad$ Let $\delta = (1\,2\,3)$.

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

$\therefore$ N contains a 3-cycle

Case 2 σ contains 2 3-cycles

wlog $\sigma = (123)(456)\tau$ $\qquad$ Let $\delta = (124)$

$\sigma^{-1}\delta^{-1}\sigma\,\delta = (132)(465)(142)(123)(456)(124) = (12436)$

so done by Case 1.

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

Proof (ctd.) Let $1 \neq \sigma \in N \trianglelefteq A_n$

We write σ as a product of disjoint cycles.

Case 1 σ contains an r-cycle with $r \geq 4$

Case 2 σ contains two 3-cycles

Case 3 σ contains two 2-cycles

wlog $\sigma = (12)(34)\tau$

Let $\delta = (123)$.

$$\pi = \underbrace{\sigma^{-1}}_{\in N} \underbrace{\delta^{-1}\sigma\delta}_{\in N} = (12)(34)(132)(12)(34)(123) = (14)(23)$$

Let $\varepsilon = (235)$. using $n \geq 5$ again

$$\pi^{-1}\varepsilon^{-1}\pi\varepsilon = (14)(23)(253)(14)(23)(235) = (253)$$

$\therefore$ N contains a 3-cycle

Conclusion of proof It remains to consider σ with cycle type

$(\cdot\cdot)$ ⇓ $\sigma \notin A_n$ ⚡ , $(\cdot\cdot\cdot)$ ⇓ done , $(\cdot\cdot)(\cdot\cdot\cdot)$ ⇓ $\sigma \notin A_n$ ⚡ □

§4 p-groups & p-subgroups

Def^n A finite group G is a p-group if $|G| = p^n$ for some prime number p.

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

Proof For $g \in G$ we have

$$|\mathrm{cl}_G(g)| \cdot |C_G(g)| = |G| = p^n$$

So each conjugacy class has size a power of p.

Since G is a union of conjugacy classes

$$|G| \equiv \#(\text{conj. classes of size } 1) \pmod p$$

$$0 \equiv |Z(G)| \pmod p$$

Check: $g \in Z(G) \iff gx = xg \ \forall x \in G$

$\iff xgx^{-1} = g \ \forall x \in G$

L5.2 $\Leftrightarrow$ $cl_G(g) = \{g\}$

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 (* to Thm. 4.1) or G (G is abelian; Apply Lemma 1.3)

□

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

Proof By Theorem 1.4, G has a composition series

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

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

Corollary 4.2 $\Rightarrow$ $G_i/G_{i-1} \cong C_p$

$\therefore |G_i| = p^i \quad \forall\ 0 \leq i \leq m = a.$ □

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

Proof Let $gZ(G)$ generate $\frac{G}{Z(G)}$.

Then each coset is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$.

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

$g^{r_1} z_1,\ g^{r_2} z_2 = g^{r_1+r_2} z_1 z_2$ since z_1 central

$= g^{r_1+r_2} z_2 z_1$ " " "

$= g^{r_2} z_2 g^{r_1} z_1$ since z_2 central

$\therefore G$ is abelian □

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

Proof

$$Z(G) = \begin{cases} 1 & * \text{ Thm. 4.1} \\ p & \Rightarrow |G/Z(G)| = p. \text{ Apply Lemma 4.4} \\ p^2 & \Rightarrow G = Z(G) \text{ so done} \end{cases}$$

□

See ex sheet for groups of order p^3.

Sylow Theorems

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

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

(ii) All elements of $Syl_p(G)$ are conjugate.

(iii) The number $n_p = |Syl_p(G)|$ of Sylow p-subgroups satisfies

$n_p \equiv 1 \pmod p$ & $n_p \mid |G|$

(so in fact $n_p \mid m$)

Proof See next Lecture

Corollary 4.6 If $n_p = 1$ then the unique Sylow p-subgroup of G is normal.

Proof Let $g \in G$ and $P \in Syl_p(G)$.

Then $gPg^{-1} \leq G$ is another Sylow p-subgroup, so we must have $gPg^{-1} = P$ for all $g \in G$.

i.e. $P \trianglelefteq G$. □

Example Let $|G| = 1000 = 2^3 5^3$.

Then $n_5 \equiv 1 \pmod 5$ & $n_5 \mid 8$, 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 $n_{11} \mid 12$.

So $n_{11} = 1$ or 12. Suppose G is simple.

Then $n_{11} \neq 1$, else the 11-Sylow subgroup is normal

$\therefore$ $n_{11} = 12$

Now $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 44$.

$\therefore$ $n_3 = \cancel{1}$ (since G simple), 4, or 22

Suppose $n_3 = 4$. Then letting G act on $Syl_3(G)$ by

L3.4 conjugation gives a group hom

$\phi : G \to S_4$

$\ker\phi \triangleleft G \Rightarrow \ker\phi = 1$ or G

(G simple; $\ker\phi = G$: $*$ to Sylow (ii))

$\therefore G \hookrightarrow S_4 \Rightarrow 132 \leq 24$ $**$

Therefore $n_3 = 22$ & $n_{11} = 12$

$n_3 = 22$ ⇓ : G has $22 \cdot (3-1) = 44$ elements of order 3

$n_{11} = 12$ ⇘ : G has $12 \cdot (11-1) = 120$ elements of order 11

But $44 + 120 > 132 = |G|$ $*$

$\therefore G$ is not simple

Proof of the Sylow Theorems

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

(i) Let $\Omega = \{X \subseteq G : |X| = p^a\}$.

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

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

$\therefore |\Omega|$ is coprime to p (*)

Let G act on Ω by left multiplication, i.e.

if $X \in \Omega$, put $g * X = \{gx : x \in X\} \in \Omega$.

For $X \in \Omega$ we have

$$|G_x|\,|\mathrm{orb}_G(X)| = |G| = p^a m.$$

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

$\therefore p^a \mid |G_x|$ ①

On the other hand if $g_1 \in G$ and $x \in X$ then $g_1 \in (g_1 x^{-1}) * X$.

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

$\Rightarrow |G| \leq |\mathrm{orb}_G(X)|\,|p^a|$

$\Rightarrow |\mathrm{stab}(X)| = |G| / |\mathrm{orb}_G(X)| \leq |p^a|$ ②

① and ② $\Rightarrow |G_x| = p^a$, so G_x is a Sylow p-subgroup.

(ii) We prove a bit more

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 of p. Since $|G/P| = m$ is coprime to p, there must be an orbit of size 1.

i.e. $\exists\, g \in G$ s.t. $q * gP = gP$ for all $q \in Q$

$\Rightarrow g^{-1} q g \in P$ for all $q \in Q$

$\Rightarrow Q \leq gPg^{-1}$. □

(iii) Let G act on $\mathrm{Syl}_p(G)$ by conjugation. Sylow (ii) $\Rightarrow$ action is transitive. By orbit-stabiliser, $n_p \mid |G|$.

Remark: If $P \in \mathrm{Syl}_p(G)$, then n_p is the index of the normaliser of P in G, $N_G(P)$.

Now let $P \in \mathrm{Syl}_p(G)$. Then P acts on $\mathrm{Syl}_p(G)$ by conjugation. The orbits have sizes 1 or a multiple of p, since they divide $|P| = p^a$.

To show $n_p \equiv 1 \pmod p$, suffices to show there is a unique orbit of size 1.

If $\{Q\}$ is an orbit of size 1, then P normalises Q, i.e. $P \leq N_G(Q)$. Now P & Q are Sylow p-subgroups in $N_G(Q)$, 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. □

§ 5 Some matrix groups

For F a field (eg $\mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$),

$GL_n(F) = n \times n$ invertible matrices over F.

$SL_n(F) = \ker\left(GL_n(F) \xrightarrow{\det} F^* \right) \trianglelefteq GL_n(F)$

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

Def: $PGL_n(F) = GL_n(F)/Z$

$PSL_n(F) = SL_n(F)/Z \cap SL_n(F) \cong ZSL_n(F)/Z \leq PGL_n(F)$

(↑ second isomorphism theorem)

Example 5.1 Let $G = GL_n(\mathbb{Z}/p\mathbb{Z})$.

We note that n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ are the columns of some $A \in G$ iff they are linearly independent.

$$\therefore |G| = \underbrace{(p^n-1)}_{\text{first vec}}\underbrace{(p^n-p)}_{\text{second vec}}\underbrace{(p^n-p^2)}_{\text{third vec}}\cdots\underbrace{(p^n-p^{n-1})}_{n^{th}\text{ vec}}$$

$$\Rightarrow |G| = p^{1+2+\cdots+n-1}(p^n-1)(p^{n-1}-1)\cdots(p-1)$$

$$= p^{\binom{n}{2}}\prod_{i=1}^{n}(p^i-1)$$

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

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

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

Just as $PGL_2(\mathbb{C})$ acts on $\mathbb{C}\cup\{\infty\}$ via Möbius maps, $PGL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z}\cup\{\infty\}$. Indeed $GL_2(\mathbb{Z}/p\mathbb{Z})$ acts via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to z$ goes to $\frac{az+b}{cz+d}$ and since scalar matrices act trivially, this gives an action of $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 5.2 The permutation representation $PGL_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow S_{p+1}$ is injective. (in fact an isomorphism for $p=2$ or 3.)

Proof Suppose $\frac{az+b}{cz+d} = z \;\forall\; z$. Putting $z=0$ shows $b=0$. Putting $z=\infty$ shows $c=0$. Putting $z=\infty$ shows $a=d$.

$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a scalar matrix, so trivial in $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 5.3 If p is an odd prime then $|PSL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{p(p^2-1)}{2}$.

Proof By Example 5.1,

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

The map $\det: GL_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^*$ is a group homomorphism with kernel $SL_2(\mathbb{Z}/p\mathbb{Z})$. It is also surjective, e.g. $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mapsto a$.

By the isomorphism theorem $\frac{GL_2(\mathbb{Z}/p\mathbb{Z})}{SL_2(\mathbb{Z}/p\mathbb{Z})} \cong (\mathbb{Z}/p\mathbb{Z})^*$.

$$\therefore |SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{1}{p-1}|GL_2(\mathbb{Z}/p\mathbb{Z})| = p(p^2-1)$$

If $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in SL_2(\mathbb{Z}/p\mathbb{Z})$ then $\lambda^2 \equiv 1 \pmod p$

$\Rightarrow p \mid (\lambda-1)(\lambda+1) \Rightarrow \lambda \equiv \pm 1 \pmod p$.

So the only scalar matrices in $SL_2(\mathbb{Z}/p\mathbb{Z})$ are $\pm I_2$

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

Example 5.4 $G = PSL_2(\mathbb{Z}/5\mathbb{Z})$

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

Let G act on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}$.

By Lemma 5.2 this gives an injective permutation representation

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

Claim $Im(\phi) \leq A_6$, i.e. the map $\psi: G \xrightarrow{\phi} S_6 \xrightarrow{sgn} \{\pm 1\}$ is trivial.

Remark If we knew G is simple, then this would follow from the fact $\ker\psi \lhd G$.

If $g \in G$ has odd order then $\psi(g)$ has odd order $\Rightarrow \psi(g) = 1$.

So it suffices to consider $g \in G$ with order a power of 2.

By Lemma 4.7, every such element belongs to a 2-Sylow subgroup, and all Sylow 2-subgroups are conjugate.

Since ψ maps to an abelian group, any two conjugate elements in G have the same image.

L7.2 So it suffices to show ψ is trivial on some Sylow 2-subgroup,

e.g. $H = \left\langle \pm\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq G = \dfrac{SL_2(\mathbb{Z}/5\mathbb{Z})}{\{\pm I_2\}}$

$\phi\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = (14)(23) \quad (z \to -z)$

$\phi\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (0\,\infty)(14) \quad (z \to \frac{-1}{z})$

These are even permutations. $\therefore \psi$ is trivial

Now $G \hookrightarrow A_6$ & $|G| = 60$.

ES1, Q14 shows $G \cong A_5$

Def^n An <u>automorphism</u> of a group G is an isomorphism from G to itself. The automorphisms of a group G form a subgroup

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

<u>Facts</u> (not proved in this course)

$PSL_n(\mathbb{Z}/p\mathbb{Z})$ is a simple group for all $n \geq 2$, p prime except for $(n,p) = (2,2)$ or $(2,3)$

The two smallest non-abelian simple groups are

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

$PSL_2(\mathbb{Z}/7\mathbb{Z})$ order 168

$\cong GL_3(\mathbb{Z}/2\mathbb{Z})$

§6 Finite Abelian Groups

Later in the course, we prove

<u>Theorem 6.1</u> Every finite abelian group is isomorphic to a product of cyclic groups.

However, such a decomposition need not be unique.

<u>Lemma 6.2</u> If m & n are coprime then $C_m \times C_n \cong C_{mn}$

<u>Proof</u> Let g and h be generators for C_m and C_n. We have $(g,h) \in C_m \times C_n$ & $(g,h)^r = (g^r, h^r)$.

In particular $(g,h)^r = 1 \iff m \mid r$ & $n \mid r \iff mn \mid r$. (since they are coprime)

$\therefore (g,h)$ 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 $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ with p_i distinct primes then Lemma 6.2 shows $C_n \cong C_{p_1^{a_1}} \times \cdots \times C_{p_r^{a_r}}$

The general case follows by Theorem 6.1 □

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

Theorem 6.4 Let G be a finite abelian group. Then

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

where $d_1 \mid d_2 \mid \cdots \mid d_t$.

Remark 6.5 The integers $n_1, \ldots, n_k$ in Cor 6.3 (up to order) and the integers $d_1, \ldots, d_t$ in Thm 6.4 (assuming $d > 1$) are uniquely determined by G.

The proof (which we omit) works by counting the number of elements of G of each given order (prime power orders suffice).

Examples (i) The abelian groups of order 8 are

$$C_8, \quad C_2 \times C_4 \quad \& \quad C_2 \times C_2 \times C_2$$

(ii) The abelian groups of order 12 are

$C_2 \times C_2 \times C_3$ & $C_4 \times C_3$ (using Cor 6.3)

$\overset{\text{II's}}{C_2 \times C_6}$ & $\overset{\text{II's}}{C_{12}}$ (using Thm 6.4)

§7 Rings – definition and examples

Def^n A ring is a triple $(R, +, \cdot)$ consisting of a set R and two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ satisfying (i) $(R, +)$ is an abelian group, with identity $0 = 0_R$

(ii) multiplication is associative and has an identity

i.e. $x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \forall\, x, y, z \in R$

and $\exists\, 1 \in R$ s.t. $1 \cdot x = x \cdot 1 = x \quad \forall\, x \in R$

" 1_R "

(iii) Distributive laws $\left.\begin{aligned} x \cdot (y+z) &= x \cdot y + x \cdot z \\ (x+y) \cdot z &= x \cdot z + y \cdot z \end{aligned}\right\} \forall\, x, y, z \in R$

Remark (i) For $x \in R$ write $-x$ for its inverse under addition & abbreviate e.g. $x + (-y) = x - y$

(ii) $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$

$\Rightarrow 0 \cdot x = 0 \quad \forall\, x \in R$

(iii) $0 = 0 \cdot x = (1-1) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x$

$\Rightarrow (-1) \cdot x = -x \quad \forall\, x \in R$

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

Def^n R is commutative if $x \cdot y = y \cdot x \quad \forall\, x, y \in R$

In this course we only consider commutative rings

Def^n A subset $S \subset R$ is a subring (written $S \leq R$) if it is a ring under the same operations $+$ and $\cdot$, with the same identities 0 and 1. extra

Examples (i) We have subrings

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$$

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

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

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

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

New rings from old

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

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

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

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

i.e. $$\left.\begin{aligned}(f+g)(x) &= f(x) + g(x)\\ (fg)(x) &= f(x)\, g(x)\end{aligned}\right\} \forall x \in X$$

Further interesting examples appear as subrings

e.g. $\{$continuous functions $\mathbb{R} \to \mathbb{R}\}$

(iii) Let R be a ring and S the set of sequences $(a_0, a_1, a_2, \ldots)$ $a_i \in R$ with $a_i = 0$ for all i suff. large

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$
$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

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

It can be checked that S is a ring.

We identify R with the subring $\{(a, 0, 0, \ldots) : a \in R\} \leq S$.

Define $X = (0, 1, 0, 0, \ldots)$.

Then $X^n = (\underbrace{0, \ldots, 0}_{n \text{ zeroes}}, 1, 0, \ldots)$ and

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

$\therefore$ S is the ring of polynomials with coefficients in R

$\overset{\frown}{} R[X]$

Remark Let $R = \mathbb{Z}/p\mathbb{Z}$, p prime, and $f(X) = X^p - X$. (?)

The function $R \to R$, $x \mapsto f(x)$ is the zero function, but the polynomial f is non-zero.

L 8.3

Further examples

(i) $R[X_1, \dots, X_n]$ = polynomials in indeterminates $X_1, \dots, X_n$ with coefficients in R

(we could define $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$)

(ii) Power series ring

$R[[X]] = \{ a_0 + a_1 X + a_2 X^2 + \cdots : a_i \in R \}$

(iii) Laurent polynomials

$R[X, X^{-1}] = \{ \sum_{i \in \mathbb{Z}} a_i X^i : a_i \in R$ and only finitely many nonzero$\}$

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

(N.B. 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. $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Def^n 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

$$x = 1 \cdot x = 0 \cdot x = 0$$

$\therefore R = \{0\}$ is the trivial ring.

Lemma 7.1 Let $f, g \in R[X]$. Suppose the leading coefficient of g is a unit. Then there exist $q, r \in R[X]$ s.t.

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

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

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

Write $f(X) = a_n X^n + \cdots + a_1 X + a_0$, $a_n \neq 0$

$g(X) = b_m X^m + \cdots + b_1 X + b_0$, $b_m \in R^*$.

If $n < m$ then $q = 0$ & $r = f$ ✓

Otherwise we have $n \geq m$. 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

$$f_1(X) = q_1(X) g(X) + r_1(X) \quad \text{with } \deg(r_1) < \deg(g).$$

$$\Rightarrow f(X) = \underbrace{\left(q_1(X) + a_n b_m^{-1} X^{n-m} \right)}_{q(X)} g(X) + \underbrace{r_1(X)}_{r(X)}$$

□

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

§ 8 Ideals & Quotients

Def^n: If R, S are rings, a function $\phi : R \to S$ is a ring homomorphism if
(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \quad \forall\, r_1, r_2 \in R$
(ii) $\phi(r_1 r_2) = \phi(r_1)\,\phi(r_2) \quad \forall\, r_1, r_2 \in R$
(iii) $\phi(1_R) = 1_S$

A ring homomorphism which is also a bijection is called an isomorphism.

The kernel of ϕ is $\mathrm{Ker}(\phi) = \{ r \in R : \phi(r) = 0_S \}$.

Lemma 8.1 A ring homomorphism is injective iff its kernel is $\{0\}$.

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

Def^n: A subset $I \subset R$ is an ideal (written $I \lhd R$) if
(i) I is a subgroup of $(R, +)$
(ii) $\forall\, r \in R$, $x \in I$, we have $rx \in I$

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

Lemma 8.2 If $\phi : R \to S$ is a ring hom., then $\mathrm{Ker}(\phi) \lhd R$.

Proof: $\phi : (R, +) \longrightarrow (S, +)$ is a gp. hom. so $\mathrm{Ker}(\phi)$ is a subgp of $(R, +)$.
If $r \in R$ and $x \in \mathrm{Ker}(\phi)$ then
$\phi(rx) = \phi(r)\,\phi(x) = \phi(r) \cdot 0_S = 0_S$
$\therefore\ rx \in \mathrm{Ker}(\phi)$ □

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

Proof: Certainly $n\mathbb{Z} \lhd \mathbb{Z}$.
Let $I \lhd \mathbb{Z}$ be a non-zero ideal, so a subgroup of $(\mathbb{Z}, +)$.

Let n be the smallest positive element of I. Then $n\mathbb{Z} \subset I$. If $m \in I$ then $m = qn + r$, $q, r \in \mathbb{Z}$, $0 \leq r < n$. Then $r = m - qn \in I$. This contradicts the choice of n unless $r = 0$.

But then $m \in n\mathbb{Z}$. $\therefore I = n\mathbb{Z}$ □

Def^n For $a \in R$ we write $(a) = \{ ra : r \in R \} \lhd R$. This is called the ideal generated by a.

More generally for $a_1, \ldots, a_n \in R$,

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

Def^n Let $I \lhd R$. If $I = (a)$ for some $a \in R$, we say I is principal

Lemma 8.3 showed every ideal in $\mathbb{Z}$ is principal.

Proposition 8.4 If $I \lhd R$ 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 $\pi : R \to R/I$, $r \to r + I$ is a ring hom. (called the quotient map.)

Proof: We already know that $(R/I, +)$ is a group.

If $r_1 + I = r_1' + I$ & $r_2 + I = r_2' + I$, then $r_1' = r_1 + a_1$ $r_2' = r_2 + a_2$ for some $a_1, a_2 \in I$.

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

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

The remaining properties of R/I follow from those of R. □

Examples (i) We have $n\mathbb{Z} \lhd \mathbb{Z}$, so we form the quotient $\mathbb{Z}/n\mathbb{Z}$. Its elements are $0+n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}$. Addition & multiplication are carried out mod n.

(ii) Consider $(X) \lhd \mathbb{C}[X]$. This is the ideal of polynomials with no constant term.

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

then $f + (X) = a_0 + (X)$. We get a bijection $\mathbb{C}[X]/(X) \leftrightarrow \mathbb{C}$

$f + (X) \mapsto f(0)$

$a + (X) \leftarrow\!\shortmid\ a$

These maps are ring homomorphisms.

$\therefore \mathbb{C}[X]/(X) \cong \mathbb{C}$

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

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

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

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

If $a + bX + (X^2+1) = a' + b'X + (X^2+1)$ then

$(a-a') + (b-b')X = q(X)(X^2+1)$ for some $q \in \mathbb{R}[X]$.

Comparing degrees, we see $q(X) = 0$, $a = a'$, $b = b'$.

There is a bijection $\phi : \dfrac{\mathbb{R}[X]}{(X^2+1)} \longleftrightarrow \mathbb{C}$

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

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

$$\phi\big((a + bX + (X^2+1))(c + dX + (X^2+1))\big)$$

$$= \phi(ac + (ad+bc)X + bd\cancel{(X^2+1)} - bd + (X^2+1))$$

$$= ac - bd + (ad+bc)i$$

$$= (a+bi)(c+di) = \phi(a + bX + (X^2+1))\,\phi(c + dX + (X^2+1)).$$

First Isomorphism Theorem

Let $\phi: R \to S$ be a ring homomorphism.

Then $\mathrm{Ker}(\phi) \lhd R$ and

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

Proof We already saw $\mathrm{Ker}(\phi) \lhd R$ (Lemma 8.2) and that $\mathrm{Im}(\phi)$ is a subgroup of $(S,+)$ (see isomorphism thm for groups).

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

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

$\therefore \mathrm{Im}(\phi) \leq S$

Let $K = \mathrm{Ker}(\phi)$. We define $\Phi: R/K \longrightarrow \mathrm{Im}(\phi)$

$r + K \longrightarrow \phi(r)$.

This is well defined, a bijection, and a group homomorphism under $+$, by the first isomorphism thm for groups.

Also $\Phi(1_R + K) = \phi(1_R) = 1_S$ and

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

□

Second Isomorphism Theorem

Let $R \leq S$ and $J \lhd S$.

Then $R \cap J \lhd R$ and $R + J \leq S$ and

$$R/R\cap J \cong R+J/J \leq S/J.$$

Proof: Clearly $R+J$ is a subgroup of $(S,+)$.

It contains 1, and if $r_1, r_2 \in R$ and $x_1, x_2 \in J$ then

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

So $R + J \leq S$.

Let $\phi: R \to S/J$. This is the composite of the inclusion $R \subset S$

$r \to r+J$

and the quotient map $S \to S/J$, therefore a ring homomorphism.

$\ker(\phi) = \{ r \in R : r+J = J \} = R \cap J \lhd R$

$\mathrm{Im}(\phi) = \{ r+J : r \in R \} = R+J/J$

Apply first isomorphism theorem. □

Analogous to the situation for groups, we have a bijection

$\{$ ideals in $R/I \} \longleftrightarrow \{$ ideals in R containing $I \}$

$K \longrightarrow \{ r \in R : r+I \in K \}$

$J/I \longleftarrow J$

Third Isomorphism Theorem

Let $I \lhd R$ and $J \lhd R$ with $I \subseteq J$.

Then $J/I \lhd R/I$ and $R/I \,/\, J/I \cong R/J$.

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

$r+I \to r+J$.

This is a ring homomorphism (well defined since $I \subset J$).

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

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

Apply first isomorphism theorem. □

Example There is a surjective ring homomorphism

$\phi: \mathbb{R}[X] \longrightarrow \mathbb{C}$

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

Using Lemma 7.1 we find $\ker(\phi) = (X^2+1)$.

First isomorphism theorem gives

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

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

$$0 \to 0_R$$
$$1 \to 1_R$$
$$n \to \underbrace{1_R + \cdots + 1_R}_{n \text{ terms}}$$
$$-n \to -(1_R + \cdots + 1_R)$$

Since $\ker(\iota) \trianglelefteq \mathbb{Z}$ we have $\ker(\iota) = n\mathbb{Z}$ for some $n \in \{0, 1, \ldots\}$

By the first isomorphism

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

Def^n: We call n the characteristic of R.

For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0, whereas $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}[X]$ have characteristic p.

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

§ 9 Integral domains, maximal and prime ideals

Def^n An integral domain is a ring R with $0 \neq 1$ such that for $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

A zero divisor in a ring R is a non-zero element $a \in R$ such that $ab = 0$ for some $0 \neq b \in R$.

So an integral domain is a ring without zero divisors.

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

(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
e.g. $(1, 0) \cdot (0, 1) = (0, 0)$

Lemma 9.1 R an integral domain $\Rightarrow$ $R[X]$ an integral domain

Moreover if $f, g \in R[X]$ are non-zero then

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

Proof Write $f(X) = a_m X^m + \cdots + a_1 X + a_0$ with $a_m \neq 0$

$g(X) = b_n X^n + \cdots + b_1 X + b_0$ " $b_n \neq 0$

Then $fg(X) = \underbrace{a_m b_n}_{\neq 0 \text{ since } R \text{ an integral domain}} X^{n+m} + \cdots$

So $fg \neq 0$ and $\deg(fg) = m+n = \deg(f) + \deg(g)$. □

Lemma 9.2 Let R be an integral domain and $0 \neq f \in R[X]$. Then $\#\{a \in R : f(a) = 0\} \leq \deg(f)$.

Proof See ex. sheet

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

Proof Let F be a field, $A \leq F^*$ finite. A is a finite abelian group.

If it is not cyclic then by Thm 6.4 (structure theorem for finite abelian groups) it contains a subgroup $C_m \times C_m$ for some $m \geqslant 2$. But then the polynomial $X^m - 1 \in F[X]$ has degree m, and yet $\geqslant m^2$ roots, contradicting Lemma 9.2 □

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

$\mu_m = \{x \in \mathbb{C} : x^m = 1\} \leq \mathbb{C}^*$ is cyclic

$\{$ ideals in $R/I\} \longleftrightarrow \{$ ideals in R containing $I\}$

$K \longrightarrow \{r \in R : r + I \in K\}$

Proposition 9.4 Any finite integral domain is a field

Proof Let R be a finite integral domain.

Let $0 \neq a \in R$.

Consider the map $\phi : R \longrightarrow R$

$x \longrightarrow ax$

If $\phi(x) = \phi(y)$ then $a(x-y) = 0 \Rightarrow x = y$

(R integral, $a \neq 0$)

$\therefore \phi$ injective

R finite $\Rightarrow \phi$ surjective

$\therefore \exists\, b \in R$ s.t. $ab = 1$ i.e. a is a unit

$\therefore R$ is a field □

Theorem 9.5 Let R be an integral domain.

Then there is a field F such that

(i) $R \leq F$, and

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

F is called the field of fractions of R.

Proof Consider the set $S = \{(a,b) \in R^2 : b \neq 0\}$ 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 $(ad)f = (bc)f = b(cf) = b(de)$.

$\Rightarrow d(af - be) = 0$.

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 $\frac{a}{b} = [(a,b)]$.

Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

These operations are easily checked to be well-defined, and make F a ring, with $0_F = [(0_R, 1_R)]$, $1_F = [(1_R, 1_R)]$.

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.

We identify R with $\left\{ \frac{r}{1_R} : r \in R \right\} \leq F$.

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

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

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

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

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

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

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

Lemma 9.6 A non-zero ring R is a field

$\Leftrightarrow$ its only ideals are $\{0\}$ & R

Proof "$\Rightarrow$" If $0 \neq I \lhd R$ then I contains a unit, and hence $I = R$.

"$\Leftarrow$" If $0 \neq x \in R$ then the principal ideal (x) is non-zero, so $(x) = R$, and $\exists\, y \in R$ s.t. $xy = 1$, i.e. x is a unit □

Def^n (i) Let S be a collection of subsets of a set X. $A \in S$ is maximal if $\nexists\, B \in S$ with $A \subsetneq B$.

(ii) An ideal $I \lhd R$ is maximal if it is maximal among all proper ideals of R.

i.e. $\nexists\ J \lhd R$ with $I \subsetneq J \subsetneq R$

Proposition 9.7 Let $I \lhd R$ be an ideal.

I maximal $\iff$ R/I is a field.

Proof R/I is a field
$\iff$ I/I & R/I are the only ideals of R/I
$\iff$ I & R are the only ideals of R containing I
$\iff$ $I \lhd R$ is maximal. □

Def^n An ideal $I \lhd R$ 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 9.8 The ideal $n\mathbb{Z} \lhd \mathbb{Z}$ is a prime ideal iff $n = 0$ or $n = p$ is a prime number.

Indeed if $ab \in p\mathbb{Z}$ then $p \mid ab$, so $p \mid a$ or $p \mid b$, so $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Conversely, if $n = uv$ is composite (so $u, v > 1$) then $uv \in n\mathbb{Z}$, yet $u \notin n\mathbb{Z}$, $v \notin n\mathbb{Z}$

Proposition 9.9 Let $I \lhd R$ be an ideal.

I is prime $\iff$ R/I is an integral domain

Proof I is prime
$\iff$ whenever $a, b \in R$ with $ab \in I$, 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. □

Example Let R be a ring. Recall there is a unique ring homomorphism $\iota : \mathbb{Z} \to R$. Moreover $\mathrm{Im}(\iota) \cong \mathbb{Z}/n\mathbb{Z}$ where $n \in \{0, 1, 2, \dots\}$ is the characteristic of R.

If R is an integral domain, then so is any subring, in particular $\mathbb{Z}/n\mathbb{Z}$. But then $n\mathbb{Z} \lhd \mathbb{Z}$ is prime,

so by Example 9.8, $n = 0$ or $n = p$ is a prime number.

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

§10 Factorisation in integral domains

In this section R is always an integral domain.

Def: (i) $a \in R$ is a unit if $\exists\, b \in R$ s.t. $ab = 1$

equivalently $(a) = R$

(ii) $a \in R$ divides $b \in R$ (written $a \mid b$) 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 $a \mid b$ & $b \mid a$

equivalently $(a) = (b)$

(iv) $r \in R$ is irreducible if it is nonzero, not a unit, and $\boxed{r = ab \Rightarrow a \text{ or } b \text{ is a unit}}$

(v) $r \in R$ is prime if it is nonzero, not a unit, and $\boxed{r \mid ab \Rightarrow r = a \text{ or } r = b}$

These properties depend on the ambient ring R

e.g. 2 is prime and irreducible in $\mathbb{Z}$, but a unit in $\mathbb{Q}$

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

Lemma 10.1 (r) is prime ideal in R

$\Leftrightarrow r = 0$ or r is prime

Proof "$\Rightarrow$" Suppose (r) is prime & $r \neq 0$

As prime ideals are proper, $(r) \neq R$, so r is not a unit

If $r \mid ab$ then $ab \in (r)$ so $a \in (r)$ or $b \in (r)$

$\Rightarrow r \mid a$ or $r \mid b$

"$\Leftarrow$" $\{0\} \lhd R$ is prime since R is an integral domain

Let $r \in R$ be prime. If $ab \in (r)$ then $r \mid ab$ so $r \mid a$ or $r \mid b$

so $a \in (r)$ or $b \in (r)$. □

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

Proof Let $r \in R$ be a prime. By def^n it is non-zero & not a unit. Suppose $r = ab$.

Then $r|ab$, so $r|a$ or $r|b$.

Suppose $r|a$, say $a = rc$ for some $c \in R$

$\Rightarrow r = ab = rcb \Rightarrow r(1-cb) = 0$

As $r \neq 0$, and R is an integral domain, $1 - bc = 0$

so $bc = 1$. Then b is a unit.

Likewise if $r|b$ then a is a unit. □

The converse does not hold in general.

Example $R = \mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5} : a, b \in \mathbb{Z} \} \leq \mathbb{C}$

It is a subring of a field, so an integral domain.

Define a function $N : R \to \mathbb{Z}_{\geq 0}$ "the norm"

$$z = a + b\sqrt{-5} \to |z|^2 = a^2 + 5b^2$$

& note that $N(z_1 z_2) = N(z_1) N(z_2)$

Claim The only units in R are ± 1

Proof If $r \in R$ is a unit, i.e. $rs = 1$ for some $s \in R$,

then $N(r) N(s) = N(rs) = N(1) = 1$

$\Rightarrow N(r) = 1$. 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 $2 = rs$. Take norms to get

$N(r) \# \cdot N(s) = 4$. Since $a^2 + 5b^2 = 2$ has no solutions

with $a, b \in \mathbb{Z}$, there are no elements of norm 2.

$\therefore N(r) = 1$, $N(s) = 4$ or viceversa

But $N(r) = 1 \Rightarrow r$ is a unit □

Similarly 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are irreducible, as there are no elements of norm 3.

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

$\therefore 2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$

yet $2 \nmid 1+\sqrt{-5}$, $2 \nmid 1-\sqrt{-5}$ ← seen by taking norms or by noting $\frac{1+\sqrt{-5}}{2} \notin R$

Two lessons

(i) irreducible $\not\Rightarrow$ prime

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

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

Def^n An integral domain R is a principle ideal domain (PID) if every ideal of R is principal

i.e. is of the form (a) for some $a \in R$

e.g. $\mathbb{Z}$ is a PID by Lemma 8.3

Next lecture: $\mathbb{Z}[i]$ & $F[X]$ for F a field are PIDs

Lemma 10.3 Let $0 \neq r \in R$. If (r) is maximal, 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 $(r) \subseteq (a) \lhd R$.

(r) maximal $\Rightarrow$ either $(r) = (a)$ or $(a) = R$

$\Downarrow$ b is a unit

$\Downarrow$ a is a unit

can also do: (r) max. $\Rightarrow$ (r) prime; r irred $\Leftarrow$ r prime

$\therefore$ r is irreducible

Conversely, suppose r is irreducible and $(r) \subseteq J \subseteq R$ for some ideal J.

R a PID $\Rightarrow J = (a)$ for some $a \in R \Rightarrow r = ab$ for some $b \in R$

Since r is irreducible, either a is a unit or b is a unit

$\Downarrow$ $J = R$

$\Downarrow$ $(r) = J$

$\therefore$ (r) is maximal $\square$

Def^n An integral domain R is a Euclidean Domain (ED) if there is a function $\phi : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ (a Euclidean function) such that (i) if $a \mid b$ then $\phi(a) \leq \phi(b)$

(ii) if $a, b \in R$ with $b \neq 0$, then $\exists\, q, r \in R$ s.t. $a = qb + r$ and either $r = 0$ or $\phi(r) < \phi(b)$

Proposition 10.4 If R is a Euclidean Domain then it is a Principal Ideal Domain (i.e. ED $\Rightarrow$ PID)

Proof Let R have Euclidean function $\phi : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$.

Let $I \lhd R$ be a non-zero ideal, & choose $b \in I \setminus \{0\}$ with $\phi(b)$ minimal.

We have $(b) \subseteq I$.

For $a \in I$, write $a = qb + r$, with $q, r \in R$, and either $r = 0$ or $\phi(r) < \phi(b)$.

But $r = a - qb \in I$, so 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 def^n of ED is that it allows us to describe the units as $R^* = \{u \in R \setminus \{0\} : \phi(u) = \phi(1)\}$ ☺

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)

(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 (i) is clear.

For property (ii), let $z_1, z_2 \in \mathbb{Z}[i]$ with $z_2 \neq 0$.

Consider $\frac{z_1}{z_2} \in \mathbb{C}$. This is at most distance 1 from the nearest element of $\mathbb{Z}[i]$.

So we write $\frac{z_1}{z_2} = q + \varepsilon$ with $q \in \mathbb{Z}[i]$, $|\varepsilon| < 1$

$\Rightarrow z_1 = q z_2 + \underbrace{\varepsilon z_2}_{r}$.

Then $r = z_1 - q z_2 \in \mathbb{Z}[i]$ & $\phi(r) = |\varepsilon z_2|^2 < |z_2|^2 = \phi(z_2)$.

It follows by Prop. 10.4 that $\mathbb{Z}[i]$ & $F[X]$ for F a field, are PIDs.

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

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

If $f, g \in I$ then $(f \pm g)(A) = f(A) \pm g(A) = 0$.

If $f \in F[X]$ and $g \in I$ then $(fg)A = f(A)\,g(A) = 0$.

So $I \lhd F[X]$ is an ideal.

$F[X]$ is a PID $\Rightarrow I = (f)$ for some $f \in F[X]$ which we may suppose is monic by dividing by a unit.

Note that for $g \in F[X]$,

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

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 $\deg(g), \deg(h) > 0$ then one of the factors is linear, so f has a root. But $f(0) \neq 0$ & $f(1) \neq 0$.

$\therefore f$ is irreducible

↑ ↑ ↑

Since $\mathbb{F}_2[X]$ is a PID, it follows by Lemma 10.3 that $(f) \lhd \mathbb{F}_2[X]$ is a maximal ideal, hence

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

is a field, and it has order 8.

L13.3

Def^n An integral domain is a unique factorisation domain (UFD) if

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

(ii) if $p_1 \cdots p_m = q_1 \cdots q_n$ where the p_i and q_i are irreducibles then $m=n$ and we may re-order s.t. p_i is an associate of q_i $\forall\ 1 \leq i \leq n$.

Lemma 10.5 Let R be an integral domain satisfying (i) in the def^n of a UFD. Then R is a UFD $\Leftrightarrow$ every irreducible of R is prime

Proof "$\Rightarrow$" Suppose $p \in R$ irreducible, and $p \mid ab$, say $ab = pc$. Writing a, b, c as products of irreducibles it follows by (ii) that $p \mid a$ or $p \mid b$.

"$\Leftarrow$" Suppose $p_1 \cdots p_m = q_1 \cdots q_n$ with each p_i, q_i irreducible.

Since p_1 is prime & $p_1 \mid q_1 \cdots q_n$ we have $p_1 \mid q_i$ for some i. After reordering we may suppose $p_1 \mid q_1$, i.e. $q_1 = up_1$ for some $u \in R$.

q_1 irreducible, p_1 not a unit $\Rightarrow$ u is a unit

$\therefore$ p_1 and q_1 are associates

Cancelling p_1 gives $p_2 \cdots p_m = (uq_2) \cdots q_n$.

The result follows by induction. □

Lemma 10.6 Let R be a PID. Then every irreducible in R is prime.

Proof (Version 1) Let $p \in R$ be irred. & suppose $p \mid ab$ & $p \nmid a$.

R a PID $\Rightarrow (a,p) = (d)$ 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 $(a,p) = (p)$ so $p \mid a$ ✗

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

$\Rightarrow \exists\ r, s \in R$ s.t. $ra + sp = 1$

$\Rightarrow b = rab + spb$

Since $p \mid ab$ this gives $p \mid b$. $\therefore$ p is prime □

Lemma 10.6 In a PID every irreducible element is prime

Proof (Version 1) – see last time

(Version 2) p irreducible $\Rightarrow$ (p) is maximal (Lemma 10.3)

hypothesis R a PID used here

$\Rightarrow$ $R/(p)$ is a field

$\Rightarrow$ $R/(p)$ is an integral domain

$\Rightarrow$ (p) is prime

$\Rightarrow$ p is prime (Lemma 10.1)

Lemma 10.7 Let R be a PID and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ a nested sequence of ideals. Then $\exists\, N \in \mathbb{N}$ s.t. $\forall\, n \geq N$, $I_n = I_{n+1}$

(Rings satisfying this "ascending chain condition" are called Noetherian – more on this later)

Proof Let $I = \bigcup_{i=1}^{\infty} I_i$. This is an ideal in R.

As R is a PID, $I = (a)$ for some $a \in R$.

Then $a \in \bigcup_{i=1}^{\infty} I_i \Rightarrow a \in I_N$ for some N.

Then for $n \geq N$, $(a) \subseteq I_N \subseteq I_n \subseteq I = (a)$ and so $I = I_n$. □

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

Proof We need to check (i) and (ii) in defn of a 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, y_1 is not a product of irreducibles, say it's x_1.

We have $(x) \subsetneq (x_1)$ 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 obtain $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$ ⚡ to Lemma 10.7

(ii) See Lemmas 10.5 and 10.6 □

Examples

	ED $\Rightarrow$	PID $\Rightarrow$	UFD $\Rightarrow$	integral domain	
$\mathbb{Z}/4\mathbb{Z}$	×	×	×	×	
$\mathbb{Z}[\sqrt{-5}]$	×	×	×	✓	] see earlier

L14.2

	ED ⇒	PID ⇒	UFD ⇒	integral domain	
$\mathbb{Z}[X]$	×	×	✓	✓	] see below
$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$	×	✓	✓	✓	] see Part II Number Fields
$\mathbb{Z}[i]$	✓	✓	✓	✓	

The ring $\mathbb{Z}[X]$ is not a PID.

Indeed, consider $I = (2, X) \lhd \mathbb{Z}[X]$.

Then $I = \{ 2f_1(X) + Xf_2(X) : f_1, f_2 \in \mathbb{Z}[X] \}$

$= \{ f \in \mathbb{Z}[X] : f(0) \text{ is even} \}$.

Suppose $I = (f)$ for some $f \in \mathbb{Z}[X]$.

Then $2 \in I \Rightarrow 2 = fg$ for some $g \in \mathbb{Z}[X]$.

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

$\Rightarrow f = \pm 1, \pm 2$

$\Rightarrow I = \mathbb{Z}[X]$ or $2\mathbb{Z}[X]$ ※

Several familiar things from arithmetic in $\mathbb{Z}$ hold in a UFD

Def^n Let R be an integral domain.

$d \in R$ is the greatest common 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 $d' | a_i \ \forall i$ then $d' | d$.

$m \in R$ is the least common multiple of $a_1, \dots, a_n \in R$ (written $m = \mathrm{lcm}(a_1, \dots, a_n)$) if $a_i | m \ \forall i$, and if $a_i | m' \ \forall i$ then $m | m'$.

Both lcms and gcds (when they exist) are unique up to associates

Proposition 10.9 In a UFD both lcms & gcds exist

Proof Write $a_i = u_i \prod_j p_j^{n_{ij}}$ 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 $a_1, \dots, a_n$.

Certainly $d | a_i \ \forall i$.

If $d' | a_i \ \forall i$ then writing $d' = v \prod_j p_j^{t_j}$ we find that $t_j \leq n_{ij} \ \forall i$

$\Rightarrow t_j \leq m_j \quad \therefore d' | d$ (v must be a unit)

The argument for lcms is similar. □

§11 Factorisation in Polynomial Rings

We aim to prove

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

Remark Repeatedly applying this result shows that if R is a UFD then $R[X_1, \dots, X_n]$ is a UFD.

In particular the theorem shows $\mathbb{Z}[X]$ and $\mathbb{C}[X_1, \dots, X_n]$ are UFDs.

Throughout this section R is a UFD with field of fractions F.

We have $R[X] \leq F[X]$.

We already know $F[X]$ is a PID and therefore a UFD.

Def^n The **content** of $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ is $c(f) = \gcd(a_0, a_1, \dots, a_n)$. We say f is **primitive** if $c(f)$ is a unit, i.e. the a_i are coprime.

Lemma 11.2 (i) If $p \in R$ is irreducible then it is prime in $R[X]$

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

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

Lemma 11.2 (i) If $p \in R$ is irreducible then p is prime in $R[X]$

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

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

Proof (i) Since R a UFD, any irreducible is prime.

$\therefore$ $R/(p)$ is an integral domain

For $a \in R$, let $\tilde{a} \in R/(p)$ be its image under the quotient map.

We define a ring homomorphism

$$\theta : R[X] \to R/(p)[X]$$

$$a_n X^n + \cdots + a_1 X + a_0 \longrightarrow \tilde{a}_n X^n + \cdots + \tilde{a}_1 X + \tilde{a}_0$$

If $f, g \in R[X]$ with $p \mid fg$

$\Rightarrow \theta(fg) = 0$

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

$\Rightarrow \theta(f) = 0$ or $\theta(g) = 0$ ← since $R/(p)[X]$ is an integral domain (see Lemma 9.1)

$\Rightarrow p \mid f$ or $p \mid g$

(ii) If fg is not primitive then $\exists\ p \in R$ irreducible with $p \mid fg$

By (i) we have $p \mid f$ or $p \mid g$ ※ to f & g primitive

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

Then $fg = c(f)c(g)\underline{f_0 g_0}$

$\therefore$ $c(fg)$ and $c(f)c(g)$ ← primitive by (ii) are associates □

Remark If $f \in F[X]$ then we can write $f = \frac{a}{b} f_0$ where $a, b \in R$, $b \neq 0$ and $f_0 \in R[X]$ is primitive.

Indeed by clearing denominators may find $0 \neq b \in R$ s.t. $\underline{bf} \in R[X]$

$= a\ \underline{c(bf)} f_0$ with f_0 primitive

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

Proof Let $f \in R[X]$ be irreducible. Suppose for a contradiction f is <u>not</u> irreducible in $F[X]$ i.e. $f = gh$ where $g, h \in F[X]$ have positive degree.

By the remark $g = \frac{a}{b} g_0$, $h = \frac{c}{d} h_0$ for some $a, b, c, d \in R$ $b, d \neq 0$ and $g_0, h_0 \in R[X]$ primitive.

Then $bdf = ac \underbrace{g_0 h_0}_{\uparrow \text{primitive by Lemma 11.2}} \Rightarrow bd \mid ac$ say $ac = \lambda bd$ for some $\lambda \in R$.

Therefore $f = \lambda g_0 h_0$.

Since g_0, h_0 have positive degree, they are not units in $R[X]$.

This contradicts that f is irreducible in $R[X]$. □

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

Proof Write $f = gh$ with $h \in F[X]$.

By the remark $h = \frac{a}{b} h_0$, $a, b \in R$, $b \neq 0$, $h_0 \in R[X]$ primitive.

Then $bf = a g h_0$. Taking contents shows $b \mid a$, say $a = \lambda b$ for some $\lambda \in R$. ($g h_0$ primitive)

Then $bf = \lambda b g h_0 \Rightarrow g \mid f$ in $R[X]$. □

Corollary 11.4 Let $g \in R[X]$ be primitive.

g prime in $F[X] \Rightarrow g$ prime in $R[X]$

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

g prime in $F[X] \Rightarrow g \mid f_1$ or $g \mid f_2$ in $F[X]$

$\overset{\text{Lemma 11.3}}{\Rightarrow} g \mid f_1$ or $g \mid f_2$ in $R[X]$

$\therefore g$ 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 $\Rightarrow c(f)$ is a product of ireds. in R (which are also ired. in $R[X]$)

If f_0 is not irreducible, say $f_0 = gh$, then the factors have smaller degree (otherwise this would contradict primitivity), and again are primitive. So by induction on the degree, f_0 is a product of irreducibles.

It remains to show (see Lemma 10.5) that if $f \in R[X]$ is ireducible then it is prime.

Again write $f = c(f) f_0$ where $f_0 \in R[X]$ primitive.

f ired. $\Rightarrow$ f either constant or primitive

Case f constant

f ired. in $R[X] \Rightarrow f$ ired in R

$\overset{\text{Lemma 11.2}}{\Rightarrow}$ f is prime in $R[X]$

Case f primitive

f ired. in $R[X] \overset{\text{Gauss}}{\Rightarrow} f$ ired. in $F[X]$

$\overset{F[X] \text{ a UFD}}{\Rightarrow} f$ prime in $F[X]$

$\overset{\text{Cor 11.4}}{\Rightarrow} f$ prime in $R[X]$ □

Remark In view of Lemma 10.2, the last 3 "$\Rightarrow$" are "$\Leftrightarrow$".

Eisenstein's Criterion Let R be a UFD and $f \in R[X]$ a primitive polynomial. Write $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$.

Suppose $p \in R$ ired. with $p \nmid a_n$, $p \mid a_i$ $\forall\, 0 \le i \le n-1$, $p^2 \nmid a_0$.

Then f is ired. in $R[X]_K$, hence in $F[X]$ by Gauss' Lemma.

Proof Suppose $f = gh$ with $g, h \in R[X]$ not units.

f primitive $\Rightarrow$ g & h are non-constant

$g = r_k X^k + \cdots + r_1 X^1 + r_0 \qquad 0 < k < n$

$h = s_l X^l + \cdots + s_1 X^1 + s_0 \qquad 0 < l < n \qquad k + l = n$

Now $p \nmid a_n = r_k s_l \Rightarrow p \nmid r_k,\ p \nmid s_l$

& $p \mid a_0 = r_0 s_0 \Rightarrow p \mid r_0$; $p \mid s_0$ wlog $p \mid r_0$

Choose j s.t. $p \mid r_0, p \mid r_1, \ldots, p \mid r_{j-1}, p \nmid r_j$ (so $j \le k$).

$a_j = \underbrace{r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1}_{\text{divisible by } p} + r_j s_0$

a_j: div. by p, $j < n$

$\therefore p \mid s_0 \Rightarrow p^2 \mid r_0 s_0 = a_0$ ※

Example Consider $f(X) = X^3 + 2X + 5 \in \mathbb{Z}[X]$

If f is reducible (in $\mathbb{Z}[X]$) then

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

for some $a, b, c \in \mathbb{Z}$.

This is impossible, since $ac = 5$, yet $\pm 1, \pm 5$ are not roots of f.

By Gauss' Lemma, f is irred. in $\mathbb{Q}[X]$.

$\therefore \mathbb{Q}[X]/(f)$ is a field (see Lemma 10.3)

Example Let p be a prime number.

By Eisenstein's criterion $X^n - p$ is irred. in $\mathbb{Z}[X]$ hence in $\mathbb{Q}[X]$ by Gauss' Lemma.

Example Let $f(X) = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1 \in \mathbb{Z}[X]$ where p is a prime number.

Eisenstein does not apply to f but it does apply to

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

Indeed $p \mid \binom{p}{i}$ $\forall\, 1 \le i \le p-1$ and $p^2 \nmid \binom{p}{p-1} = p$.

$\therefore f(X+1)$ is irred in $\mathbb{Z}[X]$

$\Rightarrow f(X)$ is irred in $\mathbb{Z}[X]$ (if $f(X) = g(X)h(X)$ then $f(X+1) = g(X+1)h(X+1)$)

Again Gauss' Lemma shows f irred. in $\mathbb{Q}[X]$

§ 12 Algebraic Integers

Recall the ring of Gaussian integers is

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \le \mathbb{C}.$$

Norm $N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_{\ge 0}$

$$a + bi \longrightarrow a^2 + b^2$$

Note: $N(z_1 z_2) = N(z_1) N(z_2)$.

We saw $\mathbb{Z}[i]$ is an ED, hence a PID, hence a UFD.

$\therefore$ primes = irreducibles

The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ as these are the only elements of norm 1.

Lemma 12.1 If $\pi \in \mathbb{Z}[i]$ is prime, then $\exists!$ prime $p \in \mathbb{Z}$ with $\pi \mid p$.

Proof Write $N(\pi) = p_1 \cdots p_r$ where $p_i \in \mathbb{Z}$ is prime in $\mathbb{Z}$.

Since $N(\pi) = \pi\overline{\pi}$ we have $\pi \mid p_1 \cdots p_r \Rightarrow \pi \mid p_i$ for some i.

Uniqueness Suppose $\pi \mid p$ & $\pi \mid q$ where $p, q \in \mathbb{Z}$ are distinct primes in $\mathbb{Z}$.

Euclid $\Rightarrow \exists\, a, b \in \mathbb{Z}$ s.t. $ap + bq = 1$

Then $\pi \mid p$ & $\pi \mid q \Rightarrow \pi \mid 1 \Rightarrow \pi$ a unit ※ □

Now let $p = 2, 3, 5, 7, \ldots$ be a prime in $\mathbb{Z}$.

We seek to factor p into primes in $\mathbb{Z}[i]$

Case $p = 2$ $2 = (1+i)(1-i)$

So 2 is not prime in $\mathbb{Z}[i]$

Case $p \equiv 3 \pmod 4$ If $p = xy$ where $x, y \in \mathbb{Z}[i]$ are not units, then $p^2 = N(p) = N(x)\,N(y)$ & $N(x), N(y) > 1$.

$\therefore N(x) = N(y) = p$

Writing $x = a + ib$ we have $a^2 + b^2 = p \equiv 3 \pmod 4$.

This is impossible since the only squares mod 4 are 0 and 1.

$\therefore p$ is prime in $\mathbb{Z}[i]$

Case $p \equiv 1 \pmod 4$ By Theorem 9.3, $\mathbb{F}_p^*$ is cyclic of order $p-1$. Since $4 \mid p-1$, $\mathbb{F}_p^*$ contains an element of order 4, i.e.

$\exists\, x \in \mathbb{Z}$ s.t. $x^4 \equiv 1 \pmod p$, yet $x^2 \not\equiv 1 \pmod p$

$\therefore x^2 \equiv -1 \pmod p$

Then $p \mid (x^2+1) = (x+i)(x-i)$.

If p is prime in $\mathbb{Z}[i]$ then $p \mid x+i$ or $p \mid x-i$ ※

$\therefore p$ is <u>not</u> prime in $\mathbb{Z}[i]$

Theorem 12.2 (i) Every prime $p \in \mathbb{Z}$ with $p \equiv 1 \pmod 4$ may be written as $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

(ii) The primes in $\mathbb{Z}[i]$ are, up to associates

- $1+i$
- the primes $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$
- $a+bi$ & $a-bi$ where a, b as in (i)

Proof Let $\pi \in \mathbb{Z}[i]$ be prime. By Lemma 12.1 $\pi \mid p$ for some prime $p \in \mathbb{Z}$. If $p \equiv 3 \pmod 4$ then p is prime in $\mathbb{Z}[i]$, so π are & p are associates.

Otherwise, p is not prime in $\mathbb{Z}[i]$, say $p = xy$ where $x, y \in \mathbb{Z}[i]$ are not units.

$p^2 = N(p) = N(x)N(y)$ & $N(x), N(y) > 1$

$\Rightarrow N(x) = N(y) = p$

Writing $x = a+ib$, we have $p = N(x) = a^2+b^2 = (a+ib)(a-ib)$

($a+ib$, $a-ib$: irreducible since have norm p)

$\therefore \pi$ is an associate of $a+bi$ or $a-bi$

Case $p=2$ $1+i$ & $1-i$ are associates

Case $p \neq 2$ $a+bi$ & $a-bi$ are not associates. Indeed if $a+bi \mid a-bi$ then ~~$a+bi$~~ $a+bi \mid 2a$

$\Rightarrow p = N(a+bi) \nmid 4a^2$

$\Rightarrow p = 2$ or $p \mid a$ ※ $p = a^2+b^2$ □

Corollary 12.3 An integer $n \geq 1$ may be written as a^2+b^2 for some $a, b \in \mathbb{Z}$ $\Leftrightarrow$ every prime factor p of n with $p \equiv 3 \pmod 4$ divides n to an even power.

Proof n = sum of two squares

$\Leftrightarrow n = N(x)$ for some $x \in \mathbb{Z}[i]$

$\Leftrightarrow n$ is a product of norms of primes in $\mathbb{Z}[i]$

However, by Theorem 12.2, the norms of primes in $\mathbb{Z}[i]$ are the primes $p \in \mathbb{Z}$ with $p \not\equiv 3 \pmod 4$ and the squares of the primes

$p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$

<u>Example</u> Consider $65 = 5 \cdot 13$.

Factoring into primes in $\mathbb{Z}[i]$ have

$5 = (2+i)(2-i)$

$13 = (2+3i)(2-3i)$

$65 = (2+i)(2+3i)\,(2-i)(2-3i)$

Rewriting as $65 = (2+i)(2+3i)\ \overline{(2+i)(2+3i)}$

we see $65 = N[(2+i)(2+3i)] = N(1+8i) = 1^2 + 8^2$.

But 65 is also the norm of $(2+i)(2-3i) = 7-4i$

so $65 = 4^2 + 7^2$.

Notation Let $R \leq S$ be rings. Given $\alpha \in S$ we write $R[\alpha]$ for the smallest subring of S containing R and α. In other words

$$R[\alpha] = \mathrm{Im}(\phi : R[X] \to S)$$
$$f(X) \to f(\alpha)$$

If R and S are fields then we write $R(\alpha)$ for the smallest subfield of S containing R and α. In other words $R(\alpha)$ is the field of fractions of $R[\alpha]$.

Def^n (i) $\alpha \in \mathbb{C}$ is an algebraic number if $\exists$ non-zero polynomial f in $\mathbb{Q}[X]$ s.t. $f(\alpha) = 0$.

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

Let α be an algebraic number & let $\phi : \mathbb{Q}[X] \to \mathbb{C}$, $g(X) \to g(\alpha)$.

$\mathbb{Q}[X]$ is a PID $\Rightarrow \mathrm{Ker}(\phi) = (f)$ for some $f \in \mathbb{Q}[X]$

α algebraic number $\Rightarrow f \neq 0$

Multiplying by a unit we may assume f is monic. We say that f is the minimal polynomial of α.

By the isomorphism thm

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

$\mathbb{Q}[\alpha]$ is an integral domain $\Rightarrow f$ is irreducible

$\Rightarrow (f)$ is maximal (Lemma 10.3)

$\Rightarrow \mathbb{Q}[\alpha]$ is a field

It is therefore usual to write $\mathbb{Q}[\alpha]$ as $\mathbb{Q}(\alpha)$

Lemma Let $\alpha \in \mathbb{C}$ be an algebraic number with minimal polynomial f. Write $f = \lambda f_0$ with $\lambda \in \mathbb{Q}^*$ and $f_0 \in \mathbb{Z}[X]$ primitive. Then the ring homomorphism $\phi : \mathbb{Z}[X] \to \mathbb{C}$, $g(X) \to g(\alpha)$ has $\mathrm{Ker}(\phi) = (f_0) \lhd \mathbb{Z}[X]$.

Proof Clearly $\phi(f_0) = f_0(\alpha) = 0$ so $(f_0) \subseteq \ker(\phi)$. Suppose $g \in \ker(\phi)$. Then $f \mid g$ in $\mathbb{Q}[X] \Rightarrow f_0 \mid g$ in $\mathbb{Q}[X]$

$\overset{\text{Lemma 11.3}}{\Rightarrow}$ $f_0 \mid g$ in $\mathbb{Z}[X]$

$\Rightarrow$ $g \in (f_0) \lhd \mathbb{Z}[X]$ □

Continuing with the notation of the last Lemma, suppose α is an algebraic integer. Then f_0 divides a monic polynomial, so $\pm f_0$ is monic. But f was monic (by defⁿ of min. poly) so $f = \pm f_0 \in \mathbb{Z}[X]$.

This has two nice consequences

(i) Applying the isomorphism thm to ϕ

$$\frac{\mathbb{Z}[X]}{(f)} \cong \mathbb{Z}(\alpha) \leq \mathbb{C}$$

Examples $i, \sqrt{2}, \frac{-1+\sqrt{-3}}{2}, \sqrt[n]{p}$ have min. polys

$X^2+1,\ X^2-2,\ X^{\$2}+X+1,\ X^n-p$

$\therefore\ \mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[i]$, etc.

(ii) We have proved the non-trivial implication in Lemma 12.5

α an algebraic integer $\Leftrightarrow$ its min. poly. has integer coeffs.

Corollary 12.6 If α is an algebraic integer and $\alpha \in \mathbb{Q}$ then $\alpha \in \mathbb{Z}$

Proof α alg integer $\Rightarrow$ min. poly has coeffs in $\mathbb{Z}$

$\alpha \in \mathbb{Q} \Rightarrow$ min. poly is $X - \alpha$

$\Rightarrow \alpha \in \mathbb{Z}$ □

§13 Noetherian Rings

We showed that a PID R satisfies the ascending chain condition (ACC):

if $I_1 \subseteq I_2 \subseteq \cdots$ 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 A ring R satisfies ACC
$\Leftrightarrow$ all ideals $I \trianglelefteq R$ are finitely generated

Proof "$\Leftarrow$" Let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals, and $I = \bigcup_{n=1}^{\infty} I_n$, which is again an ideal.

By assumption $I = (a_1, \ldots, a_m)$ for some $a_1, \ldots, a_m \in R$.
These elements lie in a nested union so $\exists\, N \in \mathbb{N}$ s.t.
$a_1, \ldots, a_m \in I_N$
Then for $n \geq N$ we have
$(a_1, \ldots, a_m) \subseteq I_N \subseteq I_n \subseteq I = (a_1, \ldots, a_m)$
so $I_n = I_N$.

"$\Rightarrow$" Suppose R satisfies ACC and let $J \trianglelefteq R$ be an ideal.

Choose $a_1 \in J$. If $J \neq (a_1)$ then choose $a_2 \in J \setminus (a_1)$. If $J \neq (a_1, a_2)$ choose $a_3 \in J \setminus (a_1, a_2)$ and so on.

If this process never stops, we obtain a chain
$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots$
$\lightning$ to ACC. Thus $J = (a_1, \ldots, a_m)$ for some m. $\square$

Def^n A ring satisfying ACC is **Noetherian**.

Hilbert Basis Theorem If R is Noetherian then so is $R[X]$

Proof Let $J \trianglelefteq R[X]$ be an ideal.

Pick $f_1 \in J$ a polynomial of minimal degree. If $J \neq (f_1)$ then pick $f_2 \in J \setminus (f_1)$ of minimal degree. If $J \neq (f_1, f_2)$ then pick $f_3 \in J \setminus (f_1, f_2)$ of minimal degree and so on.

If at any point $J = (f_1, \dots, f_m)$ we are done, so suppose not.

By construction

$$(f_1) \subsetneq (f_1, f_2) \subsetneq (f_1, f_2, f_3) \subsetneq \cdots$$

and $\deg f_1 \leq \deg f_2 \leq \deg f_3 \leq \cdots$

Let a_i = leading coeff. of f_i & consider the ideals in R

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

As R is Noetherian, these stabilise so $\exists\, m \in \mathbb{N}$ s.t.

$a_{m+1} \in (a_1, \dots, a_m)$.

Write $a_{m+1} = \sum_{i=1}^{m} \lambda_i a_i \qquad \lambda_i \in R$

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

Hilbert's Basis Theorem If R is Noetherian then so is $R[X]$

Proof (continued) We supposed $J \lhd R[X]$ is not finitely generated, and chose $f_1, f_2, \ldots \in J$ with

$$(f_1) \subsetneq (f_1, f_2) \subsetneq \cdots \qquad (*)$$

We showed $\exists\ m \geq 1$ and $g \in (f_1, f_2, \ldots, f_m)$ such that g and f_{m+1} have the same degree and leading coefficient.

Hence $\deg(f_{m+1} - g) < \deg(f_{m+1})$.

But $f_{m+1} - g \in J$, so by the fact we chose f_{m+1} of minimal degree, we see

$$f_{m+1} - g \in (f_1, \ldots, f_m)$$
$$\Rightarrow f_{m+1} \in (f_1, \ldots, f_m) \quad \lightning \text{ to } (*)$$

$\therefore J$ is finitely generated $\square$

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

Example Let $R = \mathbb{C}[X_1, \ldots, X_n]$.

Let $V \subseteq \mathbb{C}^n$ be a subset defined by the vanishing of a possibly infinite set of polynomials $\mathcal{F} \subseteq R$.

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

Then $I \lhd R$, and R is Noetherian

$\Rightarrow I$ is finitely generated

$\therefore V$ may be defined by the vanishing of finitely many polynomials

Lemma 13.2 Any quotient of a Noetherian ring is Noetherian

Proof Let R be Noetherian, $I \lhd R$

and $J_1' \subseteq J_2' \subseteq \cdots$ a chain of ideals in R/I.

By the ideal correspondence, we have $J_i' = J_i/I$ with

$J_1 \subseteq J_2 \subseteq \cdots$ ideals in R containing I.

R Noetherian $\Rightarrow \exists\ N \in \mathbb{N}$ s.t. $\forall n \geq N$, $J_n = J_{n+1}$

$\Rightarrow \forall n \geq N$, $J_n' = J_{n+1}'$ $\square$

Examples (i) $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$ is Noetherian

(ii) $R[x]$ Noetherian $\Rightarrow$ $R[x]/(x) \cong R$ 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

$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$

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

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

↑ since $2 \in R$ is not a unit

(iii) $R = \{$infinitely diff'ble functions $[-1,1] \to \mathbb{R}\}$ with pointwise operations (proof omitted)

§ 14 Modules – definition & examples

Def^ A module over a ring R is a triple $(M, +, \cdot)$ consisting of a set M and two operations $+ : M \times M \to M$ and $\cdot : R \times M \to M$ satisfying

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

(ii) The operation $\cdot$ satisfies

$(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m \quad \forall\, r_1, r_2 \in R,\ m \in M$

$r_1 \cdot (m_1 + m_2) = r_1 \cdot m_1 + r_1 \cdot m_2 \quad \forall\, r_1 \in R,\ m_1, m_2 \in M$

$r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m \quad \forall\, r_1, r_2 \in R,\ m \in M$

$1_R \cdot m = m \quad \forall\, m \in M$

Remark As ever, as part of checking $+$ and $\cdot$ are well-defined, we must check closure.

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

(ii) For any ring R, $R^n = R \times \cdots \times R$ 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.

(iii) If $I \lhd R$, then I is an R-module with $\cdot : R \times I \to I$ the restriction of multiplication on R,

and R/I is an R-module with $r \cdot (r_1 + I) = rr_1 + I$.

(iv) For $R = \mathbb{Z}$, a $\mathbb{Z}$-module is precisely the same as an abelian group, where $\mathbb{Z} \times A \to A$

$$(n, a) \to \underbrace{a + \cdots + a}_{n \text{ times}}$$

(v) Let F be a field, V a vector space over F, and $\alpha : V \to V$ a linear map.

We make V a $F[X]$-module via

$F[X] \times V \longrightarrow V$

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

Different choices of α make V into different $F[X]$ modules.

(vi) If $\phi : R \to S$ is a ring homomorphism then an S-module M may be regarded as an R-module via

$R \times M \longrightarrow M$

$(r, m) \longrightarrow \phi(r) \cdot m$

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

Def^n Let M be an R-module.

A subset $N \subseteq M$ is an R-submodule (written $N \leq M$) if it is a subgroup of $(M, +)$ and $r \cdot n \in N \quad \forall r \in R, n \in N$

Examples (i) A subset of an F-vector space is an F-submodule precisely when it is a vector subspace.

(ii) A subset of R is an R-submodule precisely when it is an ideal

Def^n If $N \leq M$ is an R-submodule
the quotient module M/N is the quotient of groups under $+$
with $r \cdot (m+N) = r \cdot m + N$.
This operation is well-defined & makes M/N an R-module.

Def^n Let M and N be R-modules.

A function $f: M \to N$ is a R-module homomorphism if it is a homomorphism of additive groups, and

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

Example If F is a field then a F-module (= vector space) homomorphism is a linear map

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

$\mathrm{Ker}(f) = \{ m \in M : f(m) = 0_N \} \leq M$

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

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

Proof Similar to before.

Second Isomorphism Theorem Let $A, B \leq M$ be R-submodules.

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

$A \cap B \leq M$

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

To motivate the Third Isomorphism Thm, we note the correspondence

$$\left\{ \begin{matrix} \text{submodules} \\ \text{of } M/N \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{submodules of} \\ M \text{ containing } N \end{matrix} \right\}$$

Third Isomorphism Thm If $N \leq L \leq M$ are R-modules, then

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

In particular, these results apply to vector spaces, so you should compare them to results from linear algebra.

Let M be an R-module. If $m \in M$ then we write Rm for $\{ rm : r \in R \}$, the submodule generated by m.

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

Def^n M is cyclic if $\exists\, m \in M$ such that $M = Rm$

M is finitely generated if $\exists\, m_1, \ldots, m_n \in M$ such that

$M = Rm_1 + \cdots + Rm_n$.

Lemma 14.1 M is cyclic $\Leftrightarrow$ $M \cong R/I$ for some $I \lhd R$

Proof "$\Rightarrow$" Suppose $M = Rm$. There is a surjective R-module homomorphism from R to M sending r to rm.

Its kernel is an R-submodule of R i.e. an ideal $I \lhd R$ annihilator

By the isomorphism theorem, $R/I \cong M$.

"$\Leftarrow$" R/I is generated by $1_R + I$ □

Lemma 14.2 M is finitely generated if and only if

$\exists$ a surjective R-module homomorphism $f : R^n \to M$ for some n.

Proof "$\Rightarrow$" If $M = Rm_1 + \cdots + Rm_n$ then we define

$$f : R^n \longrightarrow M$$
$$(r_1, \ldots, r_n) \longrightarrow \sum_{i=1}^{n} r_i m_i$$

This is a surjective R-module homomorphism.

"$\Leftarrow$" Let $e_i = (0, \ldots, 0, \overset{i^{th}}{1}, 0, \ldots, 0) \in R^n$

Given f, let $m_i = f(e_i)$. Then any $m \in M$ is of the form

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

$\therefore M = Rm_1 + \cdots + Rm_n$. □

Corollary 14.3 Let $N \leq M$ be a R-submodule.

If M is finitely generated then so is M/N.

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

$$R^n \xrightarrow{f} M \longrightarrow M/N \quad \text{is also a surjective } R\text{-module hom so}$$
$$m \longrightarrow m + N$$

M/N is finitely generated. □

Remark A submodule of a f.g. module need not be f.g. Indeed take R a non-Noetherian ring and $I \lhd R$ an ideal which is not finitely generated.

Then R is a finitely generated R-module (generated by 1_R) & I is a submodule which is not f.g.

Lemma 14.4 Let R be an integral domain. Every submodule of a cyclic R-module is cyclic iff R is a PID.

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

"$\Leftarrow$" If M is a cyclic R-module then $M \cong R/I$ by Lemma 14.1. Any submodule takes the form J/I where $I \subseteq J \lhd R$.

R is a PID $\Rightarrow$ J is principal $\Rightarrow$ J/I is cyclic $\square$

Theorem 14.5 Let R be a PID and M an R-module generated by n-elements. Then any submodule $N \leq M$ is generated by $\leq n$ elements.

Proof Lemma 14.4 was the case $n=1$

Suppose $M = Rx_1 + \cdots + Rx_n$.

Let $M_i = Rx_1 + \cdots + Rx_i$.

Then $0 = M_0 \leq M_1 \leq \cdots \leq M_n = M$.

& $0 = M_0 \cap N \leq M_1 \cap N \leq \cdots \leq M_n \cap N = N$.

The R-module ~~map~~ hom $M_i \cap N \longrightarrow M_i/M_{i-1}$ has kernel $M_{i-1} \cap N$.

Iso. thm $\Rightarrow$ $\dfrac{M_i \cap N}{M_{i-1} \cap N} \cong$ a submodule of $\dfrac{M_i}{M_{i-1}}$

$\dfrac{M_i}{M_{i-1}}$: cyclic, generated by $x_i + M_{i-1}$

$\dfrac{M_i \cap N}{M_{i-1} \cap N}$: cyclic by Lemma 14.4 generated by $y_i + (M_{i-1} \cap N)$

Then $M_i \cap N = (M_{i-1} \cap N) + Ry_i$

It follows by induction on i that $M_i \cap N = Ry_1 + \cdots + Ry_i$.

Taking $i=n$ gives $N = M_n \cap N = Ry_1 + \cdots + Ry_n$. $\square$

Remark This applies when $R = \mathbb{Z}$. We've shown any subgroup of $(\mathbb{Z}^n, +)$ can be generated by $\leq n$ elements.

§15 Direct Sums & Free Modules

Def^n If $M_1, \dots, M_n$ are R-modules then the direct sum $M_1 \oplus \cdots \oplus M_n$ is the set $M_1 \times \cdots \times M_n$ with operations

$(m_1, \dots, m_n) + (m_1', \dots, m_n') = (m_1 + m_1', \dots, m_n + m_n')$ &

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

Examples (i) $R^n = \underbrace{R \oplus \cdots \oplus R}_{n \text{ copies}}$

(ii) If $M_1, M_2 \leq M$ the R-module homomorphism $M_1 \oplus M_2 \longrightarrow M$ taking (m_1, m_2) to $m_1 + m_2$ is an isomorphism iff

$M_1 \cap M_2 = \{0\}$ and $M_1 + M_2 = M$. (iso Thm)

(iii) Suppose $M = \hat{\bigoplus_{i=1}} M_i$ and $N_i \leq M_i$.

The R-module homomorphism

$$M \longrightarrow \hat{\bigoplus_{i=1}} M_i/N_i$$

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

is surjective with kernel $\hat{\bigoplus_{i=1}} N_i = N$ (say).

$\therefore M/N \cong \hat{\bigoplus_{i=1}} M_i/N_i$

e.g. taking $R = \mathbb{Z}$ we have

$$\frac{\mathbb{Z} \oplus \mathbb{Z}}{m\mathbb{Z} \oplus n\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}$$

Def^n Let $m_1, \dots, m_n \in M$. Then the set $\{m_1, \dots, m_n\}$ is *independent* if $\hat{\sum_{i=1}} r_i m_i = 0 \Rightarrow r_1 = \cdots = r_n = 0$.

Def^n A subset $S \subset M$ *generates M freely* if

(i) S generates M

(ii) any *function* $\psi : S \longrightarrow N$ where N is a R-module extends to an R-module *homomorphism* $\theta : M \longrightarrow N$

N.B. Such an extension is unique by (i)

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

Proposition 15.1 For a subset $S = \{m_1, \dots, m_n\} \subset R$ the following are equivalent.

(i) S generates M freely

(ii) S generates M and S is independent

(iii) every element of M is uniquely expressible as $r_1 m_1 + \cdots + r_n m_n$ for some $r_1, \dots, r_n \in R$

(iv) the R-module homomorphism $R^n \longrightarrow M$

$$(r_1, \dots, r_n) \longrightarrow \sum_{i=1}^{n} r_i m_i$$

is an isomorphism

Proof (i) $\Rightarrow$ (ii) Let S generate M freely.

If S is not independent, then $\exists\, r_1, \dots, r_n \in R$ s.t. $\sum_{i=1}^{n} r_i m_i = 0$ and some $r_j \neq 0$.

Define $\psi : S \longrightarrow R$

$$m_i \longrightarrow \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

This extends to an R-module homomorphism $\theta : M \longrightarrow R$.

Then $\theta\left(\sum_{i=1}^{n} r_i m_i\right) = \sum_{i=1}^{n} r_i\, \theta(m_i) = r_j$.

But $\theta(0) = 0$, so $r_j = 0$. ※

So S is independent.

The other implications (e.g. (ii) $\underset{\text{EZ}}{\Rightarrow}$ (iii) $\underset{\text{EZ}}{\Rightarrow}$ (i) & (iii) $\underset{\text{iso}}{\Leftrightarrow}$ (iv)) are left as an exercise. □

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

Example The subset $\{2, 3\}$ generates the $\mathbb{Z}$-module $\mathbb{Z}$, but these elements are not independent as $(3)\cdot 2 + (-2)\cdot 3 = 0$.

Furthermore, no subset of $\{2, 3\}$ gives a basis.

$\{2\}$ and $\{3\}$ are independent but do not generate.

Proposition 15.2 (Invariance of dimension)

- Let R be a non-zero ring.
  If $R^m \cong R^n$ as R-modules then $m = n$.

Proof We first introduce a general construction.
Let $I \lhd R$ and M be an R-module.
Let $IM = \{ \sum a_i m_i : a_i \in I, m_i \in M \} \leq M$
Then the quotient M/IM is an R/I module via
$(r + I) \cdot (m + IM) = rm + IM$
We now return to the case at hand and suppose $R^n \cong R^m$.

- Choose $I \lhd R$ a maximal ideal. (not hard to see this exists if R is Noetherian, but in fact exists in general using Sheet 2, Question 4 + Zorn's Lemma).

By the above we get an isomorphism of R/I modules

$$\begin{array}{ccc} R^m/I(R^m) & \cong & R^n/I(R^n) \\ \| & & \| \\ (R/I)^m & & (R/I)^n \end{array}$$

But $I \lhd R$ maximal $\Rightarrow$ R/I is a field.

- So $m = n$ by invariance of dimension for vector spaces. □

Remark Let A and B be $n \times n$ matrices over a ring R. We have $\det(AB) = \det(A)\det(B)$

$$\operatorname{adj}(A) \cdot A = A \cdot \operatorname{adj}(A) = (\det A) I_n.$$

In particular A is invertible (i.e. $\exists$ B with entries in R s.t. $AB = BA = I_n$) iff $\det A$ is a unit.

Cayley Hamilton Theorem Let $A = (a_{ij})$ be an $n \times n$ matrix over a field F.

- Let $\chi_A(X) = \det(XI_n - A) \in F[X]$.
  Then $\chi_A(A) = 0$.

Proof Let $V = F^n$ be the $F[X]$ module with X acting as A, i.e. $f(X) \cdot v = f(A)(v)$.

Let $e_1, \dots, e_n$ be the standard basis of F^n.

$$X \cdot e_j = \sum_{i=1}^{n} a_{ij} e_i \quad \forall \ 1 \le j \le n$$

$$\Rightarrow \sum_{i=1}^{n} (\delta_{ij} X - a_{ij}) \cdot e_i = 0 \quad \forall \ 1 \le j \le n$$

matrix with poly coeffs

$$\Rightarrow (X I_n - A) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0$$

Multiply on left by adj $(X I_n - A)$

$$\Rightarrow \det(X I_n - A) \cdot e_i = 0 \quad \forall \ 1 \le i \le n$$

$$\Rightarrow \chi_A(X) \cdot e_i = 0 \quad "$$

$$\Rightarrow \chi_A(A)\, e_i = 0 \quad "$$

$$\Rightarrow \chi_A(A) = 0$$

□

§ 16 The Structure Theorem & Applications

In this section, R is a Euclidean domain with Euclidean function $\phi : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$.

Let A be an $m \times n$ matrix with entries in R.

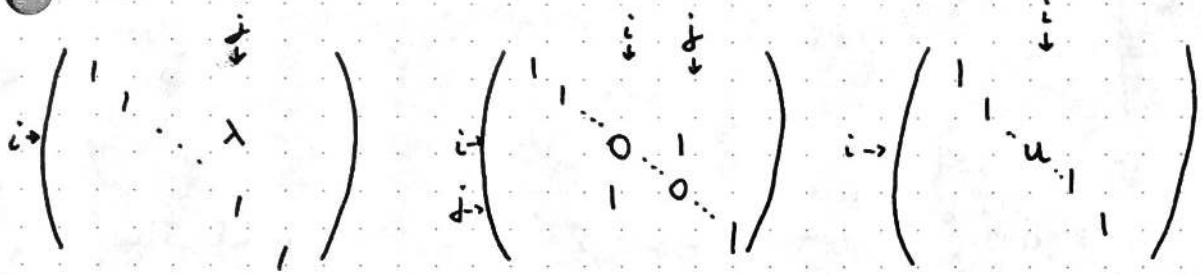
Def^n The elementary row operations are as follows

(i) Add λ times the j^{th} row to the i^{th} row ($\lambda \in R$, $i \neq j$)

(ii) Swap the i^{th} and j^{th} rows

(iii) Multiply the i^{th} row by a unit $u \in R^\times$

Each of these operations may be realised by multiplying on the left by a $m \times m$ invertible matrix.



In particular, these operations are reversible.

Similarly, find column operations, which may be realised by multiplying on the right by a $n \times n$ invertible matrix.

Def^n Two $m \times n$ matrices A and B are equivalent if there is a sequence of row and column operations taking A to B.

If they are equivalent, then there exist invertible matrices P, Q such that $B = QAP$.

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

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

where each $d_i \neq 0$ and $d_1 \mid d_2 \mid \cdots \mid d_t$.

The d_i are called invariant factors.

We will show they are unique up to associates,

Proof If the matrix is zero we are done. Otherwise, by swapping rows and columns, we may assume $a_{11} \neq 0$.

We will try to make $\phi(a_{11})$ as small as possible.

Case 1 If $a_{11} \nmid a_{1j}$ for some $j \geq 2$ then write

$$a_{1j} = q a_{11} + r \quad \text{with} \quad \phi(r) < \phi(a_{11}).$$

Subtracting q times the first column from the j^{th} column, and then swapping these columns leaves r in position $(1,1)$.

Case 2 If $a_{11} \nmid a_{i1}$ for some $i \geq 2$, then we likewise perform row operations.

Cases 1 and 2 each decrease $\phi(a_{11})$, and so may be repeated only finitely many times, until $a_{11} \mid a_{1j}\ \forall\ j \geq 2$, $a_{11} \mid a_{i1}\ \forall\ i \geq 2$.

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

$$A = \left(\begin{array}{c|c} a_{11} & 0 \cdots 0 \\ \hline 0 \\ \vdots & A' \\ 0 \end{array}\right)$$

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

Case 3 If $a_{11} \nmid a_{ij}$ for some $i, j \geq 2$ then we add the i^{th} row to the first row, and then perform column operations as in Case 1 to decrease $\phi(a_{11})$. We then restart the algorithm.

After finitely many iterations we have

$$A = \left(\begin{array}{c|c} a_{11} & 0 \cdots 0 \\ \hline 0 \\ \vdots & A' \\ 0 \end{array}\right)$$

with a_{11} $(= d_1$ say$)$ dividing every entry of A'.

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

To study the uniqueness of the invariant factors, we will consider the minors of A.

Def^n A $k \times k$ minor of the matrix A is the determinant of a $k \times k$ submatrix of A (i.e. a matrix formed by removing all but k rows and all but k columns).

Def^n For a matrix A over R the k^{th} Fitting ideal $Fit_k(A) \lhd R$ is the ideal generated by all the $k \times k$ minors of A.

Lemma 16.2 If A and B are equivalent matrices then $Fit_k(A) = Fit_k(B) \quad \forall\, k$.

Proof We show that the row operations (i) – (iii) don't change $Fit_k(A)$. Of course the same proof works for column operations.

(i) Suppose $i=1, j=2$, i.e. we add λ times the second row to the first row, so that A becomes

$$\begin{pmatrix} a_{11}+\lambda a_{21} & a_{12}+\lambda a_{22} & \cdots & a_{1n}+\lambda a_{2n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = A'$$

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

- If we did not choose the first row then $C = C'$ & so $\det C = \det C'$
- If we chose both the first and second rows then C and C' differ by a row operation & so $\det C = \det C'$
- If we chose the first row, but not the second then by expanding along the first row

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

where D is another $k \times k$ minor of A.

$\therefore \det(C') \in Fit_k(A)$

In conclusion $Fit_k(A') \subset Fit_k(A)$.

Since row operations are reversible we get $Fit_k(A) \subset Fit_k(A')$ & hence equality.

(ii) & (iii) These cases are similar, but easier. □

Now if A has SNF $\begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_t \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$

where $d_1 | \cdots | d_t$,

then $\mathrm{Fit}_k(A) = (d_1 d_2 \cdots d_k)$.

This shows that the products $d_1 d_2 \cdots d_k$ (up to associates) are uniquely determined by A.

Dividing out shows each d_i (up to associates) is uniquely determined by A.

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

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \xrightarrow{C_1 \leftrightarrows C_2} \begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix} \xrightarrow{C_2 \mp C_1} \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix}$$

$$\xrightarrow{R_2 \mp R_1} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

But also $(d_1) = (1) \Rightarrow d_1 = \pm 1$

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

Theorem 16.3 Let R be a Euclidean domain and $N \leq R^m$. Then there is a basis $x_1, \dots, x_m$ of R^m such that N is generated by $d_1 x_1, d_2 x_2, \dots, d_t x_t$ for some $t \leq m$ and all $d_i \neq 0$, & $d_1 \mid d_2 \mid \cdots \mid d_t$.

Proof By Theorem 14.5 (& ED $\Rightarrow$ PID) we have $N = Ry_1 + \cdots + Ry_n$ for some $n \leq m$.

Each y_i belongs to R^m, so we may form an $m \times n$ matrix

$$A = \left(y_1 \middle| y_2 \middle| \cdots \middle| y_n \right).$$

By Theorem 16.1, A is equivalent to

$$A' = \left(\begin{array}{c|c} d_1 & \cdots \\ & d_t \\ \hline 0 & 0 \end{array} \right) \quad \text{with } d_1 \mid d_2 \mid \cdots \mid d_t.$$

A' is obtained from A by elementary row and column operations.

Each row operation corresponds to changing our basis for R^m.

Each column operation corresponds to changing our set of generators for N.

After changing our basis for R^m to $x_1, \dots, x_m$ (say) the submodule N is generated by $d_1 x_1, d_2 x_2, \dots, d_t x_t$ as claimed. □

Structure Theorem Let R be a ED and M a finitely generated R-module. Then

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

for some $d_i \neq 0$ with $d_1 \mid d_2 \mid \cdots \mid d_t$.

Proof Since M is finitely generated, there exists a surjective R-module homomorphism $\phi: R^m \longrightarrow M$ for some m (see Lemma 14.2).

By the first isomorphism thm $M \cong R^m / \ker(\phi)$.

By theorem 16.3, $\exists$ basis $x_1, \dots, x_m$ for R^m s.t. $\ker(\phi)$ is generated by $d_1 x_1, \dots, d_t x_t$ with $d_1 \mid d_2 \mid \cdots \mid d_t$.

Then $$M \cong \frac{R \oplus \cdots \oplus R \oplus \cdots \oplus R}{d_1 R \oplus \cdots \oplus d_t R \oplus \cdots \oplus 0}$$

$$\cong \frac{R}{(d_1)} \oplus \frac{R}{(d_2)} \oplus \cdots \oplus \frac{R}{(d_t)} \oplus \underbrace{R \oplus \cdots \oplus R}_{m-t \text{ copies.}}$$

Ü □

Corollary 16.4 As ever, let R be a ED. Then any finitely generated torsion-free R-module is free.

(torsion-free: $rm = 0 \Rightarrow r = 0$ or $m = 0$)

Proof M torsion free $\Rightarrow$ no submodule of form $\frac{R}{(d)}$ with $d \neq 0$.

$\therefore M \cong R^k$ for some k. □

Remark The structure theorem in fact holds for R a PID.

There is also a uniqueness statement: after deleting any d_i which are units the d_i (up to associates) are uniquely determined by M.

Reference Hartley & Hawkes, "Rings, Modules & Linear Algebra"

Example Let $R = \mathbb{Z}$ (as R is a ED).

Consider the abelian group G generated by a, b, c subject to the relations

$$\begin{aligned} 2a + 3b + c &= 0 \\ a + 2b &= 0 \\ 5a + 6b + 7c &= 0 \end{aligned}$$

Then $G \cong \mathbb{Z}^3 / N$ where $N \leq \mathbb{Z}^3$ generated by $(2,3,1), (1,2,0), (5,6,7)$.

$$A = \begin{pmatrix} 2 & 1 & 5 \\ 3 & 2 & 6 \\ 1 & 0 & 7 \end{pmatrix} \text{ has SNF } \begin{pmatrix} 1 & & \\ & 1 & \\ & & 3 \end{pmatrix}$$

Check The matrix contains a 1

$\therefore (d_1) = (\text{entries of } A) = (1)$

One of the 2×2 minors is $\begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} = 1$

$\therefore (d_1 d_2) = (\text{2×2 minors of } A) = (1)$

$\det A = \begin{vmatrix} 1 & 5 \\ 2 & 6 \end{vmatrix} + 7 \begin{vmatrix} 2 & 1 \\ 3 & 2 \end{vmatrix} = -4 + 7 = 3$

$\therefore (d_1 d_2 d_3) = (3)$

$\therefore d_1 = d_2 = 1, \ d_3 = 3$

We therefore change basis for $\mathbb{Z}^3$ so that N is generated by $(1,0,0), (0,1,0), (0,0,3)$.

$$G \cong \frac{\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}}{\mathbb{Z} \oplus \mathbb{Z} \oplus 3\mathbb{Z}} \cong \mathbb{Z}/3\mathbb{Z}$$

More generally we have

Structure Theorem for finitely generated abelian groups

Any finitely generated abelian group G is isomorphic to

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z} \times \mathbb{Z}^r$$

where $d_i \neq 0$, $d_1 \mid d_2 \mid \cdots \mid d_t$, $r \geq 0$.

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

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

Corollary Let A be an $m \times m$ matrix over $\mathbb{Z}$ with $\det A \neq 0$. Let $N \leq \mathbb{Z}^m$ be the subgroup generated by the columns of A. Then $\mathbb{Z}^m/N$ is finite of order $|\det A|$.

Proof A is equivalent to a matrix in SNF

$$A' = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_m \end{pmatrix} \qquad d_i \geq 0.$$

Then $d_1 \cdots d_m = \det A' = \pm \det A \neq 0$.

$$\therefore \frac{\mathbb{Z}^m}{N} \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_m\mathbb{Z}} \quad \text{has order } d_1 \cdots d_m = |\det A|.$$

□

We saw in §6 we can write any finite abelian group as a product of cyclic groups of prime power order.

To generalise this, we need

Lemma 16.5 Let R be a PID and $a, b \in R$ with $\gcd(a,b)$ being 1. Then there is an isomorphism of R-modules

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

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

Proof R a PID $\Rightarrow (a,b) = (d)$ for some $d \in R$

By assumption d is a unit.

So $\exists r, s \in R$ s.t. $\boxed{ra + sb = 1}$.

We define an R-module homomorphism

$$\begin{aligned} R &\xrightarrow{\phi} R/(a) \oplus R/(b) \\ x &\longmapsto (x+(a),\ x+(b)) \end{aligned}$$

Then $\phi(sb) = (1+(a),\ 0+(b))$,

$\phi(ra) = (0+(a),\ 1+(b))$.

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

Therefore ϕ is surjective.

Clearly $(ab) \subset \ker(\phi)$.

Conversely if $x \in \ker(\phi)$ then $x \in (a) \cap (b)$

and $x = x(ra + sb) = r(ax) + s(xb) \in (ab)$.

$\therefore \ker(\phi) = (ab)$

Isomorphism thm $\Rightarrow \dfrac{R}{(ab)} \cong \dfrac{R}{(a)} \oplus \dfrac{R}{(b)}$. □

Primary decomposition theorem Let R be a ED and M a finitely generated R-module. Then

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

where $p_1, \ldots, p_k \in R$ are primes (not necessarily distinct).

Proof By the structure theorem

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

So it suffices to write each $R/(d_i)$ in the required form.

But $d_i = u p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where u is a unit & $p_1, \ldots, p_r$ are distict primes.

↑ i.e. not associates

Lemma 16.5 $\Rightarrow \frac{R}{(d_1)} \cong \frac{R}{(p_1^{\alpha_1})} \oplus \cdots \oplus \frac{R}{(p_1)^{\alpha_r}}$ □

Recall: If V is a vector space over F a field and $\alpha: V \to V$ is an endomorphism, we consider V as an $F[X]$-module via

$$F[X] \times V \longrightarrow V$$
$$(f(x), v) \longmapsto f(\alpha)(v)$$

We write V_α for this $F[X]$-module.

Lemma 16.6 If V is a finite dim F-vector space then V_α is finitely generated as an $F[X]$-module.

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

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

$$\begin{pmatrix} 0 & & & \\ 1 & 0 & & 0 \\ & 1 & \ddots & \\ 0 & & \ddots & 0 \\ & & & 1 \end{pmatrix} \quad (*)$$

since α acts as "multiplication by X".

(ii) Suppose $V_\alpha \cong \frac{F[X]}{((X-\lambda)^n)}$ as $F[X]$-modules.

Then wrt the basis $1, X-\lambda, \ldots, (X-\lambda)^{n-1}$

$\alpha - \lambda$ id has matrix $(*)$

$$\therefore \alpha \text{ has matrix } \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & 0 \\ & 1 & \ddots & \\ 0 & & \ddots & \lambda \\ & & & 1 \end{pmatrix}$$

(iii) Suppose $V_\alpha \cong \frac{F[X]}{(f)}$ where $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$

Then wrt the basis $1, X, X^2, \ldots, X^{n-1}$ α has matrix

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

This is called the <u>companion matrix</u> $C(f)$ of the monic polynomial f.

<u>Theorem 16.7</u> (Rational Canonical Form) Let α be an endomorphism of a finite dimensional F-vector space V.

Regard V ($= V_\alpha$ say) as an $F[X]$-module with X acting as α.

We have $$V_\alpha \cong \frac{F[X]}{(f_1)} \oplus \cdots \oplus \frac{F[X]}{(f_t)}$$

where $f_1 | \cdots | f_t$ with each f_i monic.

Then there is a basis for V s.t. wrt this basis α has matrix

$$\begin{pmatrix} C(f_1) & & & 0 \\ & C(f_2) & & \\ & & \ddots & \\ 0 & & & C(f_t) \end{pmatrix} \quad -(*)(*)$$

<u>Proof</u> $F[X]$ is a ED, so we may apply the structive theorem.

Since V_α is finite dimensional as an F-vector space, it is finitely generated over $F[X]$ (see Lemma 16.6) and no copies of $F[X]$ can occur in the direct sum decomposition. Multiplying each f_i by a unit we may assume the f_i are monic $\square$

<u>Remarks</u> (i) If α is represented by a matrix A, then the theorem says A is similar to $(*)(*)$.

(ii) The minimal poly of α is f_t.

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

<u>Example</u> If $\dim V = 2$ then $\sum_{i=1}^{t} \deg f_i = 2$

$$V_\alpha \cong \frac{F[X]}{(X-\lambda)} \oplus \frac{F[X]}{(X-\lambda)} \quad \text{or} \quad V_\alpha \cong \frac{F[X]}{(f)}$$

where f is the char poly of α

$\Rightarrow$ α has matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ or $C(f)$

Corollary 16.8 Let $A, B \in GL_2(F)$ not scalar matrices. Then A & B conjugate $\iff$ have same char poly f

Proof "$\Rightarrow$" see Linear Algebra

"$\Leftarrow$" By the above each is conjugate to $C(f)$. □

Lemma 16.9 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 polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$, so a factor $X-\lambda$.

So the irreducibles have degree 1. □

Theorem 16.10 (Jordan Normal Form)

Let $\alpha : V \to V$ be an endomorphism of a finite dimensional $\mathbb{C}$-vector space.

Consider $V = V_\alpha$ as a $\mathbb{C}[X]$-module with X acting as α. Then

$$V_\alpha \cong \frac{\mathbb{C}[X]}{((X-\lambda_1)^{n_1})} \oplus \cdots \oplus \frac{\mathbb{C}[X]}{((X-\lambda_t)^{n_t})}$$

where $\lambda_1, \ldots, \lambda_t \in \mathbb{C}$ (not necessarily distinct).

In particular, $\exists$ basis for V s.t. α has matrix

$$\begin{pmatrix} J_{n_1}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & J_{n_t}(\lambda_t) \end{pmatrix} \quad \text{where} \quad J_n(\lambda) = \begin{pmatrix} \lambda & & 0 \\ 1 & \ddots & \\ & \ddots & \lambda \\ 0 & & 1 \end{pmatrix} \Big\} n.$$

Proof $R = \mathbb{C}[X]$ is a Euclidean domain.

We apply the Primary Decomposition Theorem, noting that the primes in $\mathbb{C}[X]$ are as described in Lemma 16.9.

V finite dimensional $\Rightarrow$ we get no copies of $\mathbb{C}[X]$

$J_n(\lambda)$ represents multiplication by X on $\frac{\mathbb{C}[X]}{((X-\lambda)^n)}$ wrt the basis $1, X-\lambda, (X-\lambda)^2, \ldots, (X-\lambda)^{n-1}$. □

Remarks (i) If α is represented by a matrix A, then the theorem says A is similar to a matrix in JNF.

(ii) The Jordan blocks are unique up to reordering, though we have not proved this.

(iii) The minimal polynomial of α is $\prod_\lambda (X-\lambda)^{c_\lambda}$ where c_λ is the size of the largest block with eigenvalue λ

(iv) The characteristic polynomial of α is $\prod_\lambda (X-\lambda)^{a_\lambda}$ where a_λ is

the sum of the sizes of the blocks with eigenvalue λ.

(v) The number of blocks with eigenvalue λ is the dimension of the eigenspace $\mathrm{Ker}(\alpha - \lambda\,\mathrm{id})$

(vi) The uniqueness statement in (ii) may be proved by considering the dimensions of the generalised eigenspaces $\mathrm{Ker}((\alpha - \lambda\,\mathrm{id})^m)$

We illustrate some of the ideas that go into extending the structure theorem from R a ED to R a PID

Theorem 17.1 Let R be a PID. Then any finitely generated torsion-free R-module is free

(torsion-free: $r \cdot m = 0 \Rightarrow r = 0$ or $m = 0$)

N.B. For R a ED this was Corollary 16.4

Lemma 17.2 Let R be a PID and M an R-module. Let $r_1, r_2 \in R$ not both zero & $d = \gcd(r_1, r_2)$.

(i) $\exists\ A \in SL_2(R)$ s.t. $A\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$

(ii) If $x_1, x_2 \in M$ then $\exists\ x_1', x_2' \in M$ such that

$Rx_1 + Rx_2 = Rx_1' + Rx_2'$

& $r_1 x_1 + r_2 x_2 = d x_1' + 0 x_2'$

Proof R a PID $\Rightarrow (r_1, r_2) = (d)$

$\Rightarrow \exists\ \alpha, \beta \in R$ s.t $\alpha r_1 + \beta r_2 = d$

Write $r_1 = s_1 d$ & $r_2 = s_2 d$

so $\alpha s_1 + \beta s_2 = 1$.

(i) We have $\begin{pmatrix} \alpha & \beta \\ -s_2 & s_1 \end{pmatrix}\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$

$\det = \alpha s_1 + \beta s_2 = 1$

(ii) Let $x_1' = s_1 x_1 + s_2 x_2 \Rightarrow r_1 x_1 + r_2 x_2 = d x_1'$

$x_2' = -\beta x_1 + \alpha x_2$

Then $Rx_1' + Rx_2' \subset Rx_1 + Rx_2$. To prove the reverse inclusion, we solve for x_1 and x_2 in terms of x_1' and x_2'.

This is possible since $\det \begin{pmatrix} s_1 & s_2 \\ -\beta & \alpha \end{pmatrix} = 1$. □

Proof of Theorem 17.1

We are given that, say, $M = Rx_1 + \cdots + Rx_n$ with n as small as possible. If $x_1, \ldots, x_n$ are independent then M is free and we're done. Otherwise $\exists\, r_1, \ldots, r_n \in R$ not all zero s.t.

$$\sum_{i=1}^{n} r_i x_i = 0.$$

After reordering, wlog $r_1 \neq 0$.

Lemma 17.2 shows that after replacing x_1 and x_2 by suitable x_1' and x_2' we may assume $r_1 \neq 0$ and $r_2 = 0$.

Repeating this process (changing x_1 and x_3, then x_1 and x_4 & so on) we may assume $r_1 \neq 0$, $r_2 = \cdots = r_n = 0$.

Now $r_1 x_1 = 0 \overset{M \text{ torsion free}}{\Longrightarrow} x_1 = 0$.

Then $M = Rx_2 + \cdots + Rx_n$. ⚔ to choice of n □