# Groups, rings and modules

Shing Tak Lam

May 11, 2022

## Contents



# 1 Simplicity of the alternating group

## 1.1 Group theory

**Theorem 1.1** (Canonical decomposition)**.** Let $\phi : G \to H$ be a group homomorphism, then we have

$$G \twoheadrightarrow G/\ker(\phi) \xrightarrow{\cong} \operatorname{im}(\phi) \hookrightarrow H$$

*Proof.* Suffices to define the middle isomorphism. Define the map $\Phi : G/\ker(\phi) \to \operatorname{im}(\phi)$ by $\Phi(x\ker(\phi)) = \phi(x)$. First, we need to show that is is well defined. That is, it is independent of the choice of coset representative. Suppose $x\ker(\phi) = y\ker(\phi)$. Then $xy^{-1} \in \ker(\phi)$, so $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = 1$. Thus $\phi(x) = \phi(y)$. Clearly $\Phi$ is a surjective homomorphism, so suffices to show that $\Phi$ is injective. But this follows as $\phi(x) = \phi(y)$ if and only if $x\ker(\phi) = y\ker(\phi)$. So $\Phi$ is an isomorphism. □

**Theorem 1.2** (Second isomorphism theorem)**.** Let $H \leq G, K \trianglelefteq G$, then

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

*Proof.* First, we need to show that $HK$ is infact a group (equivalently, a subgroup of $G$). Clearly $1 \in HK$. If we have $h_1, h_2 \in H$, $k_1, k_2 \in K$, then

$$h_1 k_1 h_2 k_2 = h_1 h_2((h_2^{-1} k_1 h_2) k_2) \in HK$$

So $HK$ is closed under multiplication. Finally, suppose $h \in H, k \in K$. Then

$$(hk)^{-1} = k^{-1} h^{-1} = h^{-1} h k^{-1} h^{-1} \in HK$$

So $HK$ is a subgroup of $G$. Now we need to show that $K$ is a normal subgroup of $HK$. $k = 1k$, so $K \leq HK$. Since $K \trianglelefteq G$, we must have that $K \trianglelefteq HK$. Finally, define the group homomorphism $\phi : H \to HK/K$ by $\phi(h) = hK$. This is a group homomorphism, and $\ker(\phi) = H \cap K$. Applying the first isomorphism theorem gives the required result. □

**Theorem 1.3** (Third isomorphism theorem)**.** Let $H, K \trianglelefteq G$, $K \leq H$. Then

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

**Definition 1.4** (Simple group)
A nontrivial group $G$ is simple if the only normal subgroups of $G$ are 1 and $G$.

**Lemma 1.5.** Suppose $G$ is an abelian simple group. Then $G$ is finite, and $G \cong C_p$ for some prime $p$.

*Proof.* $G$ being an abelian simple group means that the only subgroups of $G$ are 1 and $G$. Choose a nontrivial element $x \in G$. Then $x$ must in fact generate $G$, and have prime order. □

**Lemma 1.6.** Suppose $G$ is a finite group. Then $G$ has a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$$

where each $G_i/G_{i-1}$ is simple.

*Proof.* By induction on $|G|$. If $|G| = 1$, we are done. If $|G| > 1$, let $G_{n-1}$ be a proper normal subgroup with maximal order. Then $G/G_{n-1}$ is simple, since if it has a proper normal subgroup, then we have a normal subgroup of $G$ properly containing $G_{n-1}$. Contradiction. Now apply the induction hypothesis on $G_{n-1}$. □

**Theorem 1.7.** Let $G$ be a nonabelian simple group, $H \leq G$, $|G : H| = n > 1$. Then $n \geq 5$, and $G \hookrightarrow A_n$.

*Proof.* Let $X = \{gH : g \in G\} = G/H$, letting $G$ act on $X$ by left multiplication. Let $\phi : G \to \mathrm{Sym}(X)$ be the permutation representation. Since $G$ is simple, $\ker(\phi) = 1$ or $\ker(\phi) = G$. If $\ker(\phi) = G$, then $\mathrm{Im}(\phi) = 1$, but the action is transitive, and $|X| > 1$. Contradiction. So $\ker(\phi) = 1$, and we have $\phi : G \hookrightarrow S_n$.

Considering $G \leq S_n$, by the second isomorphism theorem, we have that

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

Since $G$ is simple, $G \cap A_n = 1$ or $G \cap A_n = G$. If $G \cap A_n = 1$, then $G \hookrightarrow C_2$. But $G$ is nonabelian, so $G = G \cap A_n$, and $G \leq A_n$. □

**Definition 1.8** (Normaliser)
The normaliser of $H \leq G$ is

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

**Proposition 1.9.** The normaliser is the kernel of the conjugation action of $G$ on $H$. Furthermore, it is the largest subgroup of $G$ which $H$ is normal in.

## 1.2 Alternating group

**Lemma 1.10.** $A_n$ is generated by 3-cycles.

*Proof.* Each $\sigma \in A_n$ can be written as a product of an even number of transpositions. Suffices to show the product of any two transpositions is a three cycle.

$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d) \quad \text{and} \quad (a\ b)(b\ c) = (a\ b\ c)$$

□

**Lemma 1.11.** If $n \geq 5$, then all 3-cycles in $A_n$ are conjugate.

*Proof.* All 3-cycles in $S_n$ are conjugate, so suffices to show that the conjugacy class does not split. But $(1\ 2\ 3)(4\ 5) = (4\ 5)(1\ 2\ 3)$. □

**Theorem 1.12.** $A_n$ is simple for $n \geq 5$.

*Proof.* Let $N \trianglelefteq A_n$ be a nontrivial normal subgroup. Suffices to show that it contains a 3-cycle, since this would mean that it conatins all 3-cycles.

Fix $\sigma \in N$ nontrivial, write $\sigma$ as a product of disjoint cycles $\sigma = \sigma_1 \ldots \sigma_n$.

**Case 1:** *$\sigma_i$ has length $\geq 4$ for some $i$.* Without loss of generality, suppose $\sigma_1 = (1\ \ldots\ r)$ for $r \geq 4$. Let $\delta = (1\ 2\ 3)$. Then

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

**Case 2:** *$\sigma$ contains two 3-cycles.* Without loss of generality, $\sigma_1 = (1\ 2\ 3)$ and $\sigma_2 = (4\ 5\ 6)$. Let $\delta = (1\ 2\ 4)$. Then

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

This then reduces to Case 1.

**Case 3:** *$\sigma$ contains two 2-cycles.* Without loss of generality, $\sigma_1 = (1\ 2)$ and $\sigma_2 = (3\ 4)$. Let $\delta = (1\ 2\ 3)$. Then let

$$\pi = \sigma^{-1}\delta^{-1}\sigma\delta = (1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3) = (1\ 2\ 4)(1\ 2\ 3)(1\ 4)(2\ 4) \in N$$

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

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

**Case 4:** *$\sigma$ is a 3-cycle.* Immediate. □

# 2 Sylow theorems

## 2.1 $p$-groups

**Definition 2.1** ($p$-group)

For a prime $p$, a finite group $G$ is a $p$-group if $|G| = p^n$ for some $n \geq 1$.

**Theorem 2.2.** Suppose $G$ is a $p$ group. Then $Z(G) \neq 1$.

*Proof.* For $g \in G$, we have from the Orbit-Stabiliser theorem that $|\text{ccl}(g)||C(g)| = |G| = p^n$. So the size of each conjugacy class must divide $p^n$. As conjugacy classes partition, the number of $g \in G$ such that $|\text{ccl}(g)| = 1$ must be $0 \pmod{p}$. But $\text{ccl}(1) = 1$, so there is at least one, and the centre is nontrivial. □

**Corollary 2.3.** Suppose $G$, $|G| = p^n$, $n \geq 2$. Then $G$ is not simple.

*Proof.* If $G$ is not abelian, note that $Z(G) \trianglelefteq G$. If $G$ is abelian, note that we have a subgroup of order $p$ by Cauchy's theorem. □

**Corollary 2.4.** Let $G$ be a $p$-group, $|G| = p^n$. For all $0 \leq r \leq n$, $G$ has a subgroup of order $p^r$.

*Proof.* $G$ has a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$$

where each $G_i/G_{i-1}$ is simple. Since $G$ is a $p$-group, $G_i/G_{i-1}$ is a $p$-group as well. But this means that $G_i/G_{i-1} \cong C_p$. So $|G_k| = p^k$. □

**Lemma 2.5.** Let $G$ be a group such that $G/Z(G)$ is cyclic. Then $G$ is abelian, and $Z(G) = G$.

*Proof.* Suppose $G/Z(G)$ is generated by $gZ(G)$. Let $x, y \in G$, since cosets partition, we must have $n, m \in \mathbb{Z}$, $a, b \in Z(G)$ such that $x = g^n a$ and $y = g^m b$. Then

$$xy = g^n a g^m b = g^{n+m} ab = g^{n+m} ba = g^m b g^n a = yx$$

So $G$ is abelian, and $Z(G) = G$. □

**Corollary 2.6.** Every group of order $p^2$ is abelian.

*Proof.* Since $Z(G)$ is nontrivial, $G/Z(G) = 1$ or $C_p$. Both cases we are done by the previous lemma. □

## 2.2 Sylow's theorems

**Definition 2.7** (Sylow-$p$ subgroup)

Let $G$ be a finite group, $p$ prime. Then $P \leq G$ is a Sylow-$p$ subgroup if $|G : P|$ is coprime to $p$. Let $\text{Syl}_p(G)$ be the set of all Sylow-$p$ subgroups of $G$.

**Theorem 2.8** (Sylow I).

$$\mathrm{Syl}_p(G) \neq \varnothing$$

*Proof.* Suppose $|G| = p^a m$, where $p, m$ coprime. Let

$$\Omega = \{S \subseteq G : |S| = p^a\}$$

Then

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

For $0 \leq k < p^a$, $v_p(p^a m - k) = v_p(p^a - k)$, where $v_p(n)$ is the $p$-adic valuation, or the exponent of the largest power of $p$ dividing $n$. So $|\Omega|$ is coprime to $p$. Let $G \circlearrowleft \Omega$ by left multiplication. By the orbit-stabiliser theorem, we have that for any $X \in \Omega$,

$$|G_X||\mathrm{Orb}(X)| = |G|$$

Since $|\Omega|$ is coprime to $p$ and orbits paritition, we must have $X \in \Omega$ such that $|\mathrm{Orb}(X)|$ is coprime to $p$. So $p^a \mid |G_X|$. On the other hand, for $g \in G, x \in X$, $g = gx^{-1}x \in (gx^{-1})X$, so

$$G = \bigcup_{g \in G} \left(gx^{-1}\right) X = \bigcup_{Y \in \mathrm{Orb}(X)} Y$$

Which means that $|G| \leq |\mathrm{Orb}(X)||X| = p^a|\mathrm{Orb}(X)|$. Hence $|G_X| \leq p^a$, so $|G_X| = p^a$, and $G_X \in \mathrm{Syl}_p(G)$. □

**Lemma 2.9.** Suppose $P \in \mathrm{Syl}_p(G)$, $Q \leq G$ is a $p$-subgroup. Then there exists $g \in G$ such that $Q \leq gPg^{-1}$ for all $g \in G$.

*Proof.* Let $Q$ act on $G/P$ by left multiplication. By orbit stabiliser, we have that

$$p^k = |Q| = \left|G_{gP}\right||\mathrm{Orb}(gP)|$$

This means that the size of all orbits are a $p$-power. Since $G/P$ has size coprime to $p$ and orbits partition, we have an orbit of size 1. That is, we have $g \in G$ such that for all $q \in Q$, $qgP = gP$. That is, $g^{-1}qg \in P$, or $q \in gPg^{-1}$, so $Q \leq gPg^{-1}$. □

**Theorem 2.10** (Sylow II). For any $P, Q \in \mathrm{Syl}_p(G)$, $P, Q$ are conjugate.

*Proof.* By the previous lemma, we have $g \in G$ such that $Q \leq gPg^{-1}$. By considering the orders, they must in fact be equality. So $P$ and $Q$ are conjugate. □

**Theorem 2.11** (Sylow III). Let $n_p = \left|\mathrm{Syl}_p(G)\right|$. Then $n_p \equiv 1 \pmod{p}$ and $n_p \mid |G|$. That is, if $|G| = p^a m$ with $m, p$ coprime, then $n_p \mid m$.

*Proof.* Let $G$ act on $\mathrm{Syl}_p(G)$ by conjugation. Sylow II implies that the action is transitive. So from orbit stabiliser, we have that

$$|G| = \left|\mathrm{Syl}_p(G)\right||G_P| \implies n_p \mid |G|$$

Fix $P \in \mathrm{Syl}_p(G)$, and let $P$ act on $\mathrm{Syl}_p(G)$ by conjugation. From orbit stabilier, the size of the orbits have size dividing a power of $p$. Suffices to show there is only one orbit of size 1, namely $\{P\}$. Suppose $\{Q\}$ is an orbit of size 1. Then $pQp^{-1} = Q$, so $P \leq N_G(Q)$. Then $P, Q$ are Sylow-$p$ subgroups of $N_G(Q)$, so conjugate by Sylow II. Hence $P = Q$ since $Q \trianglelefteq N_G(Q)$. □

## 3 Matrix groups

**Definition 3.1** (General linear group)
For a field $F$, the general linear group is

$$\mathrm{GL}_n(F) = \{M \in \mathrm{Mat}_n(F) : \det(M) \neq 0\}$$

**Definition 3.2** (Special linear group)
The special linear group is

$$\mathrm{SL}_n(F) = \{M \in \mathrm{Mat}_n(F) : \det(M) = 1\} = \ker(\det) \leq \mathrm{GL}_n(F)$$

**Definition 3.3** (Projective general linear group)
The projective general linear group is

$$P\,\mathrm{GL}_n(F) = \frac{\mathrm{GL}_n(F)}{Z} \quad \text{where} \quad Z = \{aI : a \in F^\times\}$$

**Definition 3.4** (Projective special linear group)
The projective special linear group is

$$P\,\mathrm{SL}_n(F) = \frac{\mathrm{SL}_n(F)}{Z \cap \mathrm{SL}_n(F)}$$

**Proposition 3.5.**

$$P\,\mathrm{SL}_n(F) \leq P\,\mathrm{GL}_n(F)$$

*Proof.*

$$P\,\mathrm{SL}_n(F) = \frac{\mathrm{SL}_n(F)}{Z \cap \mathrm{SL}_n(F)} \cong \frac{Z\,\mathrm{SL}_n(F)}{Z} \leq P\,\mathrm{GL}_n(F)$$

□

**Definition 3.6** (Möbius map)
For a fixed field $F$, $P\,\mathrm{GL}_2(F)$ acts on $F \cup \{\infty\}$ by Möbius maps.

## 4 Rings

**Theorem 4.1** (Canonical decomposition)**.** Suppose $\phi : R \to S$ is a ring homomorphism. Then we have the decomposition

$$R \twoheadrightarrow R/\ker(\phi) \xrightarrow{\cong} \mathrm{im}(\phi) \hookrightarrow S$$

**Theorem 4.2** (Second isomorphism theorem)**.** Suppose $R \leq S, J \trianglelefteq S$. Then

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

**Theorem 4.3** (Third isomorphism theorem)**.** Let $I, J \trianglelefteq R$, $I \leq J$. Then

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

**Proposition 4.4.** For all rings $R$, there exists a unique homomorphism $\iota : \mathbb{Z} \to R$.

*Proof.* $\iota(0) = 0$ and $\iota(1) = 1$ determines the homomorphism uniquely. □

**Definition 4.5** (Characteristic)

Let $\iota : \mathbb{Z} \to R$. Then $\ker(\iota) \trianglelefteq \mathbb{Z}$, so $\ker(\iota) = n\mathbb{Z}$ for some $n$. Define the characteristic of $R$ to be $\mathrm{char}(R) = n$.

**Lemma 4.6.** Suppose $R$ is an integral domain. Then so is $R[X]$.

*Proof.* Suppose $f, g \in R[X]$, $f = a_n X^n + \cdots + a_0$, $g = b_m X^m + \cdots + b_0$, where $a_n, b_m \neq 0$. The coefficient of $X^{n+m}$ in $fg$ is $a_n b_m$, which is nonzero as $R$ has no zero divisors. Hence $fg \neq 0$. □

**Lemma 4.7.** Suppose $R$ is an integral domain, $f \in R[X]$. Then

$$|\{a \in R : f(a) = 0\}| \leq \deg(f)$$

*Proof.* $f(x) = (x - a_1) \cdots (x - a_k) g(x)$, and consider degrees. □

**Theorem 4.8.** Let $F$ be a field, $G \leq F^\times$ be a finite subgroup. Then $G$ is cyclic.

*Proof.* By the structure theorem of finite abeliean groups, if $G$ is not cyclic then there exists $H \cong C_{d_1} \times C_{d_2} \leq G$, $d_1, d_2 \geq 2$, $d_1 \mid d_2$, and without loss of generality, we may assume $d_1 = d_2$. Then the polynomial

$$f(X) = X^{d_1} - 1 \in F[X]$$

has degree $d_1$ but at least $d_1^2$ roots. Contradiction. □

**Proposition 4.9.** Any finite integral domain is a field.

*Proof.* Left multiplication in an integral domain is injective. An injective map from a finite set to itself must be a bijection. □

**Definition 4.10** (Field of fractions)
Let $R$ be an integral domain, then define the field of fractions of $R$ to be

$$\text{Frac}(R) = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}$$

where we have that[a]

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

and the operations are defined as in the field of rationals.

[a]Formally, the field of fractions is a quotient.

**Theorem 4.11.** Let $R$ be an integral domain. Then $\text{Frac}(R)$ is a field, and $R \leq \text{Frac}(R)$.

**Definition 4.12** (Maximal ideal)
Let $R$ be a ring. An ideal $I \trianglelefteq R$ is maximal if for any ideal $J$ such that $I \leq J \leq R$, $J = I$ or $J = R$.

**Lemma 4.13.** A nonzero ring $R$ is a field if and only if the only ideals are $(0)$ and $(1)$.

*Proof.* Suppose $R$ is a field, and let $I \trianglelefteq R$ be an ideal. If $I = 0$ we are done. Otherwise, we have $a \in R$ such that $a \neq 0$. But then $1 = a^{-1}a \in I$, so $I = (1) = R$.

Conversely, suppose the only ideals are $(0)$ and $(1)$. Let $a \in R$ be nonzero. Then we must have that $(a) = (1)$, so $a$ is a unit. □

**Proposition 4.14.** Let $I \trianglelefteq R$ be an ideal. Then $I$ is maximal if and only if $R/I$ is a field.

*Proof.* $R/I$ is a field
$\iff$ The only ideals of $R/I$ are $0 = I/I$ and $(1) = R/I$.
$\iff$ The only ideals in $R$ containing $I$ are $I$ and $R$. □

**Definition 4.15** (Prime ideal)
Let $R$ be a ring, an ideal $I \trianglelefteq R$ is prime if $I \neq R$ and for any $a, b \in R$, if $ab \in I$ then $a \in I$ or $b \in I$.

**Proposition 4.16.** Let $I \leq R$. Then $I$ is prime if and only if $R/I$ is an integral domain.

*Proof.* Suppose $I$ is prime. Given $a, b \in R$, suppose $(a + I)(b + I) = (ab + I) = 0$. Then $ab \in I$, so either $a \in I$ or $b \in I$. Thus, either $a + I = 0$ or $b + I = 0$.

Conversely, suppose $R/I$ is an integral domain. By considering $(a + I)(b + I)$ as above, we see that $I$ is a prime ideal. □

**Definition 4.17** (Noetherian)
A ring $R$ is Noetherian if every ascending chain of ideals is eventually constant.

**Theorem 4.18.** A ring $R$ is Noetherian if and only if every ideal in $R$ is finitely generated.

*Proof.* Let $I_1 \leq I_2 \leq \dots$ be ideals, $I = \bigcup_n I_n$. Then $I$ is an ideal which is finitely generated, say $I = (a_1, \dots, a_M)$. Let $N = \max_i \min \left\{ j : a_i \in I_j \right\}$. Then $I_N = I$.

Conversely, suppose if $R$ satisfies the ascending chain condition, but $J$ is an ideal which is not finitely generated. Choose $a_1 \in J$ nonzero, then $J \neq (a_1)$. Now choose $a_2 \in J \setminus (a_1), \dots, a_n \in J \setminus (a_1, \dots, a_{n-1})$. Then $(a_1) \leq (a_1, a_2) \leq \dots$ is an infinite ascending chain of ideals which is not eventually constant. Contradiction. □

**Theorem 4.19** (Hilbert basis theorem)**.** If $R$ is a Noetherian ring, then so is $R[X]$.

*Proof.* Suppose for contradiction we have $J \trianglelefteq R[X]$ which is not finitely generated. Choose $f_1 \in J$ with minimal degree, $f_2 \in J \setminus (f_1), \dots, f_n \in J \setminus (f_1, \dots, f_{n-1})$ with minimal degrees. Then $\deg(f_1) \leq \deg(f_2) \leq \dots$. Let $a_i$ be the leading coefficient of $f_i$. We have a sequence of ideals

$$(a_1) \leq (a_1, a_2) \leq \dots$$

in $R$ which must be eventually constant. So we have $m$ such that $a_{m+1} \in (a_1, \dots, a_m)$, so

$$a_{m+1} = \sum_{i=1}^{m} \lambda_i a_i$$

and

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

Then $\deg(g) = \deg(f_{m+1})$, and they have the same leading coefficient. So $f_{m+1} - g \in J$, $\deg(f_{m+1} - g) < \deg(f_{m+1})$. By minimality of degree, $f_{m+1} - g \in (f_1, \dots, f_m)$. But $g \in (f_1, \dots, f_m)$, so $f_{m+1} \in (f_1, \dots, f_m)$. Contradiction. □

**Lemma 4.20.** Let $R$ be a Noetherian ring, $I \trianglelefteq R$ be an ideal. Then $R/I$ is Noetherian.

*Proof.* The preimage of an ideal is an ideal. □

# 5 Factorisation

In this section, $R$ will be an integral domain.

**Definition 5.1** (Divides)

$a \in R$ divides $b \in R$, $a \mid b$, if $(b) \subseteq (a)$.

**Definition 5.2** (Associates)

$a, b \in R$ are associates if $(a) = (b)$.

**Definition 5.3** (Irreducible)

$a \in R$ is irreducible if $r \neq 0$, $r \notin R^\times$ and if $r = ab$, then $a \in R^\times$ or $b \in R^\times$.

**Definition 5.4** (Prime)
$a \in R$ is prime if $r \neq 0$, $r \notin R^\times$, and if $r \mid ab$, then $r \mid a$ or $r \mid b$.

**Lemma 5.5.** $(r) \trianglelefteq R$ is prime if and only if $r = 0$ or $r$ is prime.

*Proof.* Suppose $(r)$ is prime. If $r = 0$ we are done. Suppose $r \neq 0$. Since a prime ideal is proper, we must have that $r$ is not a unit. Now suppose $r \mid ab$. Then $ab \in (r)$. So we must have that $a \in (r)$ or $b \in (r)$. So $r \mid a$ or $r \mid b$.

Conversely, $(0) = 0$ which is prime. If $r$ is prime, then by the above reasoning we can see that $(r)$ is prime. □

**Lemma 5.6.** $r \in R$ prime $\implies$ $r \in R$ irreducible.

*Proof.* Suppose $r = xy$ is a product of two elements of $R$. Then $r \mid xy$, so we must have that $r \mid x$ or $r \mid y$. Without loss of generality, assume $r \mid x$. Say $x = rz$. Then $r = xy = ryz$. As $r \neq 0$, we must in fact have that $yz = 1$. So $y$ is a unit. □

**Definition 5.7** (Principal ideal domain)
An integral domain $R$ is a principal ideal domain if all ideals $I \trianglelefteq R$ are principal.

**Lemma 5.8.** Let $r \in R$, $r \neq 0$. If $(r)$ is maximal, then $r$ is irreducible. Furthermore, if $R$ is a PID, then the converse implication also holds.

*Proof.* Suppose $r = xy$. Then $(r) \leq (x)$, and as $(r)$ is a maximal ideal, $(r) = (x)$ or $(x) = (1)$. Which corresponds to $y$ and $x$ being a unit respectively.

Suppose $R$ is a PID, and suppose $(r)$ is irreducible. Say $(r) \leq (a) \leq (1)$. Then $r = ab$ for some $b \in R$. But $r$ is irreducible, so $a$ or $b$ must be a unit, which corresponds to $(a) = (1)$ and $(r) = (a)$ respectively. □

**Proposition 5.9.** Let $R$ be a PID, $r \in R$ is irreducible if and only if it is prime.

*Proof.* Suppose $r$ is irreducible. Then $(r)$ is maximal, so $R/(r)$ is a field, which is an integral domain, so $(r)$ is prime, and as $r$ is nonzero, $r$ must be prime. □

**Definition 5.10** (Euclidean domain)
An integral domain $R$ is a Euclidean domain if there exists a function

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

such that

- If $a \mid b$, then $\phi(a) \leq \phi(b)$.
- If $a, b \in R$, $b \neq 0$, then there exists $q, r \in R$ such that

$$a = bq + r \quad \text{where} \quad r = 0 \text{ or } \phi(r) < \phi(b)$$

**Proposition 5.11.** If $R$ is an ED then it is a PID.

*Proof.* Let $I \trianglelefteq R$, $I \neq 0$. Choose $b \in I$, $b \neq 0$ such that $\phi(b)$ minimal. Then $(b) \subseteq I$, and for $a \in I$, write $a = bq + r$, where either $r = 0$ or $\phi(r) < \phi(b)$. Note that $r = a - bq \in I$, so by minimality we must have that $r = 0$. So $b \mid a$, and $I = (b)$. □

**Definition 5.12** (Unique factorisation domain)
An integral domain $R$ is a unique factorisation domain if

- Every $r \in R$, $r \neq 0$, $r \notin R^\times$ is a product of irreducible elements.
- If $p_1 \cdots p_m = q_1 \cdots q_n$ where the $p_i, q_i$ are irreducible, then $m = n$, and up to reordering, $(p_i) = (q_i)$.

**Proposition 5.13.** Let $R$ be an integral domain where every nonzero, nonunit element can be written as a product of irreducibles. Then $R$ is a UFD if and only if every irreducible is prime.

*Proof.* Suppose $R$ is an UFD and $p \in R$ is irreducible. Suppose $p \mid ab$, so there exists $c$ such that $ab = pc$. Writing $a, b, c$ as a product of irreducibles, by the uniqueness of factorisation, $p \mid a$ or $p \mid b$.

Now suppose every irreducible is prime, and say we have $p_1 \cdots p_m = q_1 \cdots q_n$, $p_i, q_i$ irreducible. Since $p_1$ is prime, then we must have some $q_i$ such that $p_1 \mid q_i$. Without loss of generality, $p_1 \mid q_1$. Since $q_1$ is irreducible, we must have that $q_1 = p_1 u$ for some $u \in R^\times$. But this means that $(p_1) = (q_1)$. Cancelling (which we can do as we are in an integral domain), and using induction we get the required result. □

**Theorem 5.14.** If $R$ is a PID, then it is a UFD.

*Proof.* Since every irreducible is prime in a PID, suffices to show nonzero, nonunit elements can be written as a product of irreducibles. Suppose $x$ is not a product of irreducibles. Then there exists $x_1, y_1 \in R$ non units such that $x = x_1 y_1$. Without loss of generality $x_1$ is not a product of irreducibles. Then $x_1 = x_2 y_2$ a product of nonunits. This gives us a sequence $x_1, x_2, \ldots$, and an ascending chain of ideals

$$(x_1) \subset (x_2) \subset \ldots$$

which does not terminate. Contradiction, as a PID is Noetherian. □

**Definition 5.15** (Greatest common divisor)
Let $R$ be an integral domain, $d \in R$ is a gcd of $a_1, \ldots, a_n \in R$ if

- $d \mid a_1, \ldots, d \mid a_n$.
- If $d' \mid a_1, \ldots, d' \mid a_n$, then $d \mid d'$.

**Definition 5.16** (Least common multiple)
Let $R$ be an integral domain, $m \in R$ is a lcm of $a_1, \ldots, a_n \in R$ if

- $a_1 \mid m, \ldots, a_n \mid m$.
- If $a_1 \mid m', \ldots, a_n \mid m'$, then $m \mid m'$.

**Remark 5.17.** $\gcd(a_1, \ldots, a_n)$ and $\operatorname{lcm}(a_1, \ldots, a_n)$ are defined up to associates. Equivalently, we can define these as principal ideals, in which case it would be uniquely defined.

**Proposition 5.18.** In a UFD, $\gcd(a_1, \ldots, a_n)$ and $\operatorname{lcm}(a_1, \ldots, a_n)$ exist.

*Proof.* Write each as a product of irreducibles and use formula as in $\mathbb{Z}$. □

## 5.1 Polynomial rings

In this section let $R$ be a UFD, and $F = \operatorname{Frac}(R)$ be its field of fractions.

**Definition 5.19** (Content)
The content of a polynomial $f \in R[X]$, $f(X) = a_n X^n + \cdots + a_0$ is $c(f) = \gcd(a_0, \ldots, a_n)$.

**Definition 5.20** (Primitive)
A polynomial $f \in R[X]$ is primitive if $c(f) \in R^\times$.

**Lemma 5.21.** If $f, g$ are primitive, then so is $fg$.

*Proof.* Suppose not. Say we have a prime $p$ such that $p \mid c(fg)$. Furthermore, suppose $f(X) = a_n X^n + \cdots + a_0$ and $g(X) = b_m X^m + \cdots + b_0$. Since $f$ and $g$ are primitive, $p \nmid c(f)$ and $p \nmid c(g)$. Let $k = \min\{i : p \nmid a_i\}$ and $l = \min\{i : p \nmid b_i\}$. The coefficient of $X^{k+l}$ in $fg$ is

$$\sum_{i+j=k+l} a_i b_j = a_k b_l + \sum_{i=0}^{k-1} a_i b_{k+l-i} + \sum_{j=0}^{l-1} a_{k+l-j} b_j$$

By minimality, we have that $p \mid a_i$ for $i \leq k-1$, $p \mid b_j$ for $j \leq l-1$, and $p \mid \sum\limits_{i+j=k+l} a_i b_j$. So $p \mid a_k b_l$, and $p \mid a_k$ or $p \mid b_l$. Contradiction. □

**Lemma 5.22.** If $f, g \in R[X]$, then $c(fg) = c(f)c(g)$[a].

[a]Equality up to associates, or equivalently, equality of ideals.

*Proof.* Write $f = c(f) f_0$ and $g = c(g) g_0$, where $f_0, g_0$ primitive. Then

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

□

**Corollary 5.23.** If $p \in R$ is prime, then $p$ is prime in $R[X]$.

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

$$p \mid fg \iff p \mid c(fg) \iff p \mid c(f)c(g) \iff p \mid c(f) \vee p \mid c(g) \iff p \mid f \vee p \mid g$$

□

**Lemma 5.24.** Let $f, g \in R[X]$, $g$ primitive. If $g \mid f$ in $F[X]$, then $g \mid f$ in $R[X]$.

*Proof.* Suppose $f = gh$, where $h \in F[X]$. Let $a \in R$ be the lcm of the denominators of the coefficients of $h$. Then $ah \in R[X]$. Let $ah = c(ah)h_0$, with $h_0 \in R[X]$ primitive. Then $af = c(ah) \underbrace{h_0 g}_{\text{primitive}}$, so $a \mid c(af)$ implies that $a \mid c(ah)$. Thus, we must have that $h \in R[X]$. □

**Lemma 5.25 (Gauss).** Let $f \in R[X]$ be primitive. Then $f$ irreducible in $R[X]$ implies that $f$ is irreducible in $F[X]$.

*Proof.* We prove the contrapositive. Suppose $f$ is not irreducible in $F[X]$, that is, we have $g, h \in F[X]$ non units (so $\deg(g), \deg(h) > 0$), such that $f = gh$. Let $b \in R, b \neq 0$ be such that $bg \in R[X]$. Then $bg = c(bg)g_0$, where $g_0$ is primitive. Let $\lambda = c(bg)b^{-1}$. Then $\lambda^{-1}g = g_0 \in R[X]$ and is primitive. Thus, by considering $\lambda^{-1}g\lambda h$, we may assume without loss of generality that $g \in R[X]$ primitive. But then $g \mid f$ in $F[X]$ implies that $g \mid f$ in $R[X]$ by the previous lemma. So $f = gh$, where $g, h \in R[X]$ are non units. So $f$ is not irreducible in $R[X]$. □

**Lemma 5.26.** Let $g \in R[X]$ be primitive. Then $g \in F[X]$ prime implies that $g \in R[X]$ prime.

*Proof.* Suppose $f_1, f_2 \in R[X]$, $g \mid f_1 f_2$ in $R[X]$. Then $g \mid f_1 f_2$ in $F[X]$. Without loss of generality, suppose $g \mid f_1$ in $F[X]$. But as $g$ is primitive, we have that $g \mid f_1$ in $R[X]$. □

**Theorem 5.27.** Let $R$ be a UFD. Then $R[X]$ is a UFD.

*Proof.* Let $f \in R[X]$, where $f = c(f)f_0$, $f_0$ primitive. Then $R$ is a UFD implies that $c(f)$ is a product of irreducibles in $R$, which must then be a product of irreducibles in $R[X]$. Suppose $f_0$ is not irreducible, say $f_0 = gh$, $g, h \in R[X]$ non units. Then as $f$ is primitive, so must $g, h$. By induction on the degree of $f_0$, we have that $f_0$ is a product of irreducibles.

Therefore, we have that every $f \in R[X]$ can be written as a product of irreducibles. Suffices to show that all irreducibles in $R[X]$ are prime. Let $f \in R[X]$ be irreducible. Let $f = c(f)f_0$, $f_0 \in R[X]$ primitive. Since $f$ is irreducible, we must have that $f$ is constant or primitive.

If $f$ is constant, then it is irreducible in $R$, so prime in $R$, and thus prime in $R[X]$. If $f$ is primitive, then $f$ is irreducible in $F[X]$, so prime in $F[X]$, so prime in $R[X]$. □

**Proposition 5.28 (Eisenstein's criterion).** Let $R$ be a UFD, $f \in R[X]$, $f = a_n X^n + \cdots + a_0$ primitive. Suppose we have a prime (or equivalently irreducible) $p \in R$ such that

- $p \mid a_{n-1}, \ldots, p \mid a_0$,
- $p^2 \nmid a_0$,
- $p \nmid a_n$,

then $f$ is irreducible over $R[X]$.

*Proof.* Suppose not. Say we have $f = gh$, $g, h \in R[X]$ non units. Then $f$ primitive implies that $\deg(g), \deg(h) > 0$. Say

$$g = r_k X^k + \cdots + r_0 \quad \text{and} \quad h = s_l X^l + \cdots + s_0$$

Since $a_n = r_k s_l$, and $p \nmid a_n$, we have that $p \nmid r_k, p \nmid s_l$. $a_0 = r_0 s_0$, so $p \mid a_0$ implies that $p \mid r_0$ or $p \mid s_0$. Without loss of generality, assume $p \mid r_0$. Let $j$ be such that $p \mid a_0, \dots, p \mid a_{j-1}$, and $p \nmid a_j$ (exists as $g$ primitive). Then

$$a_j = r_0 s_j + \cdots + r_{j-1} s_1 + r_j s_0$$

But as $p \mid a_j$ since $j \leq \deg(g) \leq n-1$, so $p \mid r_j s_0$, which means that $p \mid s_0$. But $p^2 \nmid a_0$. Contradiction. □

## 5.2 Algebraic integers

**Definition 5.29** (Norm)
Define the norm of a Gaussian integer to be $N(a+bi) = a^2 + b^2$.

**Proposition 5.30.** $\mathbb{Z}[i]$ is a Euclidean domain with Euclidean function $\phi = N$.

**Proposition 5.31.** Let $p \in \mathbb{Z}$ be prime. Then the following are equivalent.

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

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

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

*Proof.* Suppose $p$ is not prime in $\mathbb{Z}[i]$. Equivalently, $p$ is not irreducible in $\mathbb{Z}[i]$. Then $p = xy$, where $x, y \in \mathbb{Z}[i]$ non units. So

$$p^2 = N(p) = N(x)N(y) \implies N(x) = N(y) = p$$

Letting $x = a + ib$, we have that $p = N(x) = a^2 + b^2$.

Now suppose $p = a^2 + b^2$. Since all squares are 0 or 1 mod 4, we have the required result. Finally, suppose $p = 2$. Then $2 = (1+i)(1-i)$ is not irreducible. So suppose $p \equiv 1 \pmod 4$. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$, and as $4 \mid p-1$, we have an element of order 4. So we have $x \in \mathbb{Z}$ such that $x^4 + 1 \pmod p$, and $x^2 \not\equiv 1 \pmod p$. But then this means that $x^2 \equiv -1 \pmod p$, so $p \mid x^2 + 1 = (x-i)(x+i)$ in $\mathbb{Z}[i]$. □

**Theorem 5.32.** The primes in $\mathbb{Z}[i]$ are (up to associates)

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

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

*Proof.* First we need to show that these are primes. For (i), we have that $N(a+bi) = a^2 + b^2 = p$, so it must be irreducible. For (ii), this follows immediately from the previous proposition.

Now let $z \in \mathbb{Z}[i]$ be irreducible. Then $\overline{z} \in \mathbb{Z}[i]$ is also irreducible. Then $N(z) = z\overline{z}$ is a factorisation of $N(z)$ into irreducibles in $\mathbb{Z}[i]$. Let $p \in \mathbb{Z}$ be a prime, $p \mid N(z)$. If $p \equiv 3 \pmod 4$, then $p$ is prime in $\mathbb{Z}[i]$, so $p \mid z$ or $p \mid \overline{z}$. Note that $p \mid z$ if and only if $p \mid \overline{z}$, so $p$ is in fact an associate of $z$.

If $p = 2$ or $p \equiv 1 \pmod 4$, then $p = a^2 + b^2 = (a+bi)(a-bi)$ is a product of irreducibles in $\mathbb{Z}[i]$. Then $(a+bi)(a-bi) \mid z\overline{z}$, so by uniqueness of factorisation, $z$ is an associate of $a + bi$ or $a - bi$. □

**Corollary 5.33.** An integer $n \geq 1$ is the sum of two squares if and only if every prime factor $p \mid n$ where $p \equiv 3 \pmod 4$ has even multiplicity.

*Proof.* The norms of primes of $\mathbb{Z}[i]$ are precisely

- 2,
- $p$, where $p \equiv 1 \pmod 4$,
- $p^2$, where $p \equiv 3 \pmod 4$.

□

**Definition 5.34** (Algebraic number)
$\alpha \in \mathbb{C}$ is an algebraic number if there exists $p \in \mathbb{Q}[X]$ nonzero such that $p(\alpha) = 0$.

**Definition 5.35** (Algebraic integer)
$\alpha in \mathbb{C}$ is an algebraic integer if there exists $p \in \mathbb{Z}[X]$ nonzero, monic such that $p(\alpha) = 0$.

**Definition 5.36** (Adjunction)
Let $R \leq S$ be a subring, $\alpha \in S$. Then define $R[\alpha]$ to be the smallest subring of $S$ that contains both $R$ and $\alpha$.

**Definition 5.37** (Minimal polynomial)
For an algebraic number $\alpha$, let $\phi : \mathbb{Q}[X] \to \mathbb{C}$, $\phi(g) = g(\alpha)$. Then as $\mathbb{Q}[X]$ is a PID, $\ker(\phi) = (f) \neq 0$, as $\alpha$ is an algebraic number. Without loss of generality $f$ monic. Then $f$ is the minimal polynomial of $\alpha$.

**Proposition 5.38.** Suppose $f$ is the minimal polynomial for $\alpha$. Then

$$\frac{Q[x]}{(f)} \cong Q[\alpha]$$

**Proposition 5.39.** Let $\alpha$ be an algebraic integer with minimal polynomial $f$. Then $f \in \mathbb{Z}[X]$.

*Proof.* Let $\theta : \mathbb{Z}[X] \to \mathbb{C}$, $\theta(g) = g(\alpha)$ be the restriction of $\phi$ to $\mathbb{Z}[X] \leq \mathbb{Q}[X]$. Let $\lambda \in \mathbb{Q}^\times$ be such that $\lambda f \in \mathbb{Z}[X]$ and is primitive. Then $\lambda f(\alpha) = 0$, so $\lambda f \in \ker(\theta)$.

Let $g \in \ker(\theta)$. Then $g \in \ker(\phi)$, so $\lambda f \mid g$ in $\mathbb{Q}[X]$. But then this means that $\lambda f \mid g$ in $\mathbb{Z}[X]$. Suppose $g \in \ker(\theta)$ nonzero monic. Then as $f$ and $g$ are both monic, $\lambda = \pm 1$, so $f \in \mathbb{Z}[X]$. □

# 6 Modules

**Theorem 6.1** (Canonical decomposition)**.** For a $R$-module homomorphism $f : M \to N$, we have that

$$M \twoheadrightarrow M/\ker(f) \xrightarrow{\cong} \mathrm{im}(f) \hookrightarrow N$$

**Theorem 6.2** (Second isomorphism theorem)**.** Let $A, B \leq M$ be $R$-submodules. Then

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

**Theorem 6.3** (Third isomorphism theorem)**.** Let $N \leq L \leq M$, then

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

**Definition 6.4** (Annihilator)
The annihilator of an $R$-module $M$ is

$$\text{Ann}_R(M) = \{r \in R : \forall m \in M, rm = 0\} \trianglelefteq R$$

**Definition 6.5** (Finitely generated module)
An $R$-module $M$ is finitely generated if there exists $m_1, \ldots, m_n$ such that

$$M = Rm_1 + \cdots + R_{m_n}$$

**Proposition 6.6.** An $R$-module $M$ is finitely generated if and only if there exists a surjective $R$-module homomorphism $R^n \twoheadrightarrow M$.

**Corollary 6.7.** Suppose $N \leq M$, $M$ is finitely generated. Then $M/N$ is also finitely generated.

**Definition 6.8** (Torsion)
Let $M$ be a $R$-module, $m \in M$ is torsion if there exists $r \in R$, $r \neq 0$ such that $rm = 0$.

**Definition 6.9** (Torsion module)
An $R$-module $M$ is torsion if every element of $M$ is torsion. $M$ is torsion free if the only torsion element is 0.

**Definition 6.10** ((External) direct sum)
Let $M_1, \ldots, M_n$ be $R$-modules, then define the direct sum

$$\bigoplus_{i=1}^{n} M_i = \{(m_1, \ldots, m_n) : m_i \in M_i\}$$

with pointwise operations.

**Lemma 6.11.** Suppose $N_i \leq M_i$ for all $i$. Then

$$\frac{\bigoplus_{i=1}^n M_i}{\bigoplus_{i=1}^n N_i} \cong \bigoplus_{i=1}^n \frac{M_i}{N_i}$$

*Proof.* Consider the canonical decomposition of the $R$-module homomorphism

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

□

**Definition 6.12** (Generator)
Let $S \subseteq M$. If every element $m \in M$ can be written as a finite $R$-linear combination of elements of $S$, then $S$ is a generator for $M$.

**Definition 6.13** (Free generator)
A generator $S \subseteq M$ is free if any function $\phi : S \to N$, where $N$ is a $R$-module, can be extended (uniquely) to an $R$-module homomorphism $\psi : M \to N$.

**Proposition 6.14.** For $S = \{m_1, \dots, m_n\} \subseteq M$, the following are equivalent.

(i) $S$ generates $M$ freely.

(ii) $S$ generates $M$, $S$ is $R$-linearly independent.

(iii) Every element of $M$ can be written uniquely as a $R$-linear combination of elements of $S$.

(iv) The $R$-module homomorphism $R^n \twoheadrightarrow M$ is an isomorphism.

**Proposition 6.15** (Invariance of dimension)**.** Suppose $R \neq 0$, $R^m \cong R^n$. Then $m = n$.

*Proof.* Let $I \trianglelefteq R$ be an ideal. For an $R$-module $M$, define

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

Then the quotient $M/IM$ is an $R/I$ module, by $(r + I)(m + IM) = (rm + IM)$. From Zorn's lemma, suppose $I$ is a maximal ideal. Then $R/I$ is a field and we have an isomorphism of $R/I$ modules. The result then follows from the corresponding result for vector spaces. □

# 7 Structure theorem

Let $R$ be a Euclidean domain with Euclidean function $\phi$. Let $A \in \mathrm{Mat}_m(R)$.

**Definition 7.1** (Elementary row operations)
The elementary rop operations are

(i) Add $\lambda \times$ (row $i$) to (row $j$).

(ii) Swap rows $i$ and $j$.

(iii) Multiply row $i$ by $u$, where $u \in R^\times$.

**Proposition 7.2.** Each row operation corresponds to left multiplication by an invertible matrix.

**Remark 7.3.** Column operations are defined similarly.

**Definition 7.4** (Equivalent)

$A, B \in \text{Mat}_m(R)$ are equivalent if we have a sequence of elementary row/column operations taking $A$ to $B$. Equivalently, $B = QAP$, where $P, Q$ invertible.

**Definition 7.5** (Smith normal form)

A diagonal matrix

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

is in Smith Normal Form if each $d_i$ is nonzero, and $d_1 \mid d_2, d_2 \mid d_3, \ldots, d_{t-1} \mid d_t$.

**Theorem 7.6.** $A \in \text{Mat}_{m,n}(R)$ is equivalent to a diagonal matrix in Smith normal form. The diagonal terms $(d_i)$ are called invariant factors.

*Proof.* If $A = 0$ then we are done. Otherwise, we have $a_{ij} \neq 0$. By swapping rows and columns, without loss of generality $a_{11} \neq 0$. Using the Euclidean algorithm with $a_{11}$ and elements of the first row/column, we can make $\phi(a_{11})$ minimal among the first row/column, and divides the first entry in each row/column. Using this, we can clear out the first row/column. If $a_{11} \nmid a_{ij}$ for some $i, j \geq 2$, add the $i$-th row to the first row and repeat. Then we get that $a_{11} \mid a_{ij}$ for all $i, j \geq 2$, the first row/column are zero except at $a_{11}$. Repeating this process for the $(m-1) \times (n-1)$ submatrix in the bottom right gives the required result. □

**Definition 7.7** (Fitting ideal)

The $k$-th Fitting ideal, $\text{Fit}_k(A)$, is the ideal generated by the $k \times k$ minors.

**Lemma 7.8.** If $A$ and $B$ are equivalent, then the Fitting ideals are the same.

*Proof.* Compute for each row/column op. □

**Proposition 7.9.** The invariant factors are unique up to associates.

*Proof.*

$$\text{Fit}_k(A) = (d_1 \ldots d_k)$$

□

**Lemma 7.10.** Let $R$ be a PID. Then any submodule of $R^m$ is generated by at most $m$ elements.

*Proof.* By induction on $m$. Let $N \leq R^m$, and consider the ideal

$$I = \{r \in R : \exists n = (n_1, \dots, n_m) \in N, n_1 = r\}$$

$I$ is a principal ideal, say $I = (a)$. Choose $n \in N$ such that $n = (a, a_2, \dots, a_m)$. For $(r_1, \dots, r_m) \in N$, $r_1 = ra$ for some $r$, so $(r_1, \dots, r_m) - rn = (0, x_2, \dots, x_m) \in N'$, where $N' = N \cap \left(0 \times R^{m-1}\right) \hookrightarrow R^{m-1}$. Then $N = Rn \oplus N'$, and using the induction hypothesis for $N'$ we get the required result. □

**Theorem 7.11.** Let $R$ be an Euclidean domain, $N \leq R^m$. Then there is a free basis $x_1, \dots, x_m$ for $R^m$ such that $N = \langle d_1 x_1, \dots, d_t x_t \rangle$ for some $t \leq m$, and $d_1 \mid d_2, \dots, d_{t-1} \mid d_t$.

*Proof.* By previous lemma, $N$ is generated by at $y_1, \dots, y_n$, where $n \leq m$. Let $A$ have columns $y_i$. Then $A$ is equivalent to a matrix in Smith Normal form. Each row operation corresponds to a change in free basis, and each column operation is a change in the choice of generators of $N$. □

**Theorem 7.12** (Structure theorem)**.** Let $R$ be an Euclidean domain, $M$ a finitely generated $R$-module. Then

$$M \cong \left( \bigoplus_{i=1}^{t} \frac{R}{(d_i)} \right) \oplus R^k$$

where $d_1, \dots, d_t$ nonzero, $d_1 \mid d_2, \dots, d_{t-1} \mid d_t$. The $(d_i)$ are called invariant factors.

*Proof.* Since $M$ is finitely generated, we have $\phi : R^m \twoheadrightarrow M$. Then the first isomorphism theorem gives us that

$$M \cong \frac{R^m}{\ker(\phi)}$$

By the previous theorem, there exists a free basis $(x_1, \dots, x_m)$ for $R^m$ such that $\ker(\phi) = \langle d_1 x_1, \dots, d_t x_t \rangle$, with $d_1 \mid d_2, \dots, d_{t-1} \mid d_t$. Define $d_i = 0$ for $i > t$, then

$$M \cong \frac{\bigoplus_{i=1}^m R}{\bigoplus_{i=1}^m d_i R} \cong \bigoplus_{i=1}^{m} \frac{R}{(d_i)}$$

□

**Corollary 7.13.** A finitely generated torsion free $R$-module over a Euclidean domain is free.

**Theorem 7.14** (Structure theorem for finitely generated abelian groups)**.** Any finitely generated abelian group $G$ is isomorphic to

$$G \cong \left( \bigoplus_{i=1}^{m} \frac{\mathbb{Z}}{d_i \mathbb{Z}} \right) \bigoplus \mathbb{Z}^r$$

*Proof.* Abelian groups are $\mathbb{Z}$-modules. □

**Lemma 7.15.** Let $R$ be a PID, $a, b \in R$ such that $\gcd(a, b) = 1$. Then

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

as $R$-modules.

*Proof.* We have $r, s \in R$ such that $ra + sb = 1$. □

**Theorem 7.16** (Primary decomposition)**.** Let $R$ be a Euclidean domain, $M$ a finitely generated $R$-module. Then

$$M \cong \left( \bigoplus_{i=1}^{k} \frac{R}{(p_i^{n_i})} \right) \oplus R^m$$

where $p_1, \dots, p_k$ primes.

*Proof.* By structure theorem and previous lemma. □

# 8 Jordan normal form

Let $F$ be a field, $V$ be a $F$-vector space.

**Definition 8.1**

Given $\alpha \in \mathrm{End}(V)$, Define the $F[X]$-module $V_\alpha$ to be $V$, with the scalar product given by

$$f \cdot v = f(\alpha)(v)$$

**Lemma 8.2.** If $V$ is finite dimensional, then $V_\alpha$ is finitely generated.

*Proof.* $F \leq F[X]$ as rings, so the basis $v_1, \dots, v_n$ for $V$ still spans $V_\alpha$. □

**Definition 8.3** (Companion matrix)

Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in F[X]$. Then the companion matrix for $f$ is

$$C(f) = \begin{pmatrix} 0 & \dots & 0 & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -a_{n-1} \end{pmatrix}$$

**Proposition 8.4.** Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in F[X]$, and suppose $V_\alpha \cong F[X]/(f)$ as $F[X]$-modules. Then we have an isomorphism of $F$-vector spaces, and $1, X, \dots, X^{n-1}$ forms a basis of $V_\alpha$. Under this basis, $\alpha(x) = X \cdot \alpha$ has matrix $C(f)$.

*Proof.* Compute. □

**Theorem 8.5** (Rational canonical form)**.** Let $\alpha \in \mathrm{End}(V)$, $V$ be a finite dimensional $F$-vector space. Then we have a decomposition of the $F[X]$-module $V_\alpha$ as

$$F[X] \cong \bigoplus_{i=1}^{t} \frac{F[X]}{(f_i)}$$

where $f_1 \mid f_2, \ldots, f_{t-1} \mid f_t$. Moreover, with respect to a suitable basis, $\alpha$ as block diagonal matrix

$$\begin{pmatrix} c(f_1) & & \\ & \ddots & \\ & & c(f_t) \end{pmatrix}$$

*Proof.* Decomposition follows from the structure theorem for finitely generated modules. Furthermore, we can (as in finite dimensions the direct sum is the coproduct *and* the product) decompose $\alpha$ as $\alpha_i \in \mathrm{End}(F[X]/(f_i))$. Then we have a basis for each one where we get the companion matrix for $f_i$. □

**Remark 8.6.** The minimal polynomial of $\alpha$ is $f_t$, the characteristic polynomial is $\prod_{i=1}^{t} f_i$.

**Corollary 8.7** (Cayley-Hamilton)**.** The minimum polynomial of $\alpha$ divides the characteristic polynomial of $\alpha$.

**Corollary 8.8.**

$$\mathrm{Ann}_{F[X]}(V_\alpha) = (f)$$

where $f$ is the minimal polynomial of $\alpha$.

**Lemma 8.9.** The primes (or equivalently irreducibles) in $\mathbb{C}[X]$ are $X - \lambda$.

*Proof.* By fundamental theorem of algebra, if $f \in \mathbb{C}[X]$, then there exists $\lambda$ such that $f(\lambda) = 0$. So $X - \lambda \mid f$. Thus any irreducible element must have degree 1. □

**Definition 8.10** (Jordan block)

A Jordan block $J_n(\lambda) \in \mathrm{Mat}_n(\mathbb{C})$ is a matrix of the form

$$J_n(\lambda) = \begin{pmatrix} \lambda & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

**Remark 8.11.** In Linear Algebra we had the 1s above the main diagonal, it is easy to modify the proof of the Jordan normal form (reverse basis) to get that.

**Proposition 8.12.** Suppose $V_\alpha \cong F[X]/((X-\lambda)^n)$. Then with respect to the basis $1, X-\lambda, \ldots, (X-\lambda)^{n-1}$, $\alpha$ (or the action of multiplying by $X$) has matrix $J_n(\lambda)$.

*Proof.* Consider the action of $X - \lambda$. This has matrix

$$\begin{pmatrix} 0 & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}$$

Then $X = (X - \lambda) + \lambda$ has matrix

$$\begin{pmatrix} \lambda & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \lambda \end{pmatrix}$$

□

**Theorem 8.13 (Jordan normal form).** Let $V$ be a finite dimensional $\mathbb{C}$-vector space, $\alpha \in \mathrm{End}(V)$. Then we have a decomposition of the $\mathbb{C}[X]$ module $V_\alpha$ as

$$V_\alpha \cong \bigoplus_{i=1}^{t} \frac{\mathbb{C}[X]}{((X-\lambda_i)^{n_i})}$$

where $\lambda_i \in \mathbb{C}$ not necessarily distinct. Furthermore, there exists a basis for $V$ such that $\alpha$ has block diagonal matrix

$$\begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_t}(\lambda_t) \end{pmatrix}$$

*Proof.* Applying the primary decomposition theorem we get the decomposition of $V_\alpha$. Restricting $\alpha$ to each part and using the previous proposition we get the required result. □

**Remark 8.14.** By considering generalised eigenspaces $\ker((\alpha - \lambda\,\mathrm{id})^m)$, the Jordan blocks are determined up to reordering.

**Proposition 8.15.** The minimal polynomial for $\alpha$ is

$$\prod_\lambda (X-\lambda)^{c_\lambda}$$

and the characteristic polynomial is

$$\prod_\lambda (X-\lambda)^{a_\lambda}$$

where $c_\lambda$ is size of the largest Jordan block with eigenvalue $\lambda$, and $a_\lambda$ is the sum of the sizes of the $\lambda$ values.

**Proposition 8.16.** The number of $\lambda$-blocks is $\dim(V_\lambda)$, or the geometric multiplicity of the eigenvalue $\lambda$.