IB Groups, Rings & Modules

Ishan Nath, Lent 2022

Based on Lectures by Dr. Rong Zhou

April 30, 2022

Contents

I Groups **3**

1 Revision and Basic Theory **3**
1.1 Basic Definitions . . . 3
1.2 Homomorphisms . . . 5
1.3 Isomorphism Theorems . . . 5
1.4 Simple Groups . . . 7

2 Group Actions **9**
2.1 Definitions and Permutation Groups . . . 9
2.2 Orbits and Stabilizers . . . 10
2.3 Examples of Group Actions . . . 10

3 Alternating Groups **13**
3.1 Simplicity of A_n . . . 14

4 p-groups and p-subgroups **15**
4.1 Sylow Theorems . . . 16

5 Matrix Groups **19**

6 Finite Abelian Groups **21**

II Rings **22**

7 Definitions and Examples **22**

8 Homomorphisms, Ideals and Quotients **25**
8.1 Definitions . . . 25
8.2 Isomorphism Theorems . . . 27

9 Integral Domains and Ideals **31**
9.1 Integral Domains . . . 31
9.2 Maximal Ideals . . . 33
9.3 Prime Ideals . . . 34

10 Factorisation in Integral Domains **35**
10.1 Principal Ideal Domains . . . 36
10.2 Euclidean Domains . . . 37

10.3 Unique Factorisation Domains 39

11 Factorisation in Polynomial Rings **41**
11.1 Gauss' Lemma 42
11.2 Applications 43

12 Algebraic Integers **46**
12.1 Primes in $\mathbb{Z}[i]$ 46
12.2 Algebraic Numbers 48

13 Noetherian Rings **50**
13.1 Definitions 50
13.2 Hilbert's Basis Theorem 51

III Modules **53**

14 Definitions and Examples **53**
14.1 Basic Definitions 53
14.2 Isomorphism Theorems 55

15 Direct Sums and Free Modules **57**

16 The Structure Theorem and Applications **60**
16.1 Smith Normal Form 60
16.2 Structure Theorem and Corollaries 62
16.3 Rational Canonical Form and Jordan Normal Form 64

17 Modules over PID's **69**

Index **70**

Part I

Groups

1 Revision and Basic Theory

1.1 Basic Definitions

Definition 1.1. A **group** is a pair $(G, \cdot)$, where G is a set and $\cdot : G \times G \to G$ is a binary operation satisfying:

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- There exists $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$.
- For all $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Remark.

(i) In addition to check $\cdot$ is well defined, we also need to check **closure**, i.e. $g \cdot h \in G$.

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

Definition 1.2. A subset $H \subseteq G$ is a **subgroup** (written $H \leq G$) if it is closed under $\cdot$, and $(H, \cdot)$ is a group.

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

Examples:

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

(ii) Cyclic and dihedral groups. C_n is the cyclic group of order n, and D_{2n} is the dihedral group of order $2n$, where $C_n \leq D_{2n}$.

(iii) **Abelian groups** satisfy $gh = hg$ for every $g, h \in G$.

(iv) Symmetric and alternating groups. S_n is the permutations of $\{1, \ldots, n\}$ under composition, and $A_n \leq S_n$ is the subgroup of even permutations.

(v) The quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

(vi) General and special linear groups. $GL_n(\mathbb{R})$ is the set of invertible $n \times n$ matrices over $\mathbb{R}$ under matrix multiplication, and $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ is the subgroup of matrices with determinant 1.

Definition 1.3. The **direct product** of groups G and H is the set $G \times H$ with operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2).$$

Let $H \leq G$. The left cosets of H in G are the sets $gH = \{gh \mid h \in H\}$. These partition G, and each has the same cardinality.

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

Remark. We can also copy this with right cosets. Lagrange's implies the number of left cosets equals the number of right cosets.

Definition 1.4. Let $g \in G$. If there exists $n \geq 1$ such that $g^n = 1$, then the least such n is the order of g. Otherwise g has infinite order.

Remark. If g has order d, then;

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

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

Definition 1.5. A subgroup $N \leq G$ is **normal** if $g^{-1}Ng = N$ for all $g \in G$. We write $N \lhd G$.

Proposition 1.1. *If $H \lhd G$ 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 need to check $\cdot$ is well defined. Suppose $g_1H = g_1'H$ and $g_2H = g_2'H$. Then $g_1' = g_1h_1$ and $g_2' = g_2h_2$ for some $h_1, h_2 \in H$. Therefore,

$$g_1'g_2' = g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2 = g_1g_2h,$$

where $h = (g_2^{-1}h_1g_2)h_2 \in H$ by our normality criterion. Therefore, $g_1'g_2'H = g_1g_2H$.

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

1.2 Homomorphisms

Definition 1.6. For groups G, H, a function $\phi : G \to H$ is a **group homomorphism** if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

It has kernel

$$\mathrm{Ker}(\phi) = \{g \in G \mid \phi(g) = e_H\} \leq G$$

and image

$$\mathrm{Im}(\phi) = \{\phi(g) \mid g \in G\} \leq H.$$

In fact, $\mathrm{Ker}(\phi) \lhd G$, since if $h \in \mathrm{Ker}(\phi)$ and $g \in G$, then

$$\phi(g^{-1}hg) = \phi(g^{-1})\phi(h)\phi(g) = \phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e_G) = e_H.$$

Therefore $g^{-1}hg \in \mathrm{Ker}(\phi)$.

Definition 1.7. An isomorphism of groups is a group homomorphism that is also a bijection. We say G and H are isomorphic (written $G \cong H$) if there exists an isomorphism $\phi : G \to H$.

It can be shown that $\phi^{-1} : H \to G$ is also a group homomorphism.

1.3 Isomorphism Theorems

Theorem 1.2 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a group homomorphism. Then* $\mathrm{Ker}(\phi) \lhd G$*, and*

$$G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi).$$

Proof: Let $K = \mathrm{Ker}(\phi)$. We have already shown K is normal in G, so we only need to show $G/K \cong \mathrm{Im}(\phi)$. Define

$$\begin{aligned} \Phi : G/K &\to \mathrm{Im}(\phi) \\ gK &\mapsto \phi(g) \end{aligned}$$

We will show Φ is an isomorphism. To show it is well-defined and injective,

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

To show it is a group homomorphism,

$$\Phi(g_1Kg_2K) = \Phi(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \Phi(g_1K)\Phi(g_2K).$$

Finally, it is surjective as if $x \in \mathrm{Im}(\phi)$, then $x = \phi(g)$ for some $g \in G$, so $x = \Phi(gK)$.

Example: Consider $\phi : \mathbb{C} \to \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, given by $z \mapsto e^z$. Then,

$$\begin{aligned} \mathrm{Ker}(\phi) &= \{z \in \mathbb{C} \mid e^z = 1\} = 2\pi i\mathbb{Z}, \\ \mathrm{Im}(\phi) &= \mathbb{C}^\times. \end{aligned}$$

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

Theorem 1.3 (Second Isomorphism Theorem)**.** *Let $H \leq G$ and $K \lhd G$. Then $HK = \{hk \mid h \in H, k \in K\} \leq G$, $H \cap K \lhd H$, and*

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

Proof: Let $h_1k_1, h_2k_2 \in HK$. Then,

$$h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_2^{-1}(h_2k_1k_2^{-1}h_2^{-1}) \in HK,$$

since $K \lhd G$. Thus $HK \leq G$. Consider

$$\begin{aligned} \phi : H &\to G/K \\ h &\mapsto hK \end{aligned}$$

This is the composition of $H \to G$ and quotient map $G \to G/K$, thus ϕ is a group homomorphism.

$$\begin{aligned} \mathrm{Ker}(\phi) &= \{h \in H \mid hK = K\} = H \cap K \lhd H, \\ \mathrm{Im}(\phi) &= \{hK \mid h \in H\} = HK/K. \end{aligned}$$

Therefore we are done by the first isomorphism theorem.

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

$$\begin{aligned} \{\text{subgroups of } G/K\} &\mapsto \{\text{subgroups of } G \text{ containing } K\}, \\ X &\mapsto \{g \in G : gK \in X\}, \\ H/K &\mapsto H. \end{aligned}$$

This map takes normal subgroups of G/K to normal subgroups of G containing K.

Theorem 1.4 (Third Isomorphism Theorem)**.** *Let $K \leq H \leq G$ be normal subgroups of G. Then*

$$(G/K)/(H/K) = G/H.$$

Proof: Define

$$\begin{aligned} \phi : G/K &\to G/H \\ gK &\mapsto gH \end{aligned}$$

If $g_1K = g_2K$, then $g_2^{-1}g_1 \in K \leq H$, so $g_1H = g_2H$. Therefore ϕ is well-defined, and is a surjective group homomorphism with kernel H/K, so we are finished by the first isomorphism theorem.

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

1.4 Simple Groups

Definition 1.8. A group G is **simple** if it has no non-trivial proper normal subgroups.

We do not consider the trivial group to be a simple group.

Lemma 1.1. *Let G be an abelian group. G is simple iff $G \cong C_p$ for some prime p.*

Proof: Let $H \leq C_p$. Lagrange's theorem says $|H| \mid |C_p| = p$, so $|H| = 1$ or p. But this implies H is either the trivial group, or C_p, thus C_p is simple.

Let $1 \neq g \in G$. Then G contains the subgroup $\langle g \rangle$, which is normal since G is normal. Since G is simple, $\langle g \rangle = G$. If G is infinite, then $G \cong (\mathbb{Z}, +)$, but then $2\mathbb{Z}$ is a normal subgroup.

Otherwise $G \cong C_n$ for some n. If $m \mid n$, then $g^{n/m}$ generates a subgroup of order m. So if C_n is simple, then the only factors of n can be 1 and n, which implies n is prime.

Lemma 1.2. *If G is a finite group, then G has a composition series*

$$1 \cong G_0 \lhd G_1 \lhd \ldots \lhd G_n = G,$$

with each quotient G_i/G_{i-1} simple. (Note G_i may not be normal in G).

Proof: We induct on $|G|$. If $|G| = 1$, we are done. Otherwise, if $|G| > 1$, let G_{m-1} be a normal subgroup of largest possible order not equal to G. Since normal subgroups of G/G_{m-1} biject with normal subgroups of G containing G_{m-1}, we get that G/G_{m-1} is simple, and we can induct.

2 Group Actions

2.1 Definitions and Permutation Groups

Definition 2.1. For a set X, let $\mathrm{Sym}(X)$ be the group of all bijections $X \to X$ under composition.

Definition 2.2. A group G is a permutation group of degree n if $G \leq \mathrm{Sym}(X)$ with $|X| = n$.

For example, S_n is a permutation group of degree n, as is A_n and D_{2n}.

Definition 2.3. An action of a group G on a set X is a function $* : G \times X \to X$, satisfying

(i) $e * x = x$,

(ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$.

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 $g \in G$, let

$$\begin{aligned} \phi_g : X &\to X \\ x &\mapsto gx \end{aligned}$$

We have

$$\phi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \phi_{g_1}(\phi_{g_2}(x)).$$

Thus $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}$. In particular, $\phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \phi_e = \mathrm{id}_X$. Thus $\phi_g \in \mathrm{Sym}(X)$. Define

$$\begin{aligned} \Phi : G &\to \mathrm{Sym}(X) \\ g &\mapsto \phi_g \end{aligned}$$

This is a group homomorphism from the above. Conversely, let $\phi : G \to \mathrm{Sym}(X)$ be a group homomorphism. Define

$$\begin{aligned} * : G \times X &\to X \\ (g, x) &\mapsto \phi(g)(x) \end{aligned}$$

Then $e * x = \phi(e)(x) = \mathrm{id}(x) = x$, and

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

Definition 2.4. We say $\phi : G \to \mathrm{Sym}(X)$ is a permutation representation of G.

2.2 Orbits and Stabilizers

Definition 2.5. Let G act on a set X.

(i) The orbit of $x \in X$ is $\mathrm{Orb}_G(x) = \{g * x \mid g \in G\} \subseteq X$.

(ii) The stabilizer of $x \in X$ is

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

Theorem 2.1 (Orbit-Stabilizer Theorem)**.** *There is a bijection* $\mathrm{Orb}_G(x) \leftrightarrow (G : G_x)$*. In particular, if* G *is finite, then*

$$|G| = |\mathrm{Orb}_G(x)||G_x|.$$

For example, if G is the group of symmetries of a cube, and X is the set of vertices, then $|\mathrm{Orb}_G(x)| = 8$, $|G_x| = 6$, so $|G| = 48$.

Remark.

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

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

(iii) $G_{g*x} = gG_x g^{-1}$, so if $x, y \in X$, then their stabilizers are conjugate.

2.3 Examples of Group Actions

(i) Let G act on itself by left multiplication, i.e. $g * x = gx$. The kernel of this action is $\{g \in G \mid gx = x \,\forall x\} = \{e\}$. Thus G has an injection into $\mathrm{Sym}(G)$, proving the following:

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

(ii) Let $H \leq G$, and G acts on $(G : H)$ by left multiplication, i.e. $g * xH = gxH$. This action is transitive, with

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

Thus $\text{Ker}(\phi) = \bigcap_{x \in G} xHx^{-1}$, which is the largest normal subgroup of G that is contained in H.

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

Proof: Let G act on $X = (G : H)$ by left multiplication, and $\phi : G \to \text{Sym}(X)$ be the associated permutation representation.

As G is simple, $\text{Ker}(\phi) = e$ or G. However, if $\text{Ker}(\phi) = G$, then $\text{Im}(\phi) = \text{id}$, but this is a contradiction as we know G acts transitively on X and $|X| > 1$. Thus $\text{Ker}(\phi) = e$ and $G \cong \text{Im}(\phi) \leq S_n$.

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

$$G \cap A_n \lhd G \text{ and } G/G \cap A_n \cong GA_n/A_n \leq S_n/A_n \cong C_2.$$

Since G is simple, $G \cap A_n = e$ or G. However if $G \cap A_n = e$, then $G \leq C_2$, which is abelian. Thus, we have $G \cap A_n = G$, meaning $G \leq A_n$.

Finally, if $n \leq 4$, then A_n has no non-abelian simple subgroups.

(iii) Let G act on itself by conjugation, i.e. $g * x = gxg^{-1}$. In this case,

$$\text{Orb}_G(x) = \{gxg^{-1} \mid g \in G\} = \text{ccl}_G(x),$$

the **conjugacy class** of x in G. The stabilizer is

$$G_x = \{g \in G \mid gx = xg\} = C_G(x) \leq G,$$

the **centralizer** of x in G. Finally,

$$\ker(\phi) = \{g \in G \mid gx = xg\} = Z(G)$$

is the **centre** of G.

Remark. The function ϕ mapping $h \mapsto ghg^{-1}$ satisfies

$$\phi(g)(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \phi(g)(h_1)\phi(g)(h_2).$$

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

Definition 2.6. We define

$$\mathrm{Aut}(G) = \{f : G \to G \mid f \text{ is an isomorphism}\}.$$

Then $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ and $\phi : G \to \mathrm{Sym}(G)$ has image in $\mathrm{Aut}(G)$.

(iv) Let X be the set of all subgroups of G then G acts on X be conjugation, i.e.

$$g * H = gHg^{-1}.$$

The stabilizer of H is

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

the **normalizer** of H in G. This is the largest subgroup of G containing H as a normal subgroup. In particular,

$$H \lhd G \iff N_G(H) = G.$$

3 Alternating Groups

We have seen that in S_n, elements are conjugate if and only if they have the same cycle type. For example, in S_5,

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

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

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

Otherwise,

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

In S_5, the double transpositions and 3-cycles commute with transpositions, so their conjugacy class stay the same. However the 5-cycles only commutes with even elements, so its conjugacy class splits.

Thus A_5 has conjugacy classes of sizes $1, 15, 20, 12, 12$. If $H \lhd A_5$, then H is a union of conjugacy classes, so

$$|H| = 1 + 15a + 20b + 12c, \quad a, b \in \{0, 1\},\ c \in \{0, 1, 2\},$$

and $|H| \mid 60$ by Lagrange's. Thus $|H| = 1$ or 60, i.e. A_5 is simple.

Lemma 3.1. *A_n is generated by 3-cycles.*

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

For a, b, c, d distinct, two transpositions can be written as

$$\begin{cases} (a\ b)(b\ c) = (a\ b\ c) \\ (a\ b)(c\ d) = (a\ c\ b)(a\ c\ d) \end{cases}$$

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

Proof: We claim that every 3-cycle in A_n is conjugate to (1 2 3). Indeed if $(a\ b\ c)$ is a 3-cycle then

$$(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$$

for some $\sigma \in S_n$. If $\sigma \notin A_n$, then replace σ by $\sigma(4\ 5)$.

3.1 Simplicity of A_n

Theorem 3.1. *A_n is simple for all $n \geq 5$.*

Proof: Let $\mathrm{id} \neq N \lhd A_n$. It suffices to show that N contains a 3-cycle from the previous lemmas. Take $\mathrm{id} \neq \sigma \in N$ and with σ as a product of disjoint cycles.

Case 1: σ contains a cycle of length $r \geq 4$. Say

$$\sigma = (1\ 2\ \ldots\ r)\tau.$$

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

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

This implies N contains a 3-cycle.

Case 2: σ contains two 3-cycles. Say

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

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

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

Now we are done by case 1.

Case 3: σ contains two 2-cycles. Say

$$\sigma = (1\ 2)(3\ 4)\tau.$$

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

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

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

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

Thus N contains a 3-cycle.

It remains to consider σ with at most 1 3-cycle, and at most 1 transposition. However, if it has 1 transposition, it is odd, so σ must be a 3-cycle.

4 p-groups and p-subgroups

Definition 4.1. Let p be a prime. A finite group G is a p-group if $|G| = p^n$, $n \geq 1$.

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

Proof: For $g \in G$, we have

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

so each conjugacy class has size a power of p. Since G is a disjoint union of conjugacy classes,

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

Therefore,

$$0 = |Z(G)| \pmod{p},$$

and hence $Z(G) \neq 1$.

Corollary 4.1. *The only simple p-group is C_p.*

Proof: Let G be a simple p-group. Since $Z(G) \lhd G$, we have $Z(G) = 1$ or G. But the first case is impossible, so $Z(G) = G$, meaning G is abelian, so $G \cong C_p$.

Corollary 4.2. *Let G be a p-group of order p^n. Then G has a subgroup of order p^r for all $0 \leq r \leq n$.*

Proof: Consider the composition series of G:

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

with each G_i/G_{i-1} simple. However since G is a p-group, G_i/G_{i-1} is a p-group, so $G_i/G_{i-1} \cong C_p$. Then by induction, $|G_i| = p^i$, and $m = n$.

Lemma 4.1. *For G a group, if $G/Z(G)$ is cyclic, then G is abelian (so in fact $G/Z(G) \cong 1$).*

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

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

Then,

$$g^{r_1} z_1 g^{r_2} z_2 = g^{r_1} g^{r_2} z_1 z_2 = g^{r_2} g^{r_1} z_2 z_1 = g^{r_2} z_2 g^{r_1} z_1.$$

Therefore any two elements of the group commute, so G is abelian.

Corollary 4.3. *If $|G| = p^2$, then G is abelian.*

Proof: We have either $|Z(G)| = 1, p$ or p^2. However the centre is nontrivial, so $|Z(G)| \neq 1$. If $|Z(G)| = p$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic, and $|Z(G)| = |G|$, contradiction. Therefore $|Z(G)| = p^2$, so G is abelian.

4.1 Sylow Theorems

Theorem 4.2 (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 $\mathrm{Syl}_p(G) = \{P \leq G \mid |P| = p^a\}$ *is non-empty.*

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

(iii) $n_p = |\mathrm{Syl}_p(G)|$ *satisfies*

$$n_p \equiv 1 \pmod{p} \text{ and } n_p \mid |G|$$

and so $n_p \mid m$.

Corollary 4.4. *If $n_p = 1$, then the unique Sylow p-subgroup is normal.*

This follows by letting $g \in G$ and $P \in \mathrm{Syl}_p(G)$. Then $gPg^{-1} \in \mathrm{Syl}_p(G)$, meaning $gPg^{-1} = P$. Thus $P \lhd G$.

Examples:

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

Let $|G| = 132$. Then $n_{11} \equiv 1 \pmod 1$1 and $n_{11} \mid 12$. Thus $n_{11} = 1$ or 12. If G is simple, then $n_{11} \neq 1$, so it must be equal to 12. Now $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 44$, so $n_3 = 1$, 4 or 22. Note $n_3 \neq 1$, and if $n_3 = 4$, then letting G act on $\mathrm{Syl}_3(G)$ by conjugation gives a group homomorphism ϕ. Thus,

$$\mathrm{Ker}(\phi) \lhd G \implies \mathrm{Ker}(\phi) = 1 \text{ or } G.$$

However if $\mathrm{Ker}(\phi) = G$ then $\mathrm{Im}(\phi) = \mathrm{id}$, which is a contradiction to the second Sylow theorem. Therefore $\mathrm{Ker}(\phi) = 1$, so $G \leq S_4$, which is a contradiction as $|G| > |S_4|$.

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

Proof of Sylow Theorems:

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

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

From this representation, we can see that $|\Omega|$ is coprime to p. Let G act on $|\Omega|$ by left multiplication, i.e. for $g \in G$ and $X \in \Omega$,

$$g * X = \{gx \mid x \in X\} \subset \Omega.$$

For any $X \in \Omega$ we have

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

However since $|\Omega|$ is coprime to p, there exists X such that $|\mathrm{Orb}_G(X)|$ is coprime to p, and thus $p^a \mid |G_X|$. On the other hand, if $g \in G$ and $x \in X$ then $g \in (gx^{-1}) * X$ and hence

$$G = \bigcup_{g \in G} g * X = \bigcup_{Y \in \mathrm{Orb}_G(X)} Y.$$

Hence $|G| \leq |\mathrm{Orb}_G(X)| \cdot |X|$, so

$$|G_X| = \frac{|G|}{|\mathrm{Orb}_G(X)|} \leq |X| = p^a.$$

Combining these facts, $|G_X| = p^a$, i.e. $G_X \in \mathrm{Syl}_P(G)$.

(ii) We prove a stronger result.

Lemma 4.2. *If $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is a p-subgroup, then $Q \leq gPg^{-1}$ for some $g \in G$.*

To prove this, let Q act on the set of left cosets $(G : P)$ by left multiplication, i.e. $q * gP = qgP$. By orbit-stabilizer, each orbit has size $|Q|$, so either 1 or a multiple of p. But since $|(G : P)|$ is coprime to p, there is an orbit of size 1, i.e.

$$qgP = gP \quad \forall q \in Q \implies g^{-1}qg \in P \quad \forall q \in Q.$$

Thus $Q \leq gPg^{-1}$, as required.

(iii) Let G act on $\mathrm{Syl}_p(G)$ by conjugation. From the above, this action is transitive, so by orbit-stabilizer,

$$n_p = |\mathrm{Syl}_p(G)| \mid |G|.$$

Now let $P \in \mathrm{Syl}_p(G)$. Then P acts on $\mathrm{Syl}_p(G)$ by conjugation. The orbits have size dividing $|P|$, so either 1 or a multiple of p. Since P is fixed by this action, it suffices to show that $\{P\}$ is the unique orbit of size 1. If $\{Q\}$ is an orbit of size 1, then P normalizes Q, hence $P \leq N_G(Q)$. But then P and Q are both Sylow p-subgroups of $N_G(Q)$, hence they are conjugate, but since $Q \lhd N_G(Q)$, $P = Q$.

5 Matrix Groups

If F is a field, let $GL_n(F)$ denote the $n \times n$ matrices with elements in F, with non-zero determinant. Then

$$SL_n(F) = \ker(GL_n(F) \to F^\times)$$

under the determinant operation. Hence $SL_n(F) \lhd GL_n(F)$. Let $Z \lhd GL_n(F)$ be the subgroup of scalar matrices, then define

$$PGL_n(F) = GL_n(F)/Z.$$

We can then define

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

If $G = GL_n(\mathbb{Z}/p\mathbb{Z})$, then a list of n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ are the columns of some $A \in G$ if and only if they are linearly independent. Hence

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

So the Sylow p-subgroups have size $p^{\binom{n}{2}}$, Let U be the set of upper-triangular matrices with 1's on the diagonal. Then $U \in \mathrm{Syl}_p(G)$, since there $\binom{n}{2}$ entries, and each can take p values.

Just as $PGL_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ via Möbius transformations, $PGL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$ via

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

Since scalar matrices act trivially, we obtain an action of $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 5.1. *The permutation representation*

$$PGL_2(\mathbb{Z}/p\mathbb{Z}) \to S_{p+1}$$

is injective (in fact an isomorphism if $p = 2$ or 3).

Proof: Suppose

$$\frac{az + b}{cz + d} = z$$

for all $z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. Then $z = 0$ gives $b = 0$, $z = \infty$ gives $c = 0$, and $z = 1$ gives $a = d$, hence the matrix is scalar, so trivial in $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 5.2. *If p is an odd prime, then*

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

Proof: Note $|GL_2(\mathbb{Z}/p\mathbb{Z})| = p(p^2-1)(p-1)$. The homomorphism $GL_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ is surjective. Thus $|SL_2(\mathbb{Z}/p\mathbb{Z})| = p(p-1)(p+1)$. Note

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in SL_2(\mathbb{Z}/p\mathbb{Z}) \iff \lambda = \pm 1 \pmod{p}.$$

Thus $Z \cap SL_2(\mathbb{Z}/p\mathbb{Z}) = \{\pm I\}$, so modding out by Z,

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

Example: If we let $G = PSL_2(\mathbb{Z}/5\mathbb{Z})$, then $|G| = 60$. Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$. This is injective from lemma 5.1. Thus $\phi : G \to S_6$ is injective. In fact, $\mathrm{Im}(\phi) \leq A_6$, as if $\psi = \mathrm{sgn} \circ \phi$, then

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

for odd m. Thus it suffices to show $\psi(g) = 1$ for all $g \in G$ with order a power of 2. However every such g belongs to a Sylow 2-subgroup, so it suffices to show $\psi(H) = 1$ for a Sylow 2-subgroup H, since all Sylow 2-subgroups are conjugate. Take

$$H = \langle \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle \leq G.$$

Now compute

$$\phi\left(\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\right) = (1\ 4)(2\ 3) \quad z \mapsto -z,$$
$$\phi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = (0\ \infty)(1\ 4) \quad z \mapsto -\frac{1}{z}.$$

Thus $\psi(H) = 1$. Now we know that if $G \leq A_6$ and $|G| = 60$, then $G \cong A_5$.

Remark.

- $PSL_n(\mathbb{Z}/p\mathbb{Z})$ is a simple group for all $n \geq 2$, and p a prime, known as the finite groups of Lie type.
- The smallest non-abelian simple groups are $A_5 \cong PSL_2(\mathbb{Z}/5\mathbb{Z})$ with order 60 and $PSL_2(\mathbb{Z}/7\mathbb{Z}) \cong GL_3(\mathbb{Z}/2\mathbb{Z})$ with order 168.

6 Finite Abelian Groups

The main theorem is as follows:

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

Note such an isomorphism is not unique.

Lemma 6.1. *If $m, n \in \mathbb{N}$ are coprime, then $C_m \times C_n \cong C_{mn}$.*

Using this, we can edit our first theorem to get uniqueness.

Corollary 6.1. *Let G be a finite abelian group. Then*

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

where n_i is a prime power.

We can also refine theorem 6.1 as follows:

Theorem 6.2. *Let G be a finite abelian group. Then*

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

for some $d_1 \mid d_2 \mid \cdots \mid d_l$.

Remark. The integers $n_1, \ldots, n_k$ are unique (up to ordering), and $d_1, \ldots, d_l$ are unique (assuming $d_1 > 1$).

Definition 6.1. The **exponent** of a group G is the least integer $n \geq 1$ such that $g^n = 1$ for all $g \in G$, i.e. the lowest common multiple of all the orders of the elements of G.

In A_4, the exponent is 6, but there is no element of order 6.

Corollary 6.2. *Every finite abelian group contains an element whose order is the exponent of the group.*

This is direct from theorem 6.2.

Part II

Rings

7 Definitions and Examples

Definition 7.1. 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. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, and there exists $1 \in R$ such that $x \cdot 1 = 1 \cdot x = x$.

We say that R is a **commutative ring** if $x \cdot y = y \cdot x$ for all $x, y \in R$. We will only consider commutative rings.

(iii) Addition distributes over multiplication: $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

Remark.

(i) As in the case of groups, we need to check closure.

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

(iii) $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, so $0 \cdot x = 0$, and similarly $x \cdot 0 = 0$.

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

Definition 7.2. A subset $S \subseteq R$ is a subring (written $S \leq R$) if it is a ring under $+$ and $\cdot$, with the same identity elements 0 and 1.

Examples:

(i) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(ii) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$.

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

(iv) $\mathbb{Z}/n\mathbb{Z}$.

(v) For R, S rings, the ring $R \times S$ is a ring, where

- $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$.
- $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$.
- $0_{R\times S} = (0_R, 0_S)$ and $1_{R\times S} = (1_R, 1_S)$. (Note $R \times \{0\}$ is not a subring of $R \times S$).

(vi) For R a ring, a polynomial f over R is an expression

$$f = a_0 + a_1 X + \cdots + a_n X^n, \quad a_i \in R.$$

The degree of f is the largest $n \in \mathbb{N}$ such that $a_n \neq 0$. We write $R[X]$ for the set of all polynomials over R. Then if $g = b_0 + b_1 X + \cdots + b_n X^n$, then

$$f + g = \sum_i (a_i + b_i) X^i,$$

$$f \cdot g = \sum_i \left(\sum_j^i a_j b_{i-j} \right) X^i.$$

Then $R[X]$ is a ring with identities 0_R and 1_R, which are constant polynomials. Note we can identify R with the subring of $R[X]$ of constant polynomials.

Definition 7.3. An element $r \in R$ is a **unit** if it has an inverse under multiplication, i.e. there exists $s \in R$ such that $s \cdot r = 1$. The units in R form a group $(R^\times, \cdot)$ under multiplication.

For example,

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

Definition 7.4. A **field** is a ring with $0 \neq 1$, such that every non-zero element is a unit.

For example, we have $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$ for p prime.

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

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

$$f(x) = q(x)g(x) + r(x),$$

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

Proof: We will induct on $n = \deg(f)$. Write

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0,$$
$$g(X) = b_n X^m + b_{m-1} X^{m-1} + \cdots + b_0.$$

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

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

The coefficient of X^n in f_1 vanishes, and so $\deg(f_1) < n$. By the inductive hypothesis, there exists $q_1, r \in R[X]$ where

$$f_1(X) = q_1(X) g(X) + r(X),$$

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

$$f(x) = (q_1(X) + a_n b_m^{-1} X^{n-m}) g(X) + r(X).$$

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

Further Examples:

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

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

Further interesting examples appear as subrings, for example continuous functions $\mathbb{R} \to \mathbb{R}$, and polynomial functions $\mathbb{R} \to \mathbb{R} = \mathbb{R}[X]$.

(viii) Power series ring:

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

(ix) Laurent polynomials:

$$R[X, X^{-1}] = \left\{ \sum_{i \in \mathbb{Z}} a_i X_i \mid a_i \in R, a_i \neq 0 \text{ for finitely many } i \right\}.$$

8 Homomorphisms, Ideals and Quotients

8.1 Definitions

Definition 8.1. Let R and S be rings. A function $\phi : R \to S$ is called a ring homomorphism if

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$,

(ii) $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$,

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

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

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

Lemma 8.1. *A ring homomorphism $\phi : R \to S$ is injective if and only if* $\mathrm{Ker}(\phi) = \{0_R\}$.

This follows by taking the corresponding result of groups on the additive group of R.

Definition 8.2. A subset $I \subseteq R$ is an **ideal**, written $I \lhd R$, if

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

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

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

Lemma 8.2. *If $\phi : R \to S$ is a ring homomorphism, then* $\mathrm{Ker}(\phi)$ *is an ideal of R.*

Proof: Since ϕ is a group homomorphism, $\mathrm{Ker}(\phi)$ is a subgroup of $(R, +)$. Now if $r \in R$, $x \in \mathrm{Ker}(\phi)$,

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

Thus $rx \in \mathrm{Ker}(\phi)$.

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

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

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

for $n \geq 0$.

Proof: Certainly these are all ideals. Now let $I \lhd \mathbb{Z}$ be a non-zero ideal, and let n be the smallest positive integer in I. Then $n\mathbb{Z} \subseteq I$.

If $m \in I$ with $m = qn + r$, $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Then $r = m - qn \in I$, which contradicts our choice of n unless $r = 0$. Thus $m = qn$ for all $m \in I$, i.e.

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

Definition 8.3. For $a \in R$, write $(a) = \{ra \mid r \in R\} \lhd R$. This is the **ideal generated by** a. More generally, if $a_1, \ldots, a_n \in R$, we write

$$(a_1, \ldots, a_n) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\} \lhd R.$$

Definition 8.4. Let $I \lhd R$. We say I is **principal** if $I = (a)$ for $a \in R$.

Theorem 8.1. *If $I \lhd R$, then the set R/I of cosets of I in $(R, +)$ forms a ring (called the quotient ring) with the operations*

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

(ii) $(r_1 + I) \cdot (r_2 + I) = r_1r_2 + I$,

(iii) $0_{R/I} = 0_R + I = I$ *and* $1_{R/I} = 1_R + I$.

Moreover, the map

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

is a ring homomorphism (called the quotient map) with kernel I.

Proof: We already know $(R/I, +)$ is a group. Now if $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$, then $r_1' = r_1 + a_1$, $r_2' = r_2 + a_2$ for $a_1, a_2 \in I$. Then,

$$r_1'r_2' = (r_1 + a_1)(r_2 + a_2) = r_1r_2 + r_1a_2 + a_1r_2 + a_1a_2.$$

Thus $r_1r_2 + I = r_1'r_2' + I$. The remaining properties follow from those for R, and the last part follows from these properties.

Examples:

(i) $n\mathbb{Z} \lhd \mathbb{Z}$, with quotient ring $\mathbb{Z}/n\mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z}$ has elements

$$\{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Addition and multiplication are carried out modulo n.

(ii) Consider $(X) \lhd \mathbb{C}[X]$. These are the set of polynomials with constant term 0. Then $f(X) + (X) = a_0 + (X)$. There is a bijection

$$\begin{aligned} \mathbb{C}[X]/(X) &\to \mathbb{C} \\ f(X) + (X) &\mapsto f(0) \end{aligned}$$

These maps are ring homomorphisms, thus $\mathbb{C}[X]/(X) \cong \mathbb{C}$.

(iii) Consider $(X^2+1) \lhd \mathbb{R}[X]$. By proposition 7.1, $f(X) = q(X)(X^2+1) + r(X)$, with $\deg(r) < 2$, i.e. r is affine. Thus

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

These representatives are unique, by subtracting and looking at degrees. Now consider the bijection

$$\begin{aligned} \phi : \mathbb{R}[X]/(X^2+1) &\to \mathbb{C} \\ a + bX + (X^2+1) &\mapsto a + bi \end{aligned}$$

This is a bijection, so we show ϕ is a ring homomorphism. It preserves addition and maps $1 + (X^2+1)$ to 1. Now

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

so ϕ is a ring isomorphism.

8.2 Isomorphism Theorems

Theorem 8.2 (First Isomorphism Theorem)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then,* $\mathrm{Ker}(\phi) \lhd R$, $\mathrm{Im}(\phi) \leq S$, *and*

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

Proof: We have already seen $\mathrm{Ker}(\phi) \lhd R$ and $\mathrm{Im}(\phi)$ is a subgroup of $(S, +)$. To show it is a subring, we need to show it is closed under multiplication and contains 1. Now,

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

and $1_S = \phi(1_R) \in \mathrm{Im}(\phi)$. Let $K = \mathrm{Ker}(\phi)$, and define

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

By the 1st isomorphism theorem for groups, this is well-defined, a bijection and a group homomorphism under addition. Also

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

and

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

Thus Φ is a ring isomorphism.

Theorem 8.3 (Second Isomorphism Theorem)**.** *Let $R \leq S$ and $J \lhd S$. Then $R \cap J \lhd R$, $R + J = \{r + j \mid r \in R, j \in J\} \leq S$ and*

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

Proof: By the second isomorphism theorem for groups, $R + J$ is a subgroup of $(S, +)$, and also $1_S \in R + J$. Now for $r_1, r_2 \in R$, $j_1, j_2 \in J$,

$$(r_1 + j_1)(r_2 + j_2) = r_1 r_2 + r_1 j_2 + r_2 j_1 + j_1 j_2 = r_3 + j_3,$$

where $r_3 = r_1 r_2$ and $j_3 = r_1 j_2 + r_2 j_1 + j_1 j_2$. So $R + J$ is a subring of S. Let

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

This is a composition of the inclusion $R \leq S$ and $S \to S/J$, hence ϕ is a ring homomorphism. Now

$$\mathrm{Ker}(\phi) = \{r \in R \mid r + J = J\} = R + J \lhd R,$$

$$\mathrm{Im}(\phi) = \{r + J \mid r \in R\} = (R + J)/J \leq S/J.$$

We finish by applying the first isomorphism theorem.

Remark. Let $I \lhd R$. There is a bijection between ideals in R/I, and ideals of R containing I, given by

$$K \mapsto \{r \in R \mid r + I \in K\}$$
$$J/I \hookleftarrow I$$

Theorem 8.4 (Third Isomorphism Theorem)**.** *Let $I \lhd R$, $J \lhd R$ with $I \lhd J$. Then $J/I \lhd R/I$, and*

$$(R/I)/(J/I) \cong R/J.$$

Proof: Consider $\phi : R/I \to R/J$, given by $r + I \mapsto r + J$. This is surjective ring homomorphism, and

$$\mathrm{Ker}(\phi) = \{r + I \mid r \in J\} = J/I \lhd R/I.$$

Now we finish by applying the first isomorphism theorem.

We can now prove that $R[X]/(X^2 + 1) \cong \mathbb{C}$ using the first isomorphism theorem. Define

$$\phi : \mathbb{R}[X] \to \mathbb{C}$$
$$f(x) = \sum a_k x^k \mapsto f(i) = \sum a_k i^k$$

Then $\mathrm{Ker}(\phi) = (X^2 + 1)$ by the division algorithm, and $\mathrm{Im}(\phi) = \mathbb{C}$, since $\phi(a + bX) = a + bi$. Thus,

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

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

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

Since $\mathrm{Ker}(i) \lhd \mathbb{Z}$, we have $\mathrm{Ker}(i) = n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 0}$. By the first isomorphism theorem,

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

Definition 8.5. We call n the **characteristic** of R.

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

9 Integral Domains, Maximal Ideals and Prime Ideals

9.1 Integral Domains

Definition 9.1. An **integral domain** is a ring with $0 \neq 1$ and such that for $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$.

A **zero-divisor** in a ring R is a non-zero element $a \in R$ such that $ab = 0$ for some $0 \neq b \in R$. So an integral domain is a ring with no zero-divisors.

Examples:

(i) All fields are integral domains (if $ab = 0$, multiplying by b^{-1} gives $a = 0$).

(ii) Any subring of an integral domain is an integral domain.

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

Lemma 9.1. *Let R be an integral domain. Then $R[X]$ is an integral domain.*

Proof: Write $f(X) = a_m X^m + \cdots + a_0$, $g(X) = b_n X^n + \cdots + b_0$, with $a_m \neq 0$ and $b_n \neq 0$. Then

$$f(X)g(X) = a_m b_n X^{m+n} + \cdots .$$

However $a_m b_n \neq 0$ since $a_m, b_n \in R$ and R is an integral domain. Thus $\deg(fg) = m + n = \deg(f) + \deg(g)$, so we can conclude $fg \neq 0$.

Definition 9.2. A polynomial $f(x) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in R[X]$ is monic if $a_n = 1_R$.

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

$$|\text{Roots}(f)| \leq \deg(f).$$

Theorem 9.1. *Let F be a field. Then any finite subgroup $G \leq (F^\times, \cdot)$ is cyclic.*

Proof: Note G is a finite abelian group. If G is not cyclic, then there exists $H \leq G$ such that $H \cong C_{d_1} \times C_{d_1}$, where $2 \leq d_1$.

If we then consider the polynomial

$$f(x) = x^{d_1} - 1,$$

then this has degree d_1 and at least d_1^2 roots, which is a contradiction.

This implies that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Proposition 9.1. *Any finite integral domain is a field.*

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

$$\begin{aligned} \phi : R &\to R \\ x &\mapsto ax \end{aligned}$$

If $\phi(x) = \phi(y)$, then $a \cdot (x - y) = 0$, so $x = y$, since R is an integral domain. Thus ϕ is injective, so it must be surjective since R is finite. Thus there exists b such that $ab = 1$, hence a is a unit, so R is a field.

Theorem 9.2. *Let R be an integral domain. Then there exists a field F such that*

(i) *$R \leq F$.*

(ii) *Every element of F can be written in the form $a \cdot b^{-1}$, 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 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

$$\begin{aligned} (ad)f = (bc)f = b(cf) = b(de) \\ \implies d(af - bc) = 0. \end{aligned}$$

Since R is an integral domain and $d \neq 0$, this gives $af - be = 0$, i.e. $(a, b) \sim (e, f)$. So let $F = S/\sim$, and write a/b for $[(a, b)]$. We can now define operations on F. Define

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

It can be checked that these equations are well defined and make F into a ring, with

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

Now if $a/b \neq 0_F$, 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. Checking our conditions, we get that

$$R \cong \left\{ \frac{r}{1_R} \mid r \in R \right\} \leq F.$$

Moreover, by definition $a/b = a \cdot b^{-1}$ as required.

Examples of this are $\mathbb{Z}$, with field of fractions $\mathbb{Q}$, and $\mathbb{C}[X]$, with field of fractions $\mathbb{C}(X)$, the field of rational functions in X.

9.2 Maximal Ideals

Definition 9.3. An ideal $I \lhd R$ is **maximal** if $I \neq R$, and if $I \subseteq J \lhd R$, then $J = I$ or R.

Lemma 9.3. *A (non-zero) ring R is a field if and only if its only ideals are* (0) *and R.*

Proof: If $0 \neq I \lhd R$, then I contains a unit so $I = R$. Now if $0 \neq x \in R$, then the ideal (x) is non-zero, hence $(x) = R$ so x is a unit.

Proposition 9.2. *Let $I \lhd R$ be an ideal. Then I is maximal if and only if R/I is a field.*

Proof: Note R/I is a field if and only if I/I and R/I are the only ideals in R/I. However, we have seen this implies that I and R are the only ideals in R containing I, so $I \lhd R$ is maximal.

9.3 Prime Ideals

Definition 9.4. An ideal $I \lhd R$ is prime if $I \neq R$ and whenever $a, b \in R$ with $ab \in I$, we have either $a \in I$ or $b \in I$.

Note the ideal $n\mathbb{Z} \lhd \mathbb{Z}$ is prime if and only if $n = 0$ or $n = p$ is a prime number.

Proposition 9.3. *Let $I \lhd R$ be an ideal. Then I is prime if and only if R/I is an integral domain.*

Proof: I is prime if and only if, whenever $a, b \in R$ with $ab \in I$, we have either $a \in I$ or $b \in I$. However this means whenever $a + I, b + I \in R/I$ with $(a + I)(b + I) = 0 + I$, then either $a + I = 0 + I$ or $b + I = 0 + I$. This is equivalent to R/I being an integral domain.

Remark.

- Since any field is an integral domain, a maximal ideal is always a prime ideal.
- If the characteristic of R is n, then $\mathbb{Z}/n\mathbb{Z} \leq R$. So if R is an integral domain, then $\mathbb{Z}/n\mathbb{Z}$ is an integral domain,

  $$n\mathbb{Z} \lhd \mathbb{Z} \text{ a prime ideal} \implies n = 0 \text{ or } p \text{ prime.}$$

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

10 Factorisation in Integral Domains

In this section R is an integral domain.

Definition 10.1.

(i) $a \in R$ is a unit if there exists $b \in R$ with $ab = 1$ (equivalently $(a) = R$). We let $R^\times$ be the units in R.

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

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

(iv) $r \in R$ is irreducible if $r \neq 0$, r is not a unit and $r = ab \implies a$ or b is a unit.

(v) $r \in R$ is prime if $r \neq 0$, r is not a unit and $r \mid ab \implies r \mid a$ or $r \mid b$.

Remark. These properties depend on the ring R, for example 2 is prime and irreducible in $\mathbb{Z}$, but it is a unit in $\mathbb{Q}$. Moreover $2X$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{Z}[X]$.

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

Proof: Suppose (r) is a prime ideal and $r \neq 0$. Since prime ideals are proper, r is not a unit. Now if $r \mid ab$, then $ab \in (r)$, so $a \in (r)$ or $b \in (r)$, meaning $r \mid a$ or $r \mid b$, so r is prime.

If $r = 0$, then $(0) \lhd R$ is a prime ideal since R is integral. Let $r \in R$ be prime. Then $(r) \neq R$ since $r \notin R^\times$. Now if $ab \in (r)$, then $r \mid ab$, so $r \mid a$ or $r \mid b$. Hence either $a \in (r)$ or $b \in (r)$, so (r) is a prime ideal.

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

Proof: Since r is a prime, $r \neq 0$ and $r \notin R^\times$. Suppose $r = ab$. Then $r \mid ab$ so $r \mid a$ or $r \mid b$. Say that $r \mid a$, so $a = rc$ for some $c \in R$. But then

$$r = ab = rcb \implies r(1 - bc) = 0.$$

Since we assumed $r \neq 0$, then $bc = 1$ since R is an integral domain. Hence b is a unit.

Note that the converse does not hold in general. For example, let $R = \mathbb{Z}[\sqrt{-5}]$.

Since R is a subring of a field, it is an integral domain. We can define a norm

$$N : R \to \mathbb{Z}$$
$$a + b\sqrt{-5} \mapsto a^2 + 5b^2$$

Note that $N(z_1 z_2) = N(z_1)(z_2)$. Now if $r \in R^\times$, i.e. $rs = 1$, then

$$N(r)N(s) = N(1) = 1.$$

But then $a^2 + 5b^2 = 1$, i.e. $r = \pm 1$. Then 2 is irreducible since $N(2) = 4$ and there are no elements r such that $N(r) = 2$. Similarly, we can show 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are irreducible. Now,

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

Thus $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ but 2 doesn't divide either of these elements, so 2 is not prime.

10.1 Principal Ideal Domains

Definition 10.2. An integral domain R is a **principal ideal domain** (PID) if any ideal is principal, i.e. if $I \lhd R$, then $I = (r)$.

Proposition 10.1. *Let R be a PID. Then every irreducible element of R is prime.*

Proof: Let $r \in R$ be irreducible, $r \mid ab$. Since R is a PID, $(a, r) = (d)$ for some $d \in R$, i.e. $r = cd$ for some $c \in R$. Since r is irreducible, this says either c or d is a unit.

If c is a unit, then $(a, r) = (r)$, so $r \mid a$.

If d is a unit, then $(a, r) = R$. So there exists $s, t \in R$ such that

$$sa + tr = 1.$$

Then multiplying by b, we get

$$b = sab + trb.$$

Since r divides both terms on the right hand side, $r \mid b$, as desired.

Lemma 10.3. *Let R be a PID, and $0 \neq r \in R$. Then r is irreducible if and only if (r) is a maximal ideal.*

Proof: Suppose r is irreducible. Then $r \notin R^\times$, so $(r) \neq R$. Suppose $(r) \subseteq I \subseteq R$, where $I \lhd R$. However since R is a PID,

$$I = (a) \implies r = ab.$$

Since r is irreducible, either $a = R^\times$, so $I = R$, or b is a unit, so a and b are associates, meaning $I = (a) = (r)$.

Now suppose (r) is maximal. We have assumed $r \neq 0$ and since (r) is proper, $r \notin R^\times$. Suppose that $r = ab$. Then

$$(r) \subseteq (a) \subseteq R.$$

Since (r) is maximal, either $(a) = R$, meaning a is a unit, or $(a) = (r)$, meaning a and r are associates, so b is a unit.

Remark.

(i) The reverse direction holds without assuming R is a PID.

(ii) Let R be a PID. Then

$$(r) \text{ maximal} \iff r \text{ irreducible} \iff r \text{ prime} \iff (r) \text{ prime}.$$

Therefore there is a bijection between non-zero prime ideals and non-zero maximal ideals.

10.2 Euclidean Domains

Definition 10.3. An integral domain is a **Euclidean domain** if there exists a function $\phi : \mathbb{R} \setminus \{0\} \to \mathbb{Z}_{>0}$ such that

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

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

For example, $\mathbb{Z}$ is a Euclidean Domain with function $\phi(n) = |n|$.

Proposition 10.2. *If R is a Euclidean domain, then it is a PID.*

Proof: Let R have Euclidean function ϕ, and let $I \lhd R$ be non-zero. Choose $b \in I \setminus \{0\}$, with $\phi(b)$ minimal. Then $(b) \subseteq I$.

For $a \in I$, write $a = bq + r$ with $q, r \in R$ and either $r = 0$ or $\phi(r) < \phi(b)$. Since $r = bq - a \in I$, we cannot have $\phi(r) < \phi(b)$ by the minimality of b. So $r = 0$, and so $a = bq$ for element $a \in I$. Therefore, $I = (b)$.

Remark. In the proof, we only use (ii). Property (i) allows us to describe the units of R as

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

In fact, if there exists a function satisfying (ii), then we can find a function satisfying both (i) and (ii).

Examples:

(i) If F is a field, then $F[X]$ is an ED with Euclidean function $\phi(f) = \deg f$.

(ii) $R = \mathbb{Z}[i]$ is an ED with Euclidean function $\phi(a + bi) = N(a + bi) = a^2 + b^2$. Since N is multiplicative, property (i) holds, and for property (ii), let $z_1, z_2 \in \mathbb{Z}[i]$ with $z_2 \neq 0$. Consider $z_1/z_2 \in \mathbb{C}$. Then there exists $q \in \mathbb{Z}[i]$ such that

$$\left| \frac{z_1}{z_2} - q \right| < 1.$$

Setting $r = z_1 - z_2 q \in \mathbb{Z}[i]$, then $z_1 = z_2 q + r$, and

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

Therefore both $\mathbb{Z}[i]$ and $F[X]$ for a field F are PID's.

Applications:

(1) Let $A \in M_n(F)$, and let

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

Note $I \subseteq F[X]$ is an ideal, and so $I = (f)$ for some $f \in F[X]$, since $F[X]$ is a PID. We may assume f is monic by multiplying by a unit. Then for $g \in F[X]$,

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

Therefore f is the minimal polynomial of A.

(2) Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Then let

$$f(X) = X^3 + X + 1 \in \mathbb{F}_2[X].$$

If $f(X) = g(X)h(X)$ with $q, h \in \mathbb{F}_2[X]$ and $\deg(g), \deg(h) > 0$, then either $\deg(g) = 1$ or $\deg(h) = 1$. However, this is equivalent to f having a root, but

$$f(0) = 1 \neq 0, \quad f(1) = 1 \neq 0.$$

Since $\mathbb{F}_2[X]$ is a PID, the ideal generated by f is maximal ideal, hence

$$F = \mathbb{F}_2[X]/(f)$$

is a field. However, note

$$F = \{aX^2 + bX + c \mid a, b, c \in \mathbb{F}_2\}.$$

Thus this is a field of order 8.

(3) $\mathbb{Z}[X]$ is not a PID, by considering $(2, X)$. Indeed, suppose $(2, X) = I = (f)$ for some $f \in \mathbb{Z}[X]$. Then $\deg(f) = \deg(g) = 0$, and so $f \in \mathbb{Z}$, meaning $f = \pm 1$ or ± 2. However in both these cases, f does not divide X.

10.3 Unique Factorisation Domains

Definition 10.4. An integral domain is a unique factorisation domain (UFD) if

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

(ii) If $p_1 \dots p_n = q_1 \dots q_m$, where p_i, q_j are irreducible, then $m = n$ and we can reorder such that p_i is an associate of q_i for all i.

Proposition 10.3. *Let R be an integral domain satisfying (i). Then R is an irreducible if and only if every irreducible is prime.*

Proof: If p is irreducible, then p is prime by unique factorisation. So suppose $p_1 \dots p_n = q_1 \dots q_m$ with p_i, q_j irreducible. Since p_1 is prime, $p_1 = q_1 u$ for $u \in R$. Since q_1 is irreducible, u is a unit and so p_1 and q_1 are associates. Then the result follows by induction.

Lemma 10.4. *Let R be a PID an let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ a nested sequence of ideal. Then there exists N such that $I_n = I_{n+1}$ for all $n \geq N$.*

Proof: Let $I = \bigcup I_i$. Then since R is a PID, $I = (a)$ for some $a \in R$. However considering (a),

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

so $I_n = I$.

Theorem 10.1. *If R is a PID, then R is a UFD.*

Proof: We will check (i) and (ii). If $x \in R$ and x is not a product of irreducibles, then x is not irreducible, so $x = x_1 y_1$ where one of x_1, y_1 are not a product of irreducibles. As a result,

$$(x) \subset (x_1) \subset \dots$$

This is a contradiction. Now since irreducibles are primes in PIDs, we conclude.

Definition 10.5. Let R be an integral domain.

(i) $d \in R$ is the greatest common divisor of $a_1, \dots, a_n \in R$ if $d \mid a_i$ for all i, and if $d' \mid a_i$ for all i, then $d' \mid d$.

(ii) $m \in R$ is a least common multiple of $a_1, \dots, a_n \in R$ if $a_i \mid m$, and if $a_i \mid m'$ for all i, then $m \mid m'$.

Proposition 10.4. *In a UFD, both GCD's and LCM's exist.*

Proof: Let $a_i = u_i \prod p_j^{n_{ij}}$, where u_i is a unit and the p_i are irreducible and not associate to each other.

We claim that $d = \prod p_j^{m_j}$, where

$$m_j = \min n_{ij}.$$

Certainly $d \mid a_i$, and if $d' \mid a_i$, then $d' = u \prod p_j^{t_j}$, where $t_j \leq m_j$. Therefore $d' \mid d$, as required.

The argument for LCM's is similar.

11 Factorisation in Polynomial Rings

The main theorem is the following:

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

We will say that R is a UFD with a field of fractions F. Then $R[X] \leq F[X]$. Moreover $F[X]$ is a ED, hence a PID and a UFD.

Definition 11.1. The **content** of $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ is

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

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

Lemma 11.1.

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

(ii) *If $f, g \in R[X]$, then $c(fg) = c(f)c(g)$, up to a unit.*

Proof: Let $f = a_n X^n + \cdots + a_0$, $g = b_m X^m + \cdots + b_0$. If fg is not primitive, then $c(fg)$ is not a unit, so there is some prime p such that $p \mid c(fg)$. Since f and g are primitive, $p \nmid c(f)$ and $p \nmid c(g)$. Now suppose

$$p \mid a_0, p \mid a_1, \ldots, p \nmid a_k,$$

$$p \mid b_0, p \mid b_1, \ldots, p \nmid b_l.$$

Then the coefficient of X^{k+l} in fg is

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

Hence $p \mid a_k b_l$, so $p \mid a_k$ or $p \mid b_l$, since p is prime, contradiction.

To prove the second part, let $f = c(f) \cdot f_0$, $g = c(g) \cdot g_0$, where f_0, g_0 are primitive. Then,

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

Corollary 11.1. *Let $p \in R$ be prime. Then p is prime in $R[X]$.*

Proof: $R[X]^\times = R^\times$, so p is not a unit in $R[X]$. Let $f \in R[X]$. Then

$$p \mid f \iff p \mid c(f).$$

Therefore, if $p \mid gh$ in $R[X]$, we have

$$p \mid c(gh) = c(g)c(h) \implies p \mid c(g) \text{ or } p \mid c(h) \implies p \mid g \text{ or } p \mid h.$$

Thus p is prime in $R[X]$.

Lemma 11.2. *Let $f, g \in R[X]$ with g primitive. If $g \mid f$ in $F[X]$, then $g \mid f$ in $R[X]$.*

Proof: Let $f = gh$, where $h \in F[X]$. Let $0 \neq a \in R$ such that $ah \in R[X]$, and write $ah = c(ah)h_0$, with h_0 primitive. Then

$$af = c(ah)h_0 g.$$

Taking the contents, we find that $a \mid c(ah)$. However this means that $h \in R[X]$, and $g \mid f$ in $R[X]$.

11.1 Gauss' Lemma

Lemma 11.3 (Gauss' Lemma)**.** *Let $f \in R[X]$ be primitive. Then f irreducible in $R[X]$ implies f irreducible in $F[X]$.*

Proof: Since f is irreducible and primitive, we have $\deg(f) > 0$, otherwise f is a unit.

Suppose that f is not irreducible in $F[X]$, say $f = gh$, where $g, h \in F[X]$ with $\deg(g), \deg(h) > 0$. Then we may take $\lambda \in F^\times$ such that $\lambda^{-1}g \in R[X]$ is primitive by first clearing out the denominator, then dividing by the content. Upon replacing g by $\lambda^{-1}g$ and h with λh, we may assume $g \in R[X]$ is primitive.

However the previous lemma implies that $h \in R[X]$, and so $f = gh$ in $R[X]$, with $\deg g, \deg h > 0$.

Lemma 11.4. *Let $g \in R[X]$ be primitive. Then g prime in $F[X]$ implies that g is prime in $R[X]$.*

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

$$g \text{ prime in } F[X] \implies g \mid f_1 \text{ or } g \mid f_2 \text{ in } F[X] \implies g \mid f_1 \text{ or } g \mid f_2 \text{ in } R[X].$$

Thus g is prime in $R[X]$.

Now we go back and prove our main theorem. Let $f \in R[X]$, and write $f = c(f)f_0$, with $f_0 \in R[X]$ primitive. Since R is a UFD, $c(f)$ is a product of irreducibles in R (which are also irreducible in $R[X]$).

If f_0 is not irreducible, say $f_0 = gh$, then $\deg g, \deg h > 0$, since f_0 is primitive, and so g, h are also primitive. By induction, f_0 is a product of irreducibles in $R[X]$, establishing part (i) in the definition of the UFD.

It suffices to show that if $f \in R[X]$ is irreducible, then f is prime. Write $f = c(f)f_0$, where $f_0 \in R[X]$ is primitive. Then f is irreducible implies f is constant or primitive.

Case 1: f is constant. Then f is irreducible in $R[X]$ implies f is irreducible in R, however then f is prime in R since R is a UFD, and this implies f is prime in $R[X]$, from what we have seen.

Case 2: f is primitive. Then f is irreducible in $R[X]$ implies f is irreducible in $F[X]$. However then f is prime in $F[X]$, since $F[X]$ is a UFD, and this implies f is prime in $R[X]$, from our previous lemma.

This concludes the proof.

Remark. We may show that f primitive and irreducible in $R[X]$ if and only if f is irreducible in $F[X]$, using the fact if (f) is prime in $F[X]$, then it is prime in $R[X]$ (provided f is irreducible).

11.2 Applications

(i) Since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[X]$ is a UFD.

(ii) If R is a UFD, then applying 11.1 inductively, $R[X_1, \ldots, X_n]$ is a UFD.

Proposition 11.1 (Eisenstein's Criterion)**.** *Let R be a UFD and $f(x) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ is primitive. Suppose there exists $p \in R$ irreducible such that*

- $p \nmid a_n$,
- $p \mid a_i$ *for all* $0 \leq i \leq n-1$,

- $p^2 \nmid a_0$.

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

Proof: Suppose $f = gh$, where $g, h \in R[X]$ are not units. Then f primitive implies $\deg g, \deg h > 0$. Letting $g = r_k X^k + \cdots + r_0$, $h = s_l X^l + \cdots + s_0$, with $k + l = n$. Then

$$p \nmid a_n = r_k s_l \implies p \nmid r_k \text{ and } p \nmid s_l,$$

$$p \mid a_0 = r_0 s_0 \implies p \mid r_0 \text{ or } p \mid s_0.$$

Assume $p \mid r_0$, then there exists $j \leq k$ such that

$$p \mid r_0, p \mid r_1, \ldots, p \mid r_{j-1}, p \nmid r_j.$$

Then

$$a_j = r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1 + r_j s_0.$$

p divides a_j and the first j terms on the right hand side, so it must divide $r_j s_0$. Thus, since p prime and $p \nmid r_j$, $p \mid s_0$. But then

$$p^2 \mid r_0 s_0 = a_0,$$

which is a contradiction.

(iii) Let $f(X) = X^3 + 2X + 5 \in \mathbb{Z}[X]$, then assuming f is not irreducible for contradiction, this implies

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

Thus $ac = 5$, but none of $\pm 1, \pm 5$ are units of f. Thus by Gauss' Lemma, f is irreducible in $\mathbb{Q}[X]$, and so

$$\mathbb{Q}[X]/(f)$$

is a field.

(iv) Let $p \in \mathbb{Z}$ be prime. Then by Eisenstein's criterion, $X^n - p$ is irreducible in $\mathbb{Z}[X]$, hence in $\mathbb{Q}[X]$, by Gauss' Lemma.

(v) Let $f(x) = X^{p-1} + X^{p-2} \cdots + X + 1 \in \mathbb{Z}[X]$, where $p \in \mathbb{Z}$ is prime. Then Eisenstein's does not apply directly, but note that

$$f(x) = \frac{X^p - 1}{X - 1}.$$

Substituting $Y = X - 1$, this gives

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

Now using Eisenstein's with p, this implies $f(Y+1)$ is irreducible in $\mathbb{Z}[Y]$, so $f(X)$ is irreducible in $\mathbb{Z}[X]$.

12 Algebraic Integers

12.1 Primes in $\mathbb{Z}[i]$

Recall that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$ is the ring of Gaussian integers, with norm $N(a + bi) = a^2 + b^2$. We have shown this norm makes $\mathbb{Z}[i]$ a ED, hence it is a PID and a UFD, so the primes are the irreducibles in $\mathbb{Z}[i]$.

We know that the units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ are the units, as these are the only elements with norm 1. We wish to find the primes in $\mathbb{Z}[i]$. Indeed, note

$$2 = (1 + i)(1 - i), \quad 5 = (1 - 2i)(1 + 2i),$$

so neither 2 nor 3 are prime. However 3 is a prime, since if $3 = ab$, then

$$9 = N(3) = N(a)N(b).$$

However there are no elements in $\mathbb{Z}[i]$ with norm 3, so one of a, b is a unit. Similarly, 7 is a prime. In fact, we can classify exactly when p is prime in $\mathbb{Z}[i]$.

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

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

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

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

Proof: We show (i) implies (ii). Indeed, if $p = xy$, where xy are not units, then

$$p^2 = N(p) = N(x)N(y).$$

Since $N(x), N(y) > 1$, these must both equal p. But if $x = a + bi$, then

$$p = N(x) = a^2 + b^2.$$

Now (ii) implies (iii) since the squares mod 4 are 0 and 1, so if $p = a^2 + b^2$, then $p \not\equiv 3 \pmod 4$.

Now (iii) implies (i), since we have already seen that 2 is not prime. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, if $p \equiv 1 \pmod 4$, then it contains an element x of order 4, meaning $x^4 \equiv 1$ but $x^2 \not\equiv 1$. Thus, $x^2 \equiv -1$, so

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

But $p \nmid x + i$ and $p \nmid x - i$, hence p is not prime in $\mathbb{Z}[i]$.

Theorem 12.1. *The primes in $\mathbb{Z}[i]$ are (up to associates):*

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

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

Proof: First we check these are prime. If $a^2 + b^2 = p$, then

$$p = N(a + bi).$$

Hence if $a + bi = uv$, then $N(u) = 1$ or $N(v) = 1$, so one of u, v is a unit. $p \equiv 3 \pmod 4$ we have shown are prime.

Now let $z \in \mathbb{Z}[i]$ be prime. Then $\overline{z} \in \mathbb{Z}[i]$ is prime and

$$N(z) = z\overline{z}$$

is a factorisation into irreducibles. Suppose $p \mid N(z)$, where $p \equiv 3 \pmod 4$. Then p is an associate of either z, or of $\overline{z}$, which still means p is an associate of z by conjugation.

Otherwise for all $p \mid N(z)$ we have $p = 2$ or $p \equiv 1 \pmod 4$. This means $p = (a + bi)(a - bi)$ for some primes $a + bi, a - bi$. Therefore, either z is an associate of $a + bi$ or of $a - bi$, as required.

Remark. In the above theorem, if $p = a^2 + b^2$, then $a + bi$ and $a - bi$ are not conjugates, unless $p = 2$.

Corollary 12.1. *An integer $n \geq 1$ is the sum of two squares if and only if every prime factor p of n with $p \equiv 3 \pmod 4$ divides n to an even power.*

Proof:

$$n = a^2 + b^2 \iff n = N(z) \iff n \text{ is a product of norms.}$$

The above theorem implies that the norms of primes in $\mathbb{Z}[i]$ are the primes $p \in \mathbb{Z}$ with $p \not\equiv 1 \pmod 4$, and squares of primes $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$.

12.2 Algebraic Numbers

Definition 12.1.

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

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

In the following, let R be a subring of S, and $a \in S$. We write $R[\alpha]$ as the smallest subring of S containing R and α.

Let α be an algebraic number, and let

$$\begin{aligned} \phi : \mathbb{Q}[X] &\to \mathbb{C} \\ g(x) &\mapsto g(\alpha) \end{aligned}$$

$\mathbb{Q}[X]$ is a PID, so $\mathrm{Ker}(\phi) = (f)$ for some $f \in \mathbb{Q}[X]$. Then $f \neq 0$, and upon multiplying f by a unit, we may assume that f is monic.

Definition 12.2. f is the minimal polynomial of α.

By first isomorphism theorem,

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

Thus $\mathbb{Q}[\alpha]$ is an integral domain, so f is irreducible in $\mathbb{Q}[X]$, and therefore $\mathbb{Q}[\alpha]$ is a field.

Proposition 12.2. *Let α be an algebraic integer and $f \in \mathbb{Q}[X]$ its minimal polynomial. Then $f \in \mathbb{Z}[X]$ and $(f) = \mathrm{Ker}(\theta) \lhd \mathbb{Z}[X]$ where*

$$\begin{aligned} \theta : \mathbb{Z}[X] &\to \mathbb{C} \\ g(x) &\mapsto g(\alpha) \end{aligned}$$

Proof: Let $\lambda \in \mathbb{Q}^\times$ be such that $f\lambda \in \mathbb{Z}[X]$ is primitive. Then $\lambda f(\alpha) = 0$, so $\lambda f \in \mathrm{Ker}\,\theta$.

If $g \in \mathrm{Ker}\,\theta$, then $g \in \mathrm{Ker}\,\phi$ and so $\lambda f \mid g$ in $\mathbb{Q}[X]$, so $\lambda f \mid g$ in $\mathbb{Z}[X]$.

Since α is an algebraic integer, there exists $g \in \mathrm{Ker}\,\theta$ monic. Then $\lambda f \mid g$ implies $\lambda = \pm 1$, hence $f \in \mathbb{Z}[X]$ and $(f) = \mathrm{Ker}\,\theta$.

Let $\alpha \in \mathbb{C}$ be an algebraic integer. Applying the first isomorphism theorem gives us

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

For example,

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

Corollary 12.2. *If α is an algebraic integer and $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$.*

If $\alpha \in \mathbb{Q}$, then the minimal polynomial is linear, so it must be of the form $X - \alpha$, so $\alpha \in \mathbb{Z}$.

13 Noetherian Rings

13.1 Definitions

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

If $I_1 \subseteq I_2 \subseteq \ldots$ are ideals in R, then there exists $N \in \mathbb{N}$ such that $I_n = I_{n+1}$.

More generally, we have the following result:

Lemma 13.1. *Let R be a ring. Then*

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

Proof: We prove finitely generated rings satisfy the ACC. Indeed, let

$$I_1 \subseteq I_2 \subseteq \ldots$$

be a chain of ideals, and then let $I = \bigcup I_i$, which is again an ideal. By assumption,

$$I = (a_1, \ldots, a_m).$$

These elements belong to a nested union, so there exists $N \in \mathbb{N}$ such that

$$a_1, \ldots, a_m \in I_N.$$

But then for all $n \geq N$, $I_n = I$.

Now assume $J \lhd R$ is not finitely generated. Choose $a_1 \in J$, then since $J \neq (a_1)$, we may pick $a_2 \in J \setminus (a_1)$. Inductively, we can define a_i such that

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots$$

Thus R does not satisfy the ACC.

Definition 13.1. A ring satisfying the ACC is called Noetherian.

13.2 Hilbert's Basis Theorem

Theorem 13.1 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then $R[X]$ is a Noetherian ring.*

Proof: Suppose $J \lhd R[X]$ is not finitely generated and R is Noetherian. We can choose $f_1 \in J$ of minimal degree. Then inductively we pick $f_i \in J \setminus (f_1, \dots, f_{i-1})$ of minimal degree. We obtain a sequence

$$f_1, f_2, f_3, \dots \in R[X],$$

where the degrees are non-decreasing. Let a_i be the leading coefficient of f_i, then we obtain

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

a chain of ideals in R. Since R is Noetherian, there exists m such that

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

and then we can consider

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

Then $\deg f_{m+1} = \deg g$, and they have the same leading coefficient a_{m+1}, so $f_{m+1} - g \in J$ has smaller degree than f_{m+1}, so $f_{m+1} - g \in (f_1, \dots, f_m)$, but then $f_{m+1} \in (f_1, \dots, f_m)$, contradiction.

So all J is finitely generated, and so $R[X]$ is Noetherian.

Corollary 13.1. *$\mathbb{Z}[X_1, \dots, X_n]$ and $F[X_1, \dots, X_n]$ are Noetherian, where F is a field.*

An application is to varieties on $R = \mathbb{C}[X_1, \dots, X_n]$. $V \subseteq \mathbb{C}^n$ is a subset of the form

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

where $\mathcal{F} \subseteq R$ is a possibly infinite set of polynomial. By considering

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

Then since $I \lhd R$ and R is Noetherian, $I = (g_1, \dots g_r)$, so we can redefine

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

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

Proof: Let $J_1' \subseteq J_2', \dots$ be a chain of ideal in R/I. By the usual correspondence, we have $J_i' = J_i/I$, where

$$J_1 \subseteq J_2 \subseteq \dots.$$

If R is Noetherian, then there exists N such that $J_n = J_{n+1}$, so $J_n' = J_{n+1}'$, so R/I is Noetherian.

This proves that if $R[X]$ is Noetherian, then $R[X]/(x) \cong R$ is Noetherian.

Non-Noetherian Rings

(i) $R = \mathbb{Z}[X_1, X_2, \dots]$, i.e. the polynomials in countably many variables, does not obey the ascending chain condition since

$$(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \dots.$$

(ii) Let $R = \{f \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\} \leq \mathbb{Q}[X]$, i.e. the polynomials with integer constant term. Then

$$(X) \subset \left(\frac{1}{2}X\right) \subset \left(\frac{1}{4}X\right) \subset \dots.$$

Part III

Modules

14 Definitions and Examples

14.1 Basic Definitions

Definition 14.1. Let R be a ring. A module over R is a triple $(M, +, \cdot)$, consisting of a set M and two operations,

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

such that

(i) $(M, +)$ is an abelian group with identity.

(ii) $+$ distributes over $\cdot$, and also

$$r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m, \qquad 1_R \cdot m = m.$$

Remark. As with groups and rings, we must check closure as well.

Examples:

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

(ii) Let $R = \mathbb{Z}$. Then a $\mathbb{Z}$-module is **precisely the same as** an abelian group, where

$$\cdot : \mathbb{Z} \times A \to A$$
$$(n, a) \mapsto \begin{cases} \underbrace{a + \cdots + a}_{n \text{ times}} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ \underbrace{-(a + \cdots + a)}_{n \text{ times}} & \text{if } n < 0. \end{cases}$$

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

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

Remark. Difference choices of α make V into different $F[X]$ modules. We sometimes write $V = V_\alpha$ to make this clear.

We also give some more general constructions of modules.

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

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

Therefore R is an R-module.

(v) If $I \lhd R$, then I is an R-module by restricting the usual multiplication in R. Similarly, R/I is an R-module, where

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

(vi) Let $\phi : R \to S$ be a ring homomorphism. Then an S-module M may be regarded as an R-module, via

$$\begin{aligned} \cdot : R \times M &\to M \\ (r, m) &\mapsto \phi(r)m \end{aligned}$$

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

Definition 14.2. If M is an R-module, then $N \subseteq M$ is an R-submodule (written $N \leq M$) if it is a subgroup of $(M, +)$ and $r \cdot n \in N$ for all $r \in R, n \in N$.

Examples:

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

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

Definition 14.3. If $N \leq M$ is an R-submodule, the quotient M/N is the quotient of groups under addition, with

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

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

Definition 14.4. Let M, N be R-modules. A function $f : M \to N$ is an R-module homomorphism if it is a homomorphism of abelian groups, and

$$f(r \cdot m) = r \cdot f(m).$$

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

14.2 Isomorphism Theorems

Theorem 14.1 (First Isomorphism Theorem)**.** *Let $f : M \to N$ be an R-module homomorphism. Then* $\operatorname{Ker} f = \{m \in M \mid f(m) = 0\} \leq M$, $\operatorname{Im} f = \{f(m) \in N \mid m \in M\} \leq N$, *and*

$$M/\operatorname{Ker}(f) \cong \operatorname{Im}(f).$$

The proof is an exercise.

Theorem 14.2 (Second Isomorphism Theorem)**.** *Let $A, B \leq M$ be R-submodules. Then $A + B = \{a + b \mid a \in A, b \in B\} \leq M$, $A \cap B \leq M$, and*

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

This follows by applying the first isomorphism theorem to the homomorphism

$$A \to M \to M/B.$$

Remark. Let $M \leq N$. There is a bijection between submodules in M/N, and submodules of M containing N, given by

$$\begin{aligned} K &\mapsto \{m \in M \mid m + K \in N\} \\ M/L &\leftarrow\!\shortmid L \end{aligned}$$

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

$$(M/N)/(L/N) \cong M/L.$$

In particular, these all apply to vector spaces.

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

$$Rm = \{rm \in M \mid r \in R\}.$$

This is the submodule generated by m.

Definition 14.5. M is finitely generated if there exist $m_1, \ldots, m_n \in M$ such that

$$M = Rm_1 + \cdots + Rm_n.$$

Lemma 14.1. *M is finitely generated if and only if there is a surjective R-module homomorphism $f : R^n \to M$ for some $n \in \mathbb{N}$.*

Proof: If $M = Rm_1 + \cdots + Rm_n$, then define

$$f : R^n \to M$$
$$(r_1, \ldots, r_n) \mapsto \sum r_i m_i$$

By definition this is surjective.

For the other direction, let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R^n$. Given $f : R^n \to M$ surjective, we can set $m_i = f(e_i)$. Then any $m \in M$ is of the form

$$m = f(r_1, \ldots, r_n) = f(\sum r_i e_i) = \sum r_i f(e_i) = \sum r_i m_i.$$

Thus $M = Rm_1 + \cdots + Rm_n$.

Corollary 14.1. *Let $N \leq M$ be an R-submodule. If M is finitely generated, then M/N is finitely generated.*

This follows by taking

$$R^n \to M \to M/N.$$

However, a submodule of a finitely generated module need not be finitely generated. Let R be a non-Noetherian ring and $I \lhd R$ be a non-finitely generated ideal. Then R is a finitely generated R-module, and I is a submodule which is not finitely generated.

Remark. A submodule of a finitely generated module over a Noetherian ring is finitely generated.

Definition 14.6. Let M be an R-module.

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

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

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

In particular, the torsion elements in a $\mathbb{Z}$-module are the elements of finite order.

15 Direct Sums and Free Modules

Definition 15.1. Let $M_1, \ldots, M_n$ be R-modules. The direct sum $M_1 \oplus \cdots \oplus M_n$ is the set $M_1 \times \cdots \times M_n$ with operations

$$(m_1, \ldots, m_n) + (m_1', \ldots, m_n') = (m_1 + m_1', \ldots, m_n + m_n'),$$

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

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

For example, our usual $R^n = \underbrace{R \oplus \cdots \oplus R}_{n \text{ times}}$.

Lemma 15.1. *If*

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

and $N_i \leq M_i$ for all i, then setting

$$N = \bigoplus_{i=1}^{n} N_i \leq M,$$

we have

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

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

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

This has kernel N.

Definition 15.2. Let $m_1, \ldots, m_n \in M$. The set $\{m_1, \ldots, m_n\}$ is independent if

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

Definition 15.3. A subset $S \subseteq M$ generates M freely if

(i) S generates M, i.e. for all $m \in M$,

$$m = \sum r_i s_i,$$

for $r_i \in R$, $s_i \in S$.

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

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

Proposition 15.1. *For a subset $S = \{m_1, \ldots, m_n\} \subseteq M$, the following are equivalent:*

(i) *S generates M freely.*

(ii) *S generates M and S is independent.*

(iii) *Every element of M can be written uniquely as $r_1 m_1 + \cdots + r_n m_n$ for some $r_1, \ldots, r_n \in R$.*

(iv) *The R-module homomorphism*

$$R^n \to M$$
$$(r_1, \ldots, r_n) \mapsto \sum r_i m_i$$

is an isomorphism.

Proof: To prove (i) implies (ii), suppose S generates M freely. If S is not independent, then there exists $r_1, \ldots, r_n \in R$ with

$$r_1 m_1 + \cdots + r_n m_n = 0,$$

where not all of the r_i are 0. Define $\psi : S \to R$ by

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

This extends to an R-module homomorphism $\theta : M \to R$. Then,

$$0 = \theta(0) = \theta\left(\sum r_i m_i\right) = \sum r_i \theta(m_i) = r_i.$$

Thus S is independent.

The other implications are exercises.

Examples:

(i) A non-trivial finite abelian group is not a free $\mathbb{Z}$-module.

(ii) The set $\{2, 3\}$ generates $\mathbb{Z}$ as a $\mathbb{Z}$-module, but they are not independent since $(3) \cdot 2 + (-2) \cdot 3 = 0$.

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

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: First we introduce a general construction. Let $I \lhd R$ and M an R-module. Define

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

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

$$(r + I) \cdot (m + IM) = rm + IM.$$

Suppose $R^m \cong R^n$. Choose $I \lhd R$ a maximal ideal, using Zorn's lemma. By the above, we get an isomorphism of R/I-modules

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

But $I \lhd R$ is maximal, so R/I is a field. Thus $m = n$ by the invariance of dimension for vector spaces.

16 The Structure Theorem and Applications

16.1 Smith Normal Form

For now, we assume R is a Euclidean domain with $\phi : R \setminus 0 \to \mathbb{Z}_{>0}$ a Euclidean function.

Let A be an $m \times n$ matrix with entries in R.

Definition 16.1. The elementary row operations are:

(ER1) We can add λ times the i'th row to the j'th row ($\lambda \in R$, $i \neq j$).

(ER2) We can swap the i'th and j'th rows.

(ER3) We can multiply the i'th row by $u \in R^\times$.

Each of these can be realised by left multiplication by an $m \times m$ invertible matrix. In particular, these operations are reversible.

Similarly, we can define elementary column operations realized by right multiplication by an $n \times n$ matrix.

Definition 16.2. Two $m \times n$ matrices are equivalent if there exists a sequence of elementary row and column operations taking A to B.

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*

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

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

The d_i are called **invariant factors**. We will show that they are unique up to associates.

Proof: If $A = 0$, we are done. Otherwise, upon swapping rows and columns, we may assume $a_{11} \neq 0$. We reduce $\phi(a_{11})$ as much as possible, as follows:

- If $a_{11} \nmid a_{1j}$ for some $j \geq 2$, then we can write $a_{1j} = qa_{11}+r$, where $\phi(r) < \phi(a_{11})$. Subtracting q times column 1 from column j, and swapping these, $a_{11} = r$, which is smaller.
- We can do a similar thing if $a_{11} \nmid a_{i1}$.

So we can decrease $\phi(a_{11})$, until $a_{11} \mid a_{1j}$, $a_{11} \mid a_{i1}$. Subtracting multiples of the first row/column leaves

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

where A' is $(m-1) \times (n-1)$. Now if $a_{11} \nmid a_{ij}$, then adding the i'th row to the first row, we get $a_{11} \nmid a_{1j}$, so we may do the above process. Thus $a_{11} \mid a_{ij}$ for all i, j, and we can repeat this process on A' to get the Smith Normal Form.

To prove the uniqueness of the invariant factors, we introduce the notion of minors.

Definition 16.3. A $k \times k$ minor of A is the determinant of a $k \times k$ submatrix.

Definition 16.4. The k'th Fitting ideal $\mathrm{Fit}_k(A) \lhd R$ is the ideal generated by the $k \times k$ minors of A.

Lemma 16.1. *If A and B are equivalent matrices, then $\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)$ for all k.*

Proof: We show that $(ER1 - ER3)$ don't change $\mathrm{Fit}_k(A)$:

For (ER1), add λ times the j'th row to the i'th row, to take A to A'. Let C be a $k \times k$ submatrix of A and C' the corresponding submatrix of A'.

- If we did not choose the i'th row, then $C = C'$, so $\det C = \det C'$.
- If we chose both of the rows i and j, then C and C' differ by a row operation, so $\det C = \det C'$.
- If we chose the i'th row but not the j'th row, then by expanding along the i'th row,
$$\det C' = \det C + \lambda \det D,$$
where D is a $k \times k$ matrix obtained by choosing the j'th row instead of the i'th row for C.

Thus $\det C' \in \mathrm{Fit}_k(A)$, so $\mathrm{Fit}_k(A') \subset \mathrm{Fit}_k(A)$, but since (ER1) is reversible we get equality. (ER2) and (ER3) are similar. Now if A has Smith Normal Form

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

then $\mathrm{Fit}_k(A) = (d_1 d_2 \dots d_k) \lhd R$. Thus the products $d_1, \dots, d_k$ depend only on A.

16.2 Structure Theorem and Corollaries

Lemma 16.2. *Let R be an ED. Any submodule of R^m is generated by at most m elements.*

This is proven by induction on m. For $N \lhd R^m$, consider

$$I = \{r \in R \mid \exists\, r_2, \dots, r_n,\ (r, r_2, \dots, r_m) \in N\} \lhd R.$$

Since R is a PID, $I = (a)$, so we can find an $n = (a, a_2, \dots, a_m)$. Then by subtracting multiples of n, we can reduce N to a R^{m-1} submodule, and induct.

Theorem 16.2. *Let R be an ED and $N \leq R^m$. There is a free basis $x_1, \dots, x_m$ for R^m such that N is generated by $d_1 x_1, \dots, d_t x_t$ for some $t \leq m$ and $d_1, \dots, d_t \in R$ with $d_1 \mid \dots \mid d_t$.*

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

$$A = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \end{pmatrix}.$$

Then A is equivalent to

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

Each row operation changes our choice of free basis for R^m, and each column operation changes our set of generators for N. Thus after changing free basis of R^m to $x_1, \ldots, x_m$, the sub module N is generated by $d_1x_1, \ldots, d_tx_t$ as claimed.

Theorem 16.3 (Structure Theorem)**.** *Let R be an ED and M a finitely generated R-module. Then*

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_t) \oplus R^k,$$

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

Proof: Since M is finitely generated, there exists a surjective R-module homomorphism $\phi : R^m \to M$, for some m.

By the first isomorphism theorem, $M \cong R^m/\operatorname{Ker}\phi$, and we can choose a free basis $x_1, \ldots, x_m$ for R^m such that $\operatorname{Ker}\phi$ is generated by $d_1x_1, \ldots, d_tx_t$ with $d_1 \mid \ldots \mid d_t$. Thus,

$$M \cong \frac{R \oplus R \oplus \cdots \oplus R \oplus R \oplus \cdots \oplus R}{d_1R \oplus d_2R \oplus \cdots \oplus d_tR \oplus 0 \oplus \cdots \oplus 0} \cong \frac{R}{(d_1)} \oplus \frac{R}{(d_2)} \oplus \cdots \oplus \frac{R}{(d_t)} \oplus R^{m-t}.$$

Remark. After deleting the d_i which are units, the module M is uniquely determined up to associates.

Corollary 16.1. *Let R be an ED. Then any finitely generated torsion-free module is free.*

Theorem 16.4 (Structure Theorem for Finitely Generated Abelian Groups)**.** *Any finitely generated abelian group G is isomorphic to*

$$\frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_t\mathbb{Z}} \oplus \mathbb{Z}^r.$$

This follows from taking $R = \mathbb{Z}$ in the structure theorem, and this proves the special case for G finite. We also saw that any finite abelian group could be written as a product of C_{p^i}'s. We can generalise this:

Lemma 16.3. *let R be a PID and $a, b \in R$ with $\gcd(a, b) = 1$. Then*

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

as R-modules.

Proof: Since R is a PID, $(a,b) = (d)$ for some $d \in R$. But since $\gcd(a,b) = 1$, $(a,b) = (1)$, so there are $r, s \in R$ with $ra + sb = 1$. Define an R-module homomorphism by

$$\begin{aligned} \phi : R &\to \frac{R}{(a)} \oplus \frac{R}{(b)} \\ x &\mapsto (x + (a), x + (b)). \end{aligned}$$

Then $\phi(sb) = (1 + (a), 0 + (b))$, $\phi(ra) = (0 + (a), 1 + (b))$, so $\phi(sbx + ray) = (x + (a), y + (b))$, meaning ϕ is surjective. Moreover, $(ab) \subseteq \operatorname{Ker}\phi$, and if $x \in \operatorname{Ker}\phi$, then $x \in (a) \cap (b)$, and

$$x = x(ra + sb) = r(ax) + s(xb) \in (ab).$$

Thus $\operatorname{Ker}\phi = (ab)$, so

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

Theorem 16.5 (Primary Decomposition Theorem)**.** *Let R be an 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 $p_1, \ldots, p_k$ are primes and $m \geq 0$.

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 consider $M \cong R/(d_i)$. Then $d_i = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where u is a unit and $p_1, \ldots, p_r$ are distinct. From the previous lemma, this holds.

16.3 Rational Canonical Form and Jordan Normal Form

Let V be a vector space over a field F, and let $\alpha : V \to V$ be a linear map. Let V_α denote the $F[X]$ module V, where

$$\begin{aligned} F[X] \times V &\to V \\ (f(X), V) &\mapsto f(\alpha)(V). \end{aligned}$$

Lemma 16.4. *If V is finite dimensional, then V_α is a finitely generated $F[X]$-module.*

This follows since if $v_1, \ldots, v_n$ generate V as a F-vector space, then they generate V_α as an $F[X]$-module.

Examples:

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

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

(ii) Suppose $V_\alpha \cong F[X]/(X-\lambda)^n$, as an $F[X]$-module. Then this has basis $1, X-\lambda, \ldots, (X-\lambda)^{n-1}$ with respect to F, and α has matrix

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

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

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

Theorem 16.6 (Rational Canonical Form)**.** *Let $\alpha : V \to V$ be an endomorphism of a finite dimensional vector space, where F is any field. The $F[X]$-module V_α decomposes as*

$$V_\alpha \cong \frac{F[X]}{(f_1)} \oplus \cdots \oplus \frac{F[X]}{(f_t)},$$

where $f_i \in F[X]$. Moreover, with respect to a suitable basis for V, α has matrix

$$\begin{pmatrix} c(f_1) & 0 & \cdots & 0 \\ 0 & c(f_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & c(f_t) \end{pmatrix}.$$

Proof: We known V_α is finitely generated, and since $F[X]$ is an ED, we can use the structure theorem. Since V is finite dimensional, $m = 0$, so upon multiplying each f_i be a unit, we can assume f_i are monic, and use the above.

Remark.

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

(ii) The minimum polynomial of α is f_t, and the characteristic polynomial of α is $\prod f_i$. This implies the Cayley-Hamilton theorem.

If $\dim V = 2$, then the sum of the degrees of f_i is 2, so

$$V_\alpha \cong \frac{F[X]}{(X-\lambda)} \oplus \frac{F[X]}{(X-\mu)} \text{ or } \frac{F[X]}{(f)}.$$

Corollary 16.2. *Let $A, B \in GL_2(F)$ be non-scalar matrices. Then A and B are similar if and only if they have the same characteristic polynomial.*

Definition 16.5. The annihilator of an R-module M is

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

(i) If $I \lhd R$, then $\mathrm{Ann}_R(R/I) = I$.

(ii) If A is a finite abelian group, then $\mathrm{Ann}_{\mathbb{Z}}(A) = (e)$, where e is the exponent of A.

(iii) If V_α is as above, then $\mathrm{Ann}_{F[X]}(V_\alpha)$ is the ideal generated by the minimal polynomial of α, (f).

Lemma 16.5. *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 in $\mathbb{C}[X]$ has a root in $\mathbb{C}$, so has a factor of $X - \lambda$. Hence the irreducibles have degree 1.

Theorem 16.7 (Jordan Normal Form)**.** *Let $\alpha : V \to V$ be an endomorphism of a finite dimensional $\mathbb{C}$-vector space. Let V_α be V regarded as a $\mathbb{C}[X]$-module with X acting as α. Then there is an isomorphism of $\mathbb{C}[X]$-modules*

$$V_\alpha \cong \frac{\mathbb{C}[X]}{((X-\lambda_1)^{n_1})} \oplus \cdots \oplus \frac{\mathbb{C}[X]}{((X-\lambda_t)^{n_t})},$$

where $\lambda_1, \ldots, \lambda_t \in \mathbb{C}$. In particular, there exists a basis for V such that α has matrix

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

where the Jordan blocks are

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

Proof: $\mathbb{C}[X]$ is an ED, and V_α is finitely generated as a $\mathbb{C}[X]$-module. We apply the primary decomposition theorem, noting that the primes in $\mathbb{C}[X]$ are linear. Since V is finite dimensional, there are no copies of $\mathbb{C}[X]$.

Now to deduce Jordan Normal Form, note by taking a basis of $1, (X-\lambda), \cdots, (X-\lambda)^{n-1}$ on

$$\frac{\mathbb{C}[X]}{((X-\lambda)^n)},$$

this gives us our Jordan block. Then taking a union of these bases for all factors gives us the JNF.

Remark.

(i) If α is represented by matrix A, then this theorem says A is similar to a matrix in Jordan Normal Form.

(ii) The Jordan blocks are uniquely determined up to reordering. This can be proved by considering the dimensions of the generalized eigenspaces:

$$\mathrm{Ker}((A-\lambda I)^m), \quad m = 1, 2, \ldots.$$

(iii) The minimal polynomial of α is

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

over all eigenvectors λ, where c_λ is the size of the largest λ block.

(iv) The characteristic polynomial of α is

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

where a_λ is the sum of the sizes of the λ blocks.

(v) The number of λ blocks is the dimension of the λ-eigenspace.

17 Modules over PID's

The Structure Theorem also holds for PID's. There are a few ideas which go into this proof.

Theorem 17.1. *Let R be a PID. Then any finitely generated torsion-free R-module is free.*

Lemma 17.1. *Let R be a PID and M an R-module. Let $r_1, r_2 \in R$ not both zero and let $d = \gcd(r_1, r_2)$.*

(i) *There exists $A \in SL_2(R)$ such that*

$$A \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

(ii) *If $x_1, x_2 \in M$, then there exists $x_1', x_2' \in M$ such that $Rx_1 + Rx_2 = Rx_1' + Rx_2'$, and $r_1x_1 + r_2x_2 = dx_1' + 0 \cdot x_2'$.*

Proof: Since R is a PID, $(r_1, r_2) = (d)$. Therefore, there exists $\alpha, \beta \in R$ such that $\alpha r_1 + \beta r_2 = d$. Write $r_1 = s_1 d$ and $r_2 = s_2 d$ for some $s_1, s_2 \in R$. Then $\alpha s_1 + \beta s_2 = 1$. Then

$$\begin{pmatrix} \alpha & \beta \\ -s_2 & s_1 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Then by construction, $\det A = \alpha s_1 + \beta s_2 = 1$, so $A \in SL_2(R)$.

For the second part, let $x_1' = s_1x_1 + s_2x_2$ and $x_2' = -\beta x_1 + \alpha x_2$. Then $Rx_1' + Rx_2' \subseteq Rx_1 + Rx_2$, and the reverse holds since $\det A = 1$, so A is invertible and we can write x_1, x_2 in terms of x_1', x_2'. Thus $Rx_1 + Rx_2 = Rx_1' + Rx_2'$.

Finally, $r_1x_1 + r_2x_2 = d(s_1x_1 + s_2x_2) = dx_1' + 0 \cdot x_2'$.

Finally, we prove the theorem from the beginning of the section. Let $M = Rx_1 + \cdots + Rx_n$, with n as small as possible. If $x_1, \ldots, x_n$ are independent, then M is free, and we are done. Otherwise, there exists $r_1, \ldots, r_n \in R$ such that

$$r_1x_1 + \cdots + r_nx_n = 0.$$

Wlog $r_1 \neq 0$, then replacing x_1 and x_2 by x_1' and x_2', we can assume that $r_1 \neq 0$ and $r_2 = 0$. Repeating this process, we can assume $r_1 \neq 0$ and $r_i = 0$ for all $i > 1$. But then $r_1x_1' = 0 \implies x_1' = 0$, since M is torsion-free.

Thus $M = Rx_2' + \cdots + Rx_n'$, contradicting our assumption n was minimal.

Index

p-group, 15

ACC, 50
algebraic integer, 48
algebraic number, 48
alternating group, 3, 13
annihilator, 66
ascending chain condition, 50
associates, 35

Cayley's theorem, 10
Cayley-Hamilton theorem, 66
centralizer, 11
centre, 11
characteristic, 30
characteristic polynomial, 68
composition series, 8
conjugacy class, 11
content, 41
cosets, 4
cyclic group, 3

dihedral group, 3

ED, 37
Eisenstein's criterion, 43
elementary column operations, 60
elementary row operations, 60
equivalent matrices, 60
euclidean domain, 37
exponent, 21

field, 23
field of fractions, 32
finitely generated module, 55
Fitting ideal, 61
free, 58
free basis, 57

Gauss' lemma, 42
Gaussian integers, 46
general linear group, 19
group, 3
    action, 9
    direct product, 4
    homomorphism, 5
    isomorphism theorems, 5

Hilbert's basis theorem, 51

ideal, 25
    maximal, 33
    prime, 34
    principal, 26
independent set, 57
integral domain, 31
invariant factors, 60
irreducible, 35

Jordan blocks, 67
Jordan normal form, 67

Lagrange's theorem, 4
Laurent polynomials, 24

minimal polynomial, 48, 68
minor, 61
module, 53
    direct sum, 57
    homomorphism, 54
    isomorphism theorems, 55

Noetherian ring, 50
normal subgroup, 4
normalizer, 12

orbit, 10
order, 4

permutation group, 9
PID, 36

polynomial ring, 23
power series ring, 24
primary decomposition theorem, 64
prime, 35
primitive polynomial, 41
principal ideal domain, 36
projective general linear group, 19
projective special linear group, 19

quotient group, 4

rational canonical form, 65
ring, 22
    direct product, 22
    homomorphism, 25
    isomorphism theorems, 27

simple group, 7
Smith normal form, 60
special linear group, 19
stabilizer, 10
structure theorem, 63, 69
subgroup, 3
submodule, 54
subring, 22
Sylow theorems, 16
symmetric group, 3

torsion, 56
torsion module, 56
torsion-free, 56

UFD, 39
unique factorisation domain, 39
unit, 23, 35

zero-divisor, 31