Part IB — GRM

Based on lectures by Dr R Zhou and notes by thirdsgames.co.uk

Lent 2022

Contents

Part I
Groups

§0 Review of IA Groups

This section contains material covered by IA Groups.

§0.1 Definitions

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

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- there exists $e \in G$ such that for all $g \in G$, we have $g \cdot e = e \cdot g = g$; and
- for all $g \in G$, there exists an inverse $h \in G$ such that $g \cdot h = h \cdot g = e$.

Remark 1.
1. Sometimes, such as in IA Groups, a closure axiom is also specified. However, this is implicit in the type definition of $\cdot$. In practice, this must normally be checked explicitly.
2. Additive and multiplicative notation will be used interchangeably. For additive notation, the inverse of g is denoted $-g$, and for multiplicative notation, the inverse is instead denoted g^{-1}. The identity element is sometimes denoted 0 in additive notation and 1 in multiplicative notation.

A subset $H \subseteq G$ is a *subgroup* of G, written $H \leq G$, if $h \cdot h' \in H$ for all $h, h' \in H$, and $(H, \cdot)$ is a group. The closure axiom must be checked, since we are restricting the definition of $\cdot$ to a smaller set.

Remark 2. A non-empty subset $H \subseteq G$ is a subgroup of G if and only if

$$a, b \in H \implies a \cdot b^{-1} \in H$$

An *abelian* group is a group such that $a \cdot b = b \cdot a$ for all a, b in the group. The *direct product* of two groups G, H, written $G \times H$, is the group over the Cartesian product $G \times H$ with operation $\cdot$ defined such that $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$.

§0.2 Cosets

Let $H \leq G$. Then, the *left cosets* of H in G are the sets gH for all $g \in G$. The set of left cosets partitions G. Each coset has the same cardinality as H. Lagrange's theorem states that if G is a finite group and $H \leq G$, we have $|G| = |H| \cdot [G : H]$, where $[G : H]$ is the number of left cosets of H in G. $[G : H]$ is known as the *index* of H in G. We can construct Lagrange's theorem analogously using right cosets. Hence, the index of a subgroup is independent of the choice of whether to use left or right cosets; the number of left cosets is equal to the number of right cosets.

§0.3 Order

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. If no such n exists, we say that g has infinite order. If g has order d, then:

1. $g^n = 1 \implies d \mid n$;
2. $\langle g \rangle = \left\{1, g, \dots, g^{d-1}\right\} \leq G$, and by Lagrange's theorem (if G is finite) $d \mid |G|$.

§0.4 Normality and quotients

A subgroup $H \leq G$ is *normal*, written $H \trianglelefteq G$, if $g^{-1}Hg = H$ for all $g \in G$. In other words, H is preserved under conjugation over G. If $H \trianglelefteq G$, then the set ${}^{G}\!/_{H}$ of left cosets of H in G forms the *quotient group*. The group action is defined by $g_1 H \cdot g_2 H = (g_1 \cdot g_2)H$. This can be shown to be well-defined.

§0.5 Homomorphisms

Let G, H be groups. A function $\varphi : G \to H$ is a *group homomorphism* if $\varphi(g_1 \cdot_G g_2) = \varphi(g_1) \cdot_H \varphi(g_2)$ for all $g_1, g_2 \in G$. The *kernel* of φ is defined to be $\ker \varphi = \{g \in G : \varphi(g) = 1\}$, and the *image* of φ is $\operatorname{Im} \varphi = \{\varphi(g) : g \in G\}$. The kernel is a normal subgroup of G, and the image is a subgroup of H.

§0.6 Isomorphisms

An *isomorphism* is a homomorphism that is bijective. This yields an inverse function, which is of course also an isomorphism. If $\varphi : G \to H$ is an isomorphism, we say that G and H are isomorphic, written $G \cong H$. Isomorphism is an equivalence relation.

Theorem 0.1 (First Isomorphism Theorem)

If $\varphi : G \to H$, then ${}^{G}\!\big/_{\ker\varphi} \cong \operatorname{Im}\varphi$;

Theorem 0.2 (Second Isomorphism Theorem)
If $H \leq G$ and $K \trianglelefteq G$, then $H \cap K \trianglelefteq H$ and ${}^{H}\!\big/_{H \cap K} \cong {}^{HK}\!\big/_{K}$

Proof. Let $h_1k_1, h_2k_2 \in HK$ (so $h_1, h_2 \in H$, $k_1, k_2 \in K$). $h_1k_1(h_2k_2)^{-1} = \underbrace{h_1h_2^{-1}}_{\in H}\underbrace{h_2k_1k_2^{-1}h_2^{-1}}_{\in K} \in HK$. Thus $HK \subset G$ (by a previous Remark)

Let $\varphi : H \to {}^{G}\!\big/_{K}, h \mapsto hK$. This is the composite of $H \to G$ and the quotient map $G \to {}^{G}\!\big/_{K}$, hence φ a group homomorphism. $\ker\varphi = \{h \in H : hK = K\} = H \cap K \trianglelefteq H$ and $\operatorname{Im}\varphi = \{hK : h \in H\} = {}^{HK}\!\big/_{K}$.

First isomorphism theorem implies ${}^{H}\!\big/_{H \cap K} \cong {}^{HK}\!\big/_{K}$. □

Remark 3. Suppose $K \trianglelefteq G$. There is a bijection between subgroups of ${}^{G}\!\big/_{K}$ and subgroups of G containing K. This also restricts to a bijection between normal subgroups of ${}^{G}\!\big/_{K}$ and normal subgroups of G containing K.

Theorem 0.3 (Third Isomorphism Theorem)
Let $K \leq H \leq G$ be normal subgroups of G. Then ${}^{G/K}\!\big/_{H/K} = {}^{G}\!\big/_{H}$

Proof. Let $\varphi : {}^{G}\!\big/_{K} \to {}^{G}\!\big/_{H}, gK \mapsto gH$. If $g_1K = g_2K$, then $g_2^{-1}g_1 \in K \subset H \implies g_1H = g_2H$. Thus φ well-defined.

φ is a surjective group homomorphism with kernel ${}^{H}\!\big/_{K}$. □

§1 Simple groups

§1.1 Introduction

If $K \trianglelefteq G$, then studying the groups K and ${}^{G}\!/_{K}$ give information about G itself. This approach is available only if G has nontrivial normal subgroups. It therefore makes sense to study groups with no normal subgroups, since they cannot be decomposed into simpler structures in this way.

Definition 1.1 (Simple Group)
A group G is **simple** if $\{1\}$ and G are its only normal subgroups.

By convention, we do not consider the trivial group to be a simple group. This is analogous to the fact that we do not consider one to be a prime.

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

Proof. Certainly C_p is simple by Lagrange's theorem. Conversely, since G is abelian, all subgroups are normal. Let $1 \neq g \in G$. Then $\langle g \rangle \trianglelefteq G$. Hence $\langle g \rangle = G$ by simplicity. If G is infinite, then $G \cong \mathbb{Z}$, which is not a simple group; $2\mathbb{Z} \triangleleft \mathbb{Z}$. Hence G is finite, so $G \cong C_{o(g)}$. If $o(g) = mn$ for $m, n \neq 1, p$, then $\langle g^m \rangle \leq G$, contradicting simplicity. □

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

$$1 \cong G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

where each quotient ${}^{G_{i+1}}\!/_{G_i}$ is simple.

Remark 4. It is not the case that necessarily G_i be normal in G_{i+k} for $k \geq 2$.

Proof. We will consider an inductive step on $|G|$. If $|G| = 1$, then trivially $G = 1$. Conversely, if $|G| > 1$, let G_{n-1} be a normal subgroup of largest possible order not equal to $|G|$. Then, ${}^{G}\!/_{G_{n-1}}$ exists, and is simple by remark 3. □

§2 Group actions

§2.1 Definitions

Definition 2.1 (Symmetric Group)
Let X be a set. Then $\mathrm{Sym}(X)$ is the group of permutations of X; that is, the group of all bijections of X to itself under composition. The identity can be written id or id_X.

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

Example 2.1
The symmetric group S_n is exactly equal to $\mathrm{Sym}(\{1, \ldots, n\})$, so is a permutation group of order n. A_n is also a permutation group of order n, as it is a subgroup of S_n. D_{2n} is a permutation group of order n.

Definition 2.3 (Group Actions)
A **group action** of a group G on a set X is a function $\alpha : G \times X \to X$ satisfying

$$\alpha(e, x) = x; \quad \alpha(g_1 \cdot g_2, x) = \alpha(g_1, \alpha(g_2, x))$$

for all $g_1, g_2 \in G, x \in X$. The group action may be written $*$, defined by $g * x \equiv \alpha(g, x)$.

Proposition 2.1
An action of a group G on a set X is uniquely characterised by a group homomorphism $\varphi : G \to \mathrm{Sym}(X)$.

Proof. For all $g \in G$, we can define $\varphi_g : X \to X$ by $x \mapsto g * x$. Then, for all $x \in X$,

$$\varphi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \varphi_{g_1}(\varphi_{g_2}(x))$$

Thus $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$. In particular, $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e$. We now define

$$\varphi : G \to \mathrm{Sym}(X); \quad \varphi(g) = \varphi_g \implies \varphi(g)(x) = g * x$$

This is a homomorphism.

Conversely, any group homomorphism $\varphi : G \to \mathrm{Sym}(X)$ induces a group action $*$ by $g * x = \varphi(g)$. This yields $e * x = \varphi(e)(x) = \mathrm{id}\, x = x$ and $(g_1 g_2) * x = \varphi(g_1 g_2)x = \varphi(g_1)\varphi(g_2)x = g_1 * (g_2 * x)$ as required. □

Definition 2.4 (Permutation Representation)

The homomorphism $\varphi : G \to \mathrm{Sym}(X)$ defined in the above proof is called a **permutation representation** of G.

Definition 2.5 (Orbit, Stabiliser)

Let G act on X. Then,

1. the **orbit** of $x \in X$ is $\mathrm{Orb}_G(x) = \{g * x : g \in G\} \subseteq X$;
2. the **stabiliser** of $x \in X$ is $G_x = \{g \in G : g * x = x\} \leq G$.

Definition 2.6 (Transitive Group Action)

If there is only orbit, i.e. $\mathrm{Orb}_G(x) = X \quad \forall\, x$ then the group action is **transitive**.

Definition 2.7 (Kernel)

The **kernel** of a permutation representation is $\bigcap_{x \in X} G_x$.

Remark 5. The kernel of the permutation representation φ is also referred to as the kernel of the group action itself.

Definition 2.8 (Faithful Group Action)

If the kernel is trivial the action is said to be **faithful**.

Theorem 2.1 (Orbit-stabiliser theorem)

The orbit $\mathrm{Orb}_G(x)$ bijects with the set ${}^{G}\!/_{G_x}$ of left cosets of G_x in G (which may not be a quotient group). In particular, if G is finite, we have

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

Example 2.2

If G is the group of symmetries of a cube and we let X be the set of vertices in the cube, G acts on X. Here, for all $x \in X$, $|\mathrm{Orb}(x)| = 8$ and $|G_x| = 6$ (including reflections), hence $|G| = 48$.

Remark 6. The orbits partition X.

Note that $G_{g*x} = gG_xg^{-1}$. Hence, if x, y lie in the same orbit, their stabilisers are conjugate.

§2.2 Examples

Example 2.3

G acts on itself by left multiplication. This is known as the **left regular action**. The kernel is trivial, hence the action is faithful. The action is transitive, since for all $g_1, g_2 \in G$, the element $g_2g_1^{-1}$ maps g_1 to g_2.

Theorem 2.2 (Cayley's theorem)

Any finite group G is a permutation group of order $|G|$; it is isomorphic to a subgroup of $S_{|G|}$.

Example 2.4

Let $H \leq G$. Then G acts on ${}^{G}\!/_{H}$ by left multiplication, where ${}^{G}\!/_{H}$ is the set of left cosets of H in G. This is known as the **left coset action**. This action is transitive using the construction above for the left regular action. We have $\ker\varphi = \bigcap_{x \in G} xHx^{-1}$, which is the largest normal subgroup of G contained within H.

Theorem 2.3

Let G be a non-abelian simple group, and $H \leq G$ with 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. Let $\varphi : G \to \mathrm{Sym}(X)$ be the permutation representation associated to this group action.

Since G is simple, $\ker\varphi = 1$ or $\ker\varphi = G$. If $\ker\varphi = G$, then $\operatorname{Im}\varphi = 1_{S_n}$, which is a contradiction since G acts transitively on X and $|X| > 1$. Thus $\ker\varphi = 1$, and $G \cong \operatorname{Im}\varphi \leq S_n$.

Since $G \leq S_n$ and $A_n \triangleleft S_n$, the second isomorphism theorem shows that $G \cap A_n \triangleleft G$, and

$$ {}^{G}\!/_{G\cap A_n} \cong {}^{GA_n}\!/_{A_n} \leq {}^{S_n}\!/_{A_n} \cong C_2 $$

Since G is simple, $G \cap A_n = 1$ or G. If $G \cap A_n = 1$, then G is isomorphic to a subgroup of C_2, but this is false, since G is non-abelian. Hence $G \cap A_n = G$ so $G \leq A_n$. Finally, if $n \leq 4$ we can check manually that A_n is not simple; A_n has no non-abelian simple subgroups. □

§2.3 Conjugation actions

Example 2.5

Let G act on G by conjugation, so $g * x = gxg^{-1}$. This is known as the **conjugation action**.

Definition 2.9 (Conjugacy Class, Centraliser, Centre)

The orbit of the conjugation action is called the **conjugacy class** of a given element $x \in G$, written $\mathrm{ccl}_G(x)$. The stabiliser of the conjugation action is the set C_x of elements which commute with a given element x, called the **centraliser** of x in G. The kernel of φ is the set $Z(G)$ of elements which commute with all elements in x, which is the **centre** of G. This is always a normal subgroup.

Remark 7. $\varphi : G \to G$ satisfies

$$ \varphi(g)(h_1h_2) = gh_1h_2g^{-1} = hh_1g^{-1}gh_2g^{-1} = \varphi(g)(h_1)\varphi(g)(h_2) $$

Hence $\varphi(g)$ is a group homomorphism for all g. It is also a bijection, hence $\varphi(g)$ is an isomorphism from $G \to G$.

Definition 2.10 (Automorphism)

An isomorphism from a group to itself is known as an **automorphism**. We define $\mathrm{Aut}(G)$ to be the set of all group automorphisms of a given group. This set is a group. Note, $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, and the $\varphi : G \to \mathrm{Sym}(G)$ above has image in $\mathrm{Aut}(G)$.

Example 2.6

Let X be the set of subgroups of G. Then G acts on X by conjugation: $g * H = gHg^{-1}$. The stabiliser of a subgroup H is $\{g \in G : gHg^{-1} = H\} = N_G(H)$, called the **normaliser** of H in G. The normaliser of H is the largest subgroup of G that contains H as a normal subgroup. In particular, $H \triangleleft G$ if and only if $N_G(H) = G$.

§3 Alternating groups

§3.1 Conjugation in alternating groups

We know that elements in S_n are conjugate if and only if they have the same cycle type. However, elements of A_n that are conjugate in S_n are not necessarily conjugate in A_n. Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. There are two possible cases.

- If there exists an odd permutation that commutes with g, then $2|C_{A_n}(g)| = |C_{S_n}(g)|$. By the orbit-stabiliser theorem, $|\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|$.
- If there is no odd permutation that commutes with g, we have $|C_{A_n}(g)| = |C_{S_n}(g)|$. Similarly, $2|\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|$.

Example 3.1

For $n = 5$, the product $(1\ 2)(3\ 4)$ commutes with $(1\ 2)$, and $(1\ 2\ 3)$ commutes with $(4\ 5)$. Both of these elements are odd. So the conjugacy classes of the above inside S_5 and A_5 are the same. However, $(1\ 2\ 3\ 4\ 5)$ does not commute with any odd permutation. Indeed, if that were true for some h, we would have

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

Hence h must be a 5-cycle so $h \in \langle g \rangle \leq A_5$. So $|\mathrm{ccl}_{A_5}(g)| = \frac{1}{2}|\mathrm{ccl}_{S_5}(g)| = 12$. We can then show that A_5 has conjugacy classes of size $1, 15, 20, 12, 12$.

If $H \trianglelefteq A_5$, H is a union of conjugacy classes so $|H|$ must be a sum of the sizes of the above conjugacy classes. By Lagrange's theorem, $|H|$ must divide 60. We can check explicitly that this is not possible unless $|H| = 1$ or $|H| = 60$. Hence A_5 is simple.

§3.2 Simplicity of alternating groups

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. It therefore suffices to show that a product of any two transpositions can be written as a product of 3-cycles. For a, b, c, d distinct,

$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d); \quad (a\ b)(b\ c) = (a\ b\ c)$$

□

Lemma 3.2

If $n \geq 5$, all 3-cycles in A_n are conjugate (in A_n).

Proof. We claim that every 3-cycle is conjugate to $(1\ 2\ 3)$. If $(a\ b\ c)$ is a 3-cycle, we have $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \in A_n$, then the proof is finished. Otherwise, $\sigma \mapsto \sigma(4\ 5) \in A_n$ suffices, since $(4\ 5)$ commutes with $(1\ 2\ 3)$. □

Theorem 3.1

A_n is simple for $n \geq 5$.

Proof. Suppose $1 \neq N \triangleleft A_n$. To disprove normality, it suffices to show that N contains a 3-cycle by the lemmas above, since the normality of N would imply N contains all 3-cycles and hence all elements of A_n.

Let $1 \neq \sigma \in N$, writing σ as a product of disjoint cycles.

1. Suppose σ contains a cycle of length $r \geq 4$. Without loss of generality, let $\sigma = (1\ 2\ 3 \dots r)\tau$ where τ fixes $1, \dots, r$. Now, let $\delta = (1\ 2\ 3)$. We have

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

   So N contains a 3-cycle.

2. Suppose σ contains two 3-cycles, which can be written without loss of generality as $(1\ 2\ 3)(4\ 5\ 6)\tau$. Let $\delta = (1\ 2\ 4)$, and then

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

   Therefore, there exists an element of N which contains a cycle of length $5 \geq 4$. This reduces the problem to case (i).

3. Finally, suppose σ contains two 2-cycles, which will be written $(1\ 2)(3\ 4)\tau$. Then let $\delta = (1\ 2\ 3)$ and

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

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

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

   Thus N contains a 3-cycle.

There are now three remaining cases, where σ is a transposition, a 3-cycle, or a transposition composed with a 3-cycle. Note that the remaining cases containing transpositions cannot be elements of A_n. If σ is a 3-cycle, we already know A_n contains a 3-cycle, namely σ itself. $\square$

§4 p-groups

§4.1 p-groups

Definition 4.1 (p-group)

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

Theorem 4.1

If G is a p-group, the centre $Z(G)$ is non-trivial.

Proof. For $g \in G$, due to the orbit-stabiliser theorem, $|\text{ccl}(g)||C(g)| = p^n$. In particular, $|\text{ccl}(g)|$ divides p^n, and they partition G. Since G is a disjoint union of conjugacy classes, modulo p we have

$$|G| \equiv \text{number of conjugacy classes of size } 1 \equiv 0 \implies |Z(G)| \equiv 0$$

Hence $Z(G)$ has order zero modulo p so it cannot be trivial. We can check this by noting that $g \in Z(G) \iff x^{-1}gx = g$ for all x, which is true if and only if $\text{ccl}_G(g) = \{g\}$. □

Corollary 4.1

The only simple p-groups are the cyclic groups of order p.

Proof. Let G be a simple p-group. Since $Z(G)$ is a normal subgroup of G, we have $Z(G) = 1$ or $Z(G) = G$. But $Z(G)$ may not be trivial, so $Z(G) = G$. This implies G is abelian. The only abelian simple groups are cyclic of prime order by lemma 1.1, hence $G \cong C_p$. □

Corollary 4.2

Let G be a p-group of order p^n. Then G has a subgroup of order p^r for all $r \in \{0, \dots, n\}$.

Proof. Recall from lemma 1.2 that any group G has a composition series $1 = G_1 \lhd \dots \lhd G_N = G$ where each quotient ${G_{i+1}}/{G_i}$ is simple.

Since G is a p-group, ${G_{i+1}}/{G_i}$ is also a p-group. Each successive quotient is an order p group by the previous corollary, so we have a composition series of nested subgroups of order p^r for all $r \in \{0, \dots, n\}$. □

Lemma 4.1

Let G be a group. If ${}^{G}\!/\!_{Z(G)}$ is cyclic, then G is abelian. This then implies that $Z(G) = G$, so in particular ${}^{G}\!/\!_{Z(G)} = 1$.

Proof. Let $gZ(G)$ be a generator for ${}^{G}\!/\!_{Z(G)}$. Then, each coset of $Z(G)$ in G is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$. Thus, $G = \{g^r z : r \in \mathbb{Z}, z \in Z(G)\}$. Now, we multiply two elements of this group and find

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

So any two elements in G commute. □

Corollary 4.3

Any group of order p^2 is abelian.

Proof. Let G be a group of order p^2. Then $|Z(G)| \in \{1, p, p^2\}$. The centre cannot be trivial as proven above, since G is a p-group. If $|Z(G)| = p$, we have that ${}^{G}\!/\!_{Z(G)}$ is cyclic as it has order p. Applying the previous lemma, G is abelian. However, this is a contradiction since the centre of an abelian group is the group itself. If $|Z(G)| = p^2$ then $Z(G) = G$ and then G is clearly abelian. □

§4.2 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 does not divide m. Then:

1. The set $\mathrm{Syl}_p(G) = \{P \leq G : |P| = p^a\}$ of Sylow p-subgroups is non-empty.
2. All Sylow p-subgroups are conjugate.
3. The amount of Sylow p-subgroups $n_p = \left|\mathrm{Syl}_p(G)\right|$ satisfies

$$n_p \equiv 1 \mod p; \quad n_p \mid |G| \implies n_p \mid m$$

Proof. 1. Let Ω be the set of all <u>subsets</u> of G of order p^a. We can directly find

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

Note that for $0 \le k < p^a$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same power of p. In particular, $|\Omega|$ is coprime to p.

Let G act on Ω by left-multiplication, so $g * X = \{gx : x \in X\}$. For any $X \in \Omega$, the orbit-stabiliser theorem can be applied to show that

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

Since $|\Omega|$ is coprime to p, there must exist an orbit with size coprime to p, since orbits partition Ω. For such an X, $p^a \mid |G_X|$.

Conversely, note that if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$. Hence, we can consider

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

Thus $|G| \le |\mathrm{orb}_G(X)| \cdot |X|$, giving $|G_X| = \frac{|G|}{|\mathrm{orb}_G(X)|} \le |X| = p^a$.

As $p^a \mid |G_X|$ we must have $|G_X| = p^a$. In other words, the stabiliser G_X is a Sylow p-subgroup of G.

2. We will prove a stronger result for this part of the proof.

Lemma 4.2

If P is a Sylow p-subgroup and $Q \le G$ is a p-subgroup, then $Q \le gPg^{-1}$ for some $g \in G$.

Indeed, let Q act on the set of left cosets of P in G by left multiplication. By the orbit-stabiliser theorem, each orbit has size which divides $|Q| = p^k$ for some k. Hence each orbit has size p^r for some r.

Since ${}^{G}\!/_{P}$ has size m, which is coprime to p, there must exist an orbit of size 1[a]. Therefore there exists $g \in G$ such that $q * gP = gP$ for all $q \in Q$. Equivalently, $g^{-1}qg \in P$ for all $q \in Q$. This implies that $Q \le gPg^{-1}$ as required. This then weakens to the second part of the Sylow theorems.

3. Let G act on $\mathrm{Syl}_p(G)$ by conjugation. Part (ii) of the Sylow theorems implies that this action is transitive. By the orbit-stabiliser theorem, $n_p = \left|\mathrm{Syl}_p(G)\right| \mid |G|$.

Let $P \in \mathrm{Syl}_p(G)$. Then let P act on $\mathrm{Syl}_p(G)$ by conjugation. Since P is a Sylow p-subgroup, the orbits of this action have size dividing $|P| = p^a$, so the size is some power of p.
To show $n_p \equiv 1 \mod p$, it suffices to show that $\{P\}$ is the unique orbit of size 1, as the orbits of other sizes are multiples of p and orbits partition $\mathrm{Syl}_p(G)$. Suppose $\{Q\}$ is another orbit of size 1, so Q is a Sylow p-subgroup which is preserved under conjugation by P. Thus P normalises Q, so $P \le N_G(Q)$ and $Q \trianglelefteq N_G(Q)$. Notice that P and Q are both Sylow p-subgroups of $N_G(Q)$. By (ii), P and Q are conjugate inside $N_G(Q)$. Hence $gPg^{-1} = Q$ so $P = g^{-1}Qg = Q$ since $Q \trianglelefteq N_G(Q)$. Thus, $|P|$ is the unique orbit of size 1, so $n_p \equiv 1 \mod p$ as required.

□

[a] Sum of the orbit sizes is m, m coprime to p.

Corollary 4.4

If $n_p = 1$, then there is only one Sylow p-subgroup, and it is normal.

Proof. Let $g \in G$ and $P \in \mathrm{Syl}_p(G)$. Then gPg^{-1} is a Sylow p-subgroup, hence $gPg^{-1} = P$. P is normal in G. □

Remark 8. When G acts on $\mathrm{Syl}_p(G)$ by conjugation, the orbit is $\mathrm{Syl}_p(G)$ and the stabiliser is the normaliser.

Example 4.1

Let G be a group with $|G| = 1000 = 2^3 \cdot 5^3$. Here, $n_5 \equiv 1 \mod 5$, and $n_5 \mid 8$, hence $n_5 = 1$. Thus the unique Sylow 5-subgroup is normal. Hence no group of order 1000 is simple.

Example 4.2

Let G be a group with $|G| = 132 = 2^2 \cdot 3 \cdot 11$. n_{11} satisfies $n_{11} \equiv 1 \mod 11$ and $n_{11} \mid 12$, thus $n_{11} \in \{1, 12\}$.

Suppose G is simple.

Then $n_{11} = 12$[a]. The amount of Sylow 3-subgroups satisfies $n_3 \equiv 1 \mod 3$ and $n_3 \mid 44$ so $n_3 \in \{1, 4, 22\}$. Since G is simple, $n_3 \in \{4, 22\}$.

Suppose $n_3 = 4$. Then G acts on $\mathrm{Syl}_3(G)$ by conjugation, and this generates a group homomorphism $\varphi : G \to S_4$. But the kernel of this homomorphism is a normal subgroup of G, so $\ker \varphi$ is trivial or G itself as G simple. If $\ker \varphi = G$, then

$\operatorname{Im}\varphi$ is trivial, contradicting Sylow's second theorem. If $\ker\varphi = 1$, then $\operatorname{Im}\varphi$ has order $132 > |S_4|$ ↯.

Thus $n_3 = 22$ and recall $n_{11} = 12$. This means that G has $22 \cdot (3-1) = 44$ elements of order 3[b], and further G has $12 \cdot (11-1) = 120$ elements of order 11. However, the sum of these two totals is more than the total of 132 elements, so this is a contradiction. Hence G is not simple.

[a] If $n_{11} = 1$ then we have a normal subgroup by the previous corollary.

[b] Each group in $\operatorname{Syl}_3(G)$ intersect trivially, as if they didn't any non trivial element in the intersection would generate both groups as they're all C_3.

§5 Matrix groups

§5.1 Definitions

Let F be a field, such as $\mathbb{C}$ or ${}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}$.

Definition 5.1 (General Linear Group)

Let $GL_n(F)$ be set of $n \times n$ invertible matrices over F, which is called the **general linear group**.

Definition 5.2 (Special Linear Group)

Let $SL_n(F)$ be set of $n \times n$ matrices with determinant one over F, which is called the **special linear group**.

Remark 9. $SL_n(F)$ is the kernel of the determinant homomorphism on $GL_n(F)$, so $SL_n(F) \lhd GL_n(F)$.

Definition 5.3 (Scalar Matrices)

Let $Z \lhd GL_n(F)$ denote the subgroup of **scalar matrices**, the group of nonzero multiples of the identity.

Remark 10. Z is the centre of $GL_n(F)$.

Definition 5.4 (Projective General Linear Group)

The group $PGL_n(F) = {}^{GL_n(F)}\!/\!_{Z}$ is called the **projective general linear group**.

Definition 5.5 (Projective Special Linear Group)

The **projective special linear group** is $PSL_n(F) = {}^{SL_n(F)}\!/\!_{Z \cap SL_n(F)}$.

Remark 11. By the second isomorphism theorem, $PSL_n(F)$ is isomorphic to ${}^{Z \cdot SL_n(F)}\!/\!_{Z}$, which is a subgroup of $PGL_n(F)$.

Example 5.1

Consider the finite group $G = GL_n\left({}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}\right)$. A list of n vectors in ${}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}$ are the columns of a matrix $A \in G$ iff the vectors are linearly independent. Hence, by considering dimensionality of subspaces generated by each column,

$$\begin{aligned}|G| &= (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}) \\ &= p^{1+2+\cdots+(n-1)}(p^n - 1)(p^{n-1} - 1)\cdots(p-1) \\ &= p^{\binom{n}{2}}\prod_{i=1}^{n}(p^i - 1)\end{aligned}$$

Hence the Sylow p-subgroups have size $p^{\binom{n}{2}}$. Let U be the set of upper triangular matrices with ones on the diagonal. This forms a Sylow p-subgroup of G, since there are $\binom{n}{2}$ entries in a given upper triangular matrix, and there are p choices for such an entry.

§5.2 Möbius maps in modular arithmetic

Recall that $PGL_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ by Möbius transformations. Likewise, $PGL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ acts on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$ by Möbius transformations. For a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2\left(\mathbb{Z}/p\mathbb{Z}\right); \quad A : z \mapsto \frac{az+b}{cz+d}$$

Since the scalar matrices act trivially, we obtain an action on the projective general linear group instead of the general linear group by quotienting out the scalar matrices.

We can represent ∞ as an integer, say, p, for the purposes of constructing a permutation representation.

Lemma 5.1

The permutation representation $PGL_2\left(\mathbb{Z}/p\mathbb{Z}\right) \to S_{p+1}$ is injective (and is an isomorphism if $p = 2$ or $p = 3$).

Proof. Suppose that $\frac{az+b}{cz+d} = z$ for all $z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$.
Since $z = 0$, we have $b = 0$.
Since $z = \infty$, we find $c = 0$.
Thus the matrix is diagonal.
Finally, since $z = 1$, $\frac{a}{d} = 1$ hence $a = d$.
Thus the matrix is scalar. So the permutation representation from $PGL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ has trivial kernel, giving injectivity as required.

If $p = 2$ or $p = 3$ we can compute the orders of relevant groups manually and show that the permutation representation is an isomorphism. □

Lemma 5.2

Let p be an odd prime. Then

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

Proof. By example 5.1,

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

The homomorphism $GL_2\left(\mathbb{Z}/p\mathbb{Z}\right) \to \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ given by the determinant is surjective. Since $SL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ is the kernel of this homomorphism, we have

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

Now, if $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ is an element of the special linear group, then $\lambda^2 \equiv 1 \mod p$. Then, $p \mid (\lambda-1)(\lambda+1)$ hence $\lambda \equiv \pm 1 \mod p$. Thus,

$$Z \cap SL_2\left(\mathbb{Z}/p\mathbb{Z}\right) = \{\pm I\}$$

and $\pm I$ are distinct since $p > 2$.

Hence the order of the projective special linear group is half the order of the special linear group as required. $\square$

Example 5.2

Let $G = PSL_2\left(\mathbb{Z}/5\mathbb{Z}\right)$. Then by the previous lemma, $|G| = 60$. Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ by Möbius transformations. The permutation representation $\varphi : G \to \mathrm{Sym}(\{0,1,2,3,4,\infty\}) \cong S_6$ is injective by Lemma 5.1.

Claim 5.1

$\mathrm{Im}\,\varphi \subseteq A_6$, i.e. $\psi : G \xrightarrow{\varphi} S_6 \xrightarrow{\mathrm{sgn}} \{\pm 1\}$ is trivial.

Proof. Let $h \in G$, and suppose h has order $2^n m$ for odd m and so $o(h^m) = 2^n$. If $\psi(h^m) = 1$, then since ψ is a group homomorphism we have $\psi(h)^m = 1$ giving $\psi(h) \neq -1 \implies \psi(h) = 1$.

So to show ψ is trivial, it suffices to show $\psi(g) = 1$ for all $g \in G$ with order a power of 2.

By Lemma 4.2, if g has order a power of 2, it is contained in a Sylow 2-subgroup. Then it suffices to show that $\psi(H) = 1$ for all Sylow 2-subgroups H. But since $\ker \psi \triangleleft G$ and all Sylow 2-subgroups are conjugate, it suffices to show $\psi(H) = 1$ for a single Sylow 2-subgroup H.

The Sylow 2-subgroup must have order 4. Hence consider

$$H = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \{\pm I\}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \{\pm I\} \right\rangle$$

Both of these elements square to the identity element inside the projective special linear group. This generates a group of order 4 which is necessarily a Sylow 2-subgroup. We can explicitly compute the action of H on $\{0, 1, 2, 3, 4, \infty\}$.

$$\varphi\left(\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\right) = (1\ 4)(2\ 3); \quad \varphi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = (0\ \infty)(1\ 4)$$

These are products of two transpositions, hence even permutations. Thus $\psi(H) = 1$, proving the claim that $G \leq A_6$. □

We can prove that for any $G \leq A_6$ of order 60, we have $G \cong A_5$; this is a question from the example sheets.

§5.3 Properties

The following properties will not be proven in this course.

- $PSL_n\left(\mathbb{Z}/p\mathbb{Z}\right)$ is simple for all $n \geq 2$ and p prime, except where $n = 2$ and $p = 2, 3$. Such groups are called finite groups of *Lie type*.
- The smallest non-abelian simple groups are $A_5 \cong PSL_2\left(\mathbb{Z}/5\mathbb{Z}\right)$, then $PSL_2\left(\mathbb{Z}/7\mathbb{Z}\right) \cong GL_3\left(\mathbb{Z}/2\mathbb{Z}\right)$ which has order 168.

§6 Finite abelian groups

§6.1 Products of cyclic groups

Theorem 6.1

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

The proof for this theorem will be provided later in the course. Note that the isomorphism provided for by the theorem is not unique. An example of such behaviour is the following lemma.

Lemma 6.1

Let $m, n \in \mathbb{N}$ be coprime integers. Then $C_m \times C_n \cong C_{mn}$.

Proof. Let g, h be generators of C_m and C_n. Then consider the element $(g, h)^k = (g^k, h^k)$, which has order mn. Thus $\langle (g, h) \rangle$ has order mn. So every element in $C_m \times C_n$ is expressible in this way, giving $\langle (g, h) \rangle = C_m \times C_n$. $\square$

Corollary 6.1

Let G be a finite abelian group. Then $G \cong C_{n_1} \times \cdots \times C_{n_k}$ where each n_i is a power of a prime.

Proof. If $n_i = p_1 a^1 \cdots p^r a^r$ where the p_i are distinct primes, then applying Lemma 6.1 inductively gives C_{n_i} as a product of cyclic groups which have orders that are powers of primes.

We can apply this to the theorem that every finite abelian group is isomorphic to a product of cyclic groups to find the result. $\square$

Later, we will prove the following refinement of Theorem 6.1

Theorem 6.2

Let G be a finite abelian group. Then $G \cong C_{d_1} \times \cdots \times C_{d_t}$ where $d_i \mid d_{i+1}$ for all i.

Remark 12. The integers $n_1, \ldots, n_k$ in Corollary 6.1 are unique up to ordering. The integers $d_1, \ldots, d_t$ in Theorem 6.2 are also unique, assuming that $d_1 > 1$. The proofs will be omitted - but works by counting the number of elements of G of each prime power order.

Example 6.1

The abelian groups of order 8 are exactly C_8, $C_2 \times C_4$, and $C_2 \times C_2 \times C_2$.

Example 6.2

The abelian groups of order 12 are, using the corollary Corollary 6.1, $C_2 \times C_2 \times C_3$, $C_4 \times C_3$, and using Theorem 6.2, $C_2 \times C_6$ and C_{12}. However, $C_2 \times C_3 \cong C_6$ and $C_3 \times C_4 \cong C_{12}$, so the groups derived are isomorphic.

Definition 6.1 (Exponent)

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

Example 6.3

The exponent of A_4 is $\operatorname{lcm}\{2, 3\} = 6$.

Corollary 6.2 (Structure Theorem)

Let G be a finite abelian group. Then G contains an element which has order equal to the exponent of G.

Proof. If $G \cong C_{d_1} \times \cdots \times C_{d_t}$ for $d_i \mid d_{i+1}$, every $g \in G$ has order dividing d_t. Hence the exponent is d_t, and we can choose a generator of C_{d_t} to obtain an element in G of the same order[a]. □

[a] Say $o(h) = d_t$ with $h \in C_{d_t}$ then $(e, e, \ldots, e, h) \in G$ and has order d_t

Part II
Rings

§7 Rings

§7.1 Definitions

Definition 7.1 (Ring)

A **ring** is a triple $(R, +, \cdot)$ where R is a set and $+, \cdot$ are binary operations $R \times R \to R$, satisfying the following axioms.

1. $(R, +)$ is an abelian group, and we will denote the identity element 0 and the inverse of x as $-x$;
2. $(R, \cdot)$ satisfies the group axioms except for the invertibility axiom, and we will denote the identity element 1 and the inverse of x as x^{-1} if it exists;
3. for all $x, y, z \in R$ we have $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

If multiplication is commutative, we say that R is a **commutative** ring.

In this course, we will study only commutative rings.

Remark 13. For all $x \in R$,

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

Further,

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

Remark 14. Addition being commutative follows from distributive law and the other axioms so not necessary for it to be an abelian group.

Definition 7.2 (Subring)

A subset $S \subset R$ is a **subring**, denoted $S \leq R$, if $(S, +, \cdot)$ is a ring with the same identity elements.

Remark 15. It suffices to check the closure axioms for addition and multiplication; the other properties are inherited.

Example 7.1

$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ are rings. The set $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. This is known as the ring of Gaussian integers.

Example 7.2

The set $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ is a subring of $\mathbb{R}$.

Example 7.3

The set $\mathbb{Z}/n\mathbb{Z}$ is a ring.

Example 7.4

Let R, S be rings. Then the **product** $R \times S$ is a ring under the binary operations

$$(a, b) + (c, d) = (a + c, b + d); \quad (a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$$

The additive identity is $(0_R, 0_S)$ and the multiplicative identity is $(1_R, 1_S)$.

Note that the subset $R \times \{0\}$ is preserved under addition and multiplication, so it is a ring, but it is not a subring because the multiplicative identity is different.

§7.2 Polynomials

Definition 7.3 (Polynomial)

Let R be a ring. A **polynomial** f over R is an expression

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

for $a_i \in R$. The term X is a formal symbol, no substitution of X for a value will be made. We could alternatively define polynomials as finite sequences of terms in R.

The **degree** of a polynomial f is the largest n such that $a_n \neq 0$. A degree-n polynomial is **monic** if $a_n = 1$. We write $R[X]$ for the set of all such polynomials over R.

Let $g = b_0 + b_1 X + \cdots + b_n X^n$. Then we define

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n; \quad f \cdot g = \sum_i \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i$$

Then $(R[X], +, \cdot)$ is a ring. The identity elements are the constant polynomials 0 and 1. We can identify the ring R with the subring of $R[X]$ of constant polynomials.

Definition 7.4 (Unit)

An element $r \in R$ is a **unit** if r has a multiplicative inverse. The units in a ring, denoted $R^\times$, form an abelian group under multiplication.

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

Definition 7.5 (Field)

A **field** is a ring where all nonzero elements are units and $0 \neq 1$.

Example 7.5

$\mathbb{Z}/_{n\mathbb{Z}}$ is a field iff n is a prime.

Remark 16. If R is a ring such that $0 = 1$, then every element in the ring is equal to zero. Indeed, $x = 1 \cdot x = 0 \cdot x = 0$. Thus, the exclusion of rings with $0 = 1$ in the definition of a field simply excludes the trivial ring.

Proposition 7.1

Let $f, g \in R[X]$ such that the leading coefficient of g is a unit. Then there exist polynomials $q, r \in R[X]$ such that $f = qg + r$, where $\deg r < \deg g$.

Remark 17. This is the Euclidean algorithm for division, adapted to polynomial rings.

Proof. Let $n = \deg f$ and $m = \deg g$, so by induction on n

$$f = a_n X^n + \dots + a_0; \quad g = b_m X^m + \dots + b_0$$

By assumption, $b_m \in R^\times$.

If $n < m$ then let $q = 0$ and $r = f$.

Conversely, we have $n \geq m$. Consider the polynomial $f_1 = f - a_n b_m^{-1} X^{n-m} g$. This has degree at most $n - 1$. Hence, we can use induction on n to decompose f_1 as $f_1 = q_1 g + r$. Thus $f = (q_1 + a_n b_m^{-1} X^{n-m})g + r$ as required. $\square$

Remark 18. If R is a field, then every nonzero element of R is a unit. Therefore, the above algorithm can be applied for all polynomials g unless g is the constant polynomial zero.

Example 7.6

Let R be a ring and X be a set. Then the set of functions $X \to R$ is a ring under

$$(f+g)(x) = f(x) + g(x); \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

The set of continuous functions $\mathbb{R} \to \mathbb{R}$ is a subring of the ring of all functions $\mathbb{R} \to \mathbb{R}$, since they are closed under addition and multiplication. The set of polynomial functions $\mathbb{R} \to \mathbb{R}$ is also a subring, and we can identify this with the ring $\mathbb{R}[X]$.

Example 7.7

Let R be a ring. Then the *power series ring* $R[\![X]\!] = \{a_0 + a_1 X + a_2 X^2 + \dots a_i \in R\}$ is the set of power series over R. This is defined similarly to the polynomial ring, but we permit infinitely many nonzero elements in the expansion. The power series is defined formally; we cannot actually carry out infinitely many additions in an arbitrary ring. We instead consider the power series as a sequence of numbers.

Example 7.8

Let R be a ring. Then the ring of *Laurent polynomials* is $R[X, X^{-1}] = \{\sum_{i \in \mathbb{Z}} a_i X^i : a_i \in \mathbb{R}\}$ with the restriction that $a_i \neq 0$ only for finitely many i.

§8 Homomorphisms, Ideals and Quotients

§8.1 Homomorphisms

Definition 8.1 (Ring Homomorphism)

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

1. $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$;
2. $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$;
3. $\varphi(1_R) = 1_S$.

We can derive that $\varphi(0_R) = 0_S$ from (i).

Definition 8.2 (Isomorphism)

A ring homomorphism is an **isomorphism** if it is bijective.

Definition 8.3 (Kernel)

The **kernel** of a ring homomorphism is $\ker\varphi = \{r \in R : \varphi(r) = 0\}$.

Lemma 8.1

Let R, S be rings. Then a ring homomorphism $\varphi : R \to S$ is injective iff $\ker\varphi = \{0\}$.

Proof. Let $\varphi : (R, +) \to (S, +)$ be the induced group homomorphism on addition. The result then follows from the corresponding fact about group homomorphisms. □

§8.2 Ideals

Definition 8.4 (Ideal)

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

1. I is a subgroup of $(R, +)$;
2. if $r \in R$ and $x \in I$, then $rx \in I$.

Definition 8.5 (Proper Ideal)

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

Lemma 8.2

Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker\varphi$ is an ideal of R.

Proof. Considering the induced group homomorphism on addition, $\varphi : (R, +) \to (S, +)$, $\ker\varphi$ is a subgroup of $(R, +)$.

If $r \in R$ and $x \in \ker\varphi$, then

$$\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0$$

Hence $rx \in \ker\varphi$. □

Remark 19. If I contains a unit, then the multiplicative identity lies in I. Then all elements lie in I. In particular, if I is a proper ideal, $1 \notin I$. Hence a proper ideal I is not a subring of R.

Lemma 8.3

The ideals in $\mathbb{Z}$ are precisely the subsets of the form $n\mathbb{Z}$ for any $n = 0, 1, 2, \ldots$.

Proof. First, we can check directly that any subset of the form $n\mathbb{Z}$ is an ideal. Now, let I be any nonzero ideal of $\mathbb{Z}$ and let n be the smallest positive element in I. Then $n\mathbb{Z} \subseteq I$. Let $m \in I$. Then by the Euclidean algorithm, $m = qn + r$ for $q, r \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Then $r = m - qn$. We know $qn \in I$ since $n \in I$, so $r \in I$. If $r \neq 0$, this contradicts the minimality of n as chosen above. So $I = n\mathbb{Z}$ exactly. □

Definition 8.6 (Generated Ideals)

For an element $a \in R$, we write (a) to denote the subset of R given by multiples of a; that is $(a) = \{ra : r \in R\}$. This is an ideal, known as the **ideal generated by** a. More generally, if $a_1, \ldots, a_n \in R$, then $(a_1, \ldots, a_n) = \{r_1 a_1 + \ldots r_n a_n : r_i \in R\}$ is the set of elements in R given by linear combinations of the a_i. This is also an ideal.

Definition 8.7 (Prinipal Ideal)

Let $I \lhd R$. Then I is **principal** if there exists some $a \in R$ such that $I = (a)$.

§8.3 Quotients

Theorem 8.1

Let $I \lhd R$. Then the set ${}^{R}\!/_{I}$ of cosets[a] of I in $(R, +)$ forms the **quotient ring** under the operations

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

This ring has the identity elements

$$0_{R/I} = 0_R + I; \quad 1_{R/I} = 1_R + I$$

Further, the map $R \to {}^{R}\!/_{I}$ defined by $r \mapsto r + I$ is a ring homomorphism called the **quotient map**. The kernel of the quotient map is I. Hence any ideal is the kernel of some homomorphism.

[a] Left or right cosets, doesn't matter which.

Proof. From the analogous result from groups, the addition defined on the set of cosets yields the group $\left({}^{R}\!/_{I}, +\right)$. If $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$, then $r_1' = r_1 + a_1$ and $r_2' = r_2 + a_2$ for some $a_1, a_2 \in I$. Then

$$r_1'r_2' = (r_1 + a_1)(r_2 + a_2) = r_1r_2 + \underbrace{a_1r_2}_{\in I}{}^{a} + \underbrace{r_1a_2}_{\in I} + \underbrace{a_1a_2}_{\in I}$$

Hence $(r_1'r_2') + I = (r_1r_2) + I$. So the operations are well defined.

Remaining properties for ${}^{R}\!/_{I}$ follows from those for R. The remainder of the proof is trivial. □

[a] Recall we only consider commutative rings in this course so $a_1r_2 = r_2a_1$.

Example 8.1

In the integers $\mathbb{Z}$, the ideals are $n\mathbb{Z}$. Hence we can form the quotient ring ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. The ring ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ has elements $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. Addition and multiplication behave like in modular arithmetic modulo n.

Example 8.2

Consider the ideal (X) inside the polynomial ring $\mathbb{C}[X]$. This ideal is the set of polynomials with zero constant term. Let $f(X) = a_nX^n + \cdots + a_0$ be an arbitrary element of $\mathbb{C}[X]$, $a_nX^n, \ldots, a_1X^1 \in (X)$. Then $f(X) + (X) = a_0 + (X)$.
Thus, there exists a bijection between ${}^{\mathbb{C}[X]}\!/_{(X)}$ and $\mathbb{C}$, defined by $f(x) + (X) \mapsto f(0)$, with inverse $a \mapsto a + (X)$. This bijection is a ring homomorphism, hence ${}^{\mathbb{C}[X]}\!/_{(X)} \cong \mathbb{C}$.

Example 8.3

Consider $(X^2 + 1) \lhd \mathbb{R}[X]$, ${}^{\mathbb{R}[X]}\!/_{(X^2+1)} = \{f(X) + (X^2 + 1) : f(X) \in \mathbb{R}[X]\}$. For $f(X) = a_nX^n + \cdots + a_0 \in \mathbb{R}[X]$, by Proposition 7.1 we can apply the Euclidean algorithm to write $f(X) = q(X)(X^2 + 1) + r(X)$ where $\deg r < 2$. Hence $r(X) = a + bX$ for $a, b \in \mathbb{R}$.

Thus, any element of ${}^{\mathbb{R}[X]}\!/_{(X^2+1)}$ can be written $a + bX + (X^2 + 1)$. Suppose a coset can be represented by two representatives: $a + bX + (X^2 + 1) = a' + b'X + (X^2 + 1)$. Then,

$$a + bX - a' - b'X = (a - a') - (b - b')X = g(X)(X^2 + 1)$$

Hence $g(X) = 0$, giving $a - a' = 0$ and $b - b' = 0$. Hence the coset representative is unique.

Consider the bijection φ between this quotient ring and the complex numbers given by $a+bX+(X^2+1) \mapsto a+bi$. We can show that φ is a ring homomorphism. Indeed, it preserves addition, and $1+(X^2+1) \mapsto 1$, so it suffices to check that multiplication is preserved.

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

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

§8.4 Isomorphism theorems

Theorem 8.2 (First Isomorphism Theorem)
Let $\varphi : R \to S$ be a ring homomorphism. Then,

$$\ker\varphi \triangleleft R; \quad \operatorname{Im}\varphi \leq S; \quad {}^{R}\!/\!_{\ker\varphi} \cong \operatorname{Im}\varphi$$

Proof. We already saw that $\ker\varphi \triangleleft R$, Lemma 8.2.

We know that $\operatorname{Im}\varphi \leq (S,+)$. Now we show that $\operatorname{Im}\varphi$ is closed under multiplication.

$$\varphi(r_1)\varphi(r_2) = \varphi(r_1r_2) \in \operatorname{Im}\varphi$$

Finally,

$$1_S = \varphi(1_R) \in \operatorname{Im}\varphi$$

Hence $\operatorname{Im}\varphi$ is a subring of S.

Let $K = \ker\varphi$. Then, we define $\Phi : {}^{R}\!/\!_{K} \to \operatorname{Im}\varphi$ by $r+K \mapsto \varphi(r)$. By appealing to the first isomorphism theorem from groups, this is well-defined, a bijection, and a group homomorphism under addition. It therefore suffices to show that Φ preserves multiplication and maps the multiplicative identities to each other.

$$\begin{aligned}
\Phi(1_R+K) &= \varphi(1_R) = 1_S \\
\Phi((r_1+K)(r_2+K)) &= \Phi(r_1r_2+K) \\
&= \varphi(r_1r_2)
\end{aligned}$$

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

The result follows as required. □

Theorem 8.3 (Second Isomorphism Theorem)
Let $R \leq S$ and $J \triangleleft S$. Then,

$$
\begin{aligned}
R \cap J &\triangleleft R \\
R + J &= \{r + a : r \in R, a \in J\} \leq S \\
{}^{R}\!/_{R \cap J} &\cong {}^{(R+J)}\!/_{J} \leq {}^{S}\!/_{J}
\end{aligned}
$$

Proof. By the second isomorphism theorem for groups, $R + J \leq (S, +)$. Further, $1_S = 1_S + 0_S$, and since R is a subring, $1_S + 0_S \in R + J$ hence $1_S \in R + J$.

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

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

Hence $R + J$ is closed under multiplication, giving $R + J \leq S$.

Let $\varphi : R \to {}^{S}\!/_{J}$ be defined by $r \mapsto r + J$. This is a ring homomorphism, since it is the composite of the inclusion homomorphism $R \subseteq S$[a] and the quotient map $S \to {}^{S}\!/_{J}$. The kernel of φ is the set $\{r \in R : r + J = J\} = R \cap J$. Since this is the kernel of a ring homomorphism, $R \cap J$ is an ideal in R. The image of φ is

$$
\{r + J \mid r \in R\} = {}^{(R+J)}\!/_{J} \leq {}^{S}\!/_{J}.
$$

By the first isomorphism theorem, ${}^{R}\!/_{R \cap J} \cong {}^{(R+J)}\!/_{J}$ as required. □

[a] This is just $r \mapsto r$ for $r \in R$.

Remark 20. If $I \triangleleft R$, there exists a bijection between ideals in ${}^{R}\!/_{I}$ and the ideals of R containing I. Explicitly,

$$
\begin{aligned}
K &\leftarrow\!\shortmid \{r \in R \mid r + I \in K\} \\
{}^{J}\!/_{I} &\mapsto J
\end{aligned}
$$

Theorem 8.4 (Third Isomorphism Theorem)

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

$$J/I \lhd R/I$$
$$\left.R/I\middle/J/I\right. \cong R/J$$

Proof. Let $\varphi : R/I \to R/J$ defined by $r + I \mapsto r + J$. We can check that this is a surjective ring homomorphism (well-defined since $I \subseteq J$) by considering the third isomorphism theorem for groups. Its kernel is $\{r + I : r \in J\} = J/I$, which is an ideal in R/I, and we conclude by use of the first isomorphism theorem. □

Remark 21. J/I is not a quotient ring, since J is not in general a ring; this notation should be interpreted as a set of cosets.

Example 8.4

Consider the surjective ring homomorphism $\varphi : \mathbb{R}[X] \to \mathbb{C}$ which is defined by

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

Its kernel can be found by the Euclidean algorithm due to Proposition 7.1, yielding $\ker \varphi = (X^2 + 1)$. Applying the first isomorphism theorem, we immediately find $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

Example 8.5

Let R be a ring. Then there exists a unique ring homomorphism $i : \mathbb{Z} \to R$. Indeed, we must have

$$0_\mathbb{Z} \mapsto 0_R; \quad 1_\mathbb{Z} \mapsto 1_R$$

This inductively defines

$$n \mapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}$$

The negative integers are also uniquely defined, since any ring homomorphism is a group homomorphism.

$$-n \mapsto -(\underbrace{1_R + \cdots + 1_R}_{n \text{ times}})$$

We can show that any such construction is a ring homomorphism as required.

Then, the kernel of the ring homomorphism is an ideal of $\mathbb{Z}$, hence it is $n\mathbb{Z}$ for some n. Hence, by the first isomorphism theorem, any ring contains a copy of $\mathbb{Z}/n\mathbb{Z}$, since it is isomorphic to the image of i. If $n = 0$, then the ring contains a copy of $\mathbb{Z}$ itself, and if $n = 1$, then the ring is trivial since $0 = 1$.

Definition 8.8 (Characteristic)

The number n is known as the **characteristic** of R.

Example 8.6

For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic zero. The rings $\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}[X]$ have characteristic p.

§9 Integral domains, maximal ideals and prime ideals

§9.1 Integral domains

Definition 9.1 (Integral Domain)

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

Definition 9.2 (Zero-Divisor)

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

A ring is an integral domain iff it has no zero divisors.

Example 9.1

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

Example 9.2

Any subring of an integral domain is an integral domain. For instance, $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Z}[i] \leq \mathbb{C}$ are integral domains.

Example 9.3

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

Lemma 9.1

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

Proof. We will show that any two nonzero elements produce a nonzero element. In particular, let

$$f = \sum_n a_n X^n; \quad g = \sum_n b_n X^n$$

Since these are nonzero, the leading coefficients a_n and b_m are nonzero. Here, the leading term of the product fg has form $a_n b_m X^{n+m}$. Since R is an integral domain, $a_n b_m \neq 0$, so fg is nonzero.

Further, the degree of fg is $n + m$, the sum of the degrees of f and g. $\square$

Lemma 9.2

Let R be an integral domain, and $f \neq 0$ be a nonzero polynomial in $R[X]$. We define $\mathrm{roots}(f) = \{a \in R : f(a) = 0\}$. Then $|\mathrm{roots}(f)| \leq \deg(f)$.

Proof. Exercise on the Sheet 2. The main idea is to use the Euclidean algorithm on a root to extract out the linear factors. $\square$

Theorem 9.1

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

Proof. G is a finite abelian group. If G is not cyclic, we can apply Theorem 6.2 for finite abelian groups to show that there exists $H \leq G$ such that $H \cong C_{d_1} \times C_{d_1}$ [a] for some integer $d_1 \geq 2$. The polynomial $f(X) = X^{d_1} - 1 \in F[X]$ has degree d_1, but has at least d_1^2 roots, since any element of H is a root. This contradicts the previous lemma, Lemma 9.2. $\square$

[a] We get from the theorem $G \cong \prod_i C_{d_i}$, as G not cyclic wlog $d_1 \mid d_2$ and so there exists a subgroup $C_{d_1} \leq C_{d_2}$.

Example 9.4

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

Proposition 9.1

Any finite integral domain is a field.

Proof. Let $0 \neq a \in R$, where R is an integral domain. Consider the map $\varphi : R \to R$ given by $x \mapsto ax$.

If $\varphi(x) = \varphi(y)$, then $a(x-y) = 0$. But $a \neq 0$, hence $x - y = 0$ as R is an integral domain. Hence φ is injective. Since R is finite, φ is surjective so $\exists\, b$ s.t. $ab = 1$, i.e. a is a unit. This may be repeated for all a, thus R is a field. $\square$

Theorem 9.2

Let R be an integral domain then $\exists$ a field F s.t.

1. $R \leq F$
2. Every element of F can be written in the form ab^{-1} where $a, b \in R$ and $b \neq 0$.

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

Proof. Consider the set $S = \{(a,b) \in R^2 : b \neq 0\}$. We can define an equivalence relation

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

This is reflexive and symmetric. We can show directly that it is transitive.

$$\begin{aligned}(a,b) \sim (c,d) \sim (e,f) &\implies ad = bc;\ cf = de \\ &\implies adf = bcf = bde \\ &\implies d(af - be) = 0 \\ &\implies (a,b) \sim (e,f) \text{ as } d \neq 0 \text{ and } R \text{ an integral domain.}\end{aligned}$$

Hence $\sim$ is indeed an equivalence relation. Now, let $F = S/\sim$, and we write $\frac{a}{b}$ for the class $[(a,b)]$. We define the ring operations

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

These can be shown to be well-defined. Thus, F is a ring with identities $0_F = \frac{0_R}{1_R}$ and $1_F = \frac{1_R}{1_R}$.

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

1. We can identify R with the subring of F given by $\left\{\frac{r}{1_R} : r \in R\right\} \leq F$. This is clearly isomorphic to R.

2. Further, any element of F can be written as $\frac{a}{b} = ab^{-1}$ as required. □

This is analogous to the construction of the rationals using the integers.

Example 9.5

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

Example 9.6

Consider $\mathbb{C}[X]$. This has field of fractions $\mathbb{C}(X)$, called the field of *rational functions* in X.

§9.2 Maximal ideals

Definition 9.3 (Maximal Ideal)

An ideal $I \triangleleft R$ is **maximal** if $I \neq R$ and, if $I \subseteq J \triangleleft R$, we have $J = I$ or $J = R$.

So a maximal ideal is the largest proper ideal.

Lemma 9.3

A nonzero ring R is a field iff its only ideals are zero or R.

Proof. ($\Longrightarrow$): Suppose R is a field. If $0 \neq I \triangleleft R$, then I contains a nonzero element, which is a unit since R is a field. We have seen that an ideal containing a unit implies it is the whole ring, hence $I = R$.

($\Longleftarrow$): Now, suppose a ring R has ideals that are only zero or R. If $0 \neq x \in R$, consider (x). This is nonzero since it contains x. By assumption, $(x) = R$. Thus, the element 1 lies in (x). Hence, there exists $y \in R$ such that $xy = 1$, and hence this y is the multiplicative inverse as required. □

Proposition 9.2

Let $I \triangleleft R$. Then I is maximal iff ${}^{R}\!/_{I}$ is a field.

Proof. ${}^{R}\!/_{I}$ is a field iff its ideals are either zero, denoted ${}^{I}\!/_{I}$[a], or ${}^{R}\!/_{I}$ itself. By Remark 20, I and R are the only ideals in R which contain I. Equivalently, $I \triangleleft R$

is maximal. ∎

[a] This is not a ring but the set of cosets given by elements of I.

§9.3 Prime ideals

Definition 9.4 (Prime Ideals)

An ideal $I \triangleleft R$ is **prime** if $I \neq R$ and for all $a, b \in R$ such that $ab \in I$, we have $a \in I$ or $b \in I$.

Example 9.7

The ideals in the integers are $n\mathbb{Z}$ for some $n \geq 0$. $n\mathbb{Z}$ is a prime ideal iff n is prime or zero.

The case for $n = 0$ is trivial.

If $n \neq 0$ we can use the property that $p \mid ab$ implies either $p \mid a$ or $p \mid b$. So if $ab \in p\mathbb{Z}$ then $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Conversely, if n is composite, we can write $n = uv$ for $u, v > 1$. Then $uv \in n\mathbb{Z}$ but $u, v \notin n\mathbb{Z}$.

Proposition 9.3

Let $I \triangleleft R$. Then I is prime iff ${R}/{I}$ is an integral domain.

Proof. If I is prime, then for all $ab \in I$ we have $a \in I$ or $b \in I$. Equivalently, for all $a + I, b + I \in {R}/{I}$, we have $(a + I)(b + I) = 0 + I$ if $a + I = 0 + I$ or $b + I = 0 + I$. This is the definition of an integral domain. ∎

Remark 22. If I is a maximal ideal, then ${R}/{I}$ is a field by proposition 9.2. A field is an integral domain. Hence any maximal ideal is prime.

Remark 23. If the characteristic of a ring is n, then ${\mathbb{Z}}/{n\mathbb{Z}} \leq R$. In particular, if R is an integral domain, then ${\mathbb{Z}}/{n\mathbb{Z}}$ must be an integral domain. Equivalently, $n\mathbb{Z} \triangleleft \mathbb{Z}$ is a prime ideal. Hence n is zero or prime. Thus, in an integral domain, the characteristic must either be zero or prime.
In particular, a field always has a characteristic, which is either zero (in which case it contains $\mathbb{Z}$ and hence $\mathbb{Q}$) or prime (in which case it contains ${\mathbb{Z}}/{p\mathbb{Z}} = \mathbb{F}_p$ which is already a field).

§10 Factorisation in integral domains

In this section, let R be an integral domain.

§10.1 Prime and irreducible elements

Recall that an element $a \in R$ is a unit if it has a multiplicative inverse in R. Equivalently, an element a is a unit if and only if $(a) = R$. Indeed, if $(a) = R$, then $1 \in (a)$ hence there exists a multiple of a equal to 1. We denote the set of units in R by $R^\times$.

Definition 10.1 (Divides)

An element $a \in R$ **divides** $b \in R$, written $a \mid b$, if there exists $c \in R$ such that $b = ac$. Equivalently, $(b) \subseteq (a)$.

Definition 10.2 (Associates)

Two elements $a, b \in R$ are **associates** if $a = bc$ where c is a unit. Informally, the two elements differ by multiplication by a unit. Equivalently, $(a) = (b)$.

Definition 10.3

An element $r \in R$ is **irreducible** if $r \neq 0$ is not a unit, and $r = ab$ implies a or b is a unit.

Definition 10.4 (Prime)

An element $r \in R$ is **prime** if $r \neq 0$ is not a unit and $\underline{r \mid ab \text{ implies } r \mid a \text{ or } r \mid b}$.

Remark 24. These properties depend on the ambient ring R; for instance, 2 is prime and irreducible in $\mathbb{Z}$, but neither prime nor irreducible in $\mathbb{Q}$ as it's a unit.
The polynomial $2X$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{Z}[X]$.

Lemma 10.1

$(r) \triangleleft R$ is a prime ideal iff $r = 0$ or r is prime.

Proof. ($\implies$): Suppose (r) is a prime ideal with $r \neq 0$. Since prime ideals are proper, r cannot be a unit. Suppose $r \mid ab$, or equivalently, $ab \in (r)$. By the definition of a prime ideal, $a \in (r)$ or $b \in (r)$. Hence, $r \mid a$ or $r \mid b$. By definition of a prime element, r is prime.

($\Longleftarrow$): Conversely, first note that the zero ideal $(0) = \{0\}$ is a prime ideal, since R is an integral domain.
Suppose r is prime. We know $(r) \neq R$ since r is not a unit. If $ab \in (r)$, then $r \mid ab$, so $r \mid a$ or $r \mid b$, giving $a \in (r)$ or $b \in (r)$ as required for (r) to be a prime ideal. $\square$

Lemma 10.2

Prime elements are irreducible.

Proof. Let r be prime. Then r is nonzero and not a unit. Suppose $r = ab$. Then, in particular, $r \mid ab$, so $r \mid a$ or $r \mid b$ by primality. Let $r \mid a$ without loss of generality. Hence $a = rc$ for some element $c \in R$. Then, $r = ab = rcb$, so $r(1 - cb) = 0$. Since R is an integral domain, and $r \neq 0$, we have $cb = 1$, so b is a unit. $\square$

Example 10.1

The converse does not hold in general. Let

$$R = \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\} \leq \mathbb{C}; \quad R \cong {}^{\mathbb{Z}[X]}\!\big/_{(X^2 + 5)}$$

Since R is a subring of the field $\mathbb{C}$, it is an integral domain. We can define the *norm* $N : R \to \mathbb{Z}$ by $N(a + b\sqrt{-5}) = a^2 + 5b^2 \geq 0$. Note that this norm is multiplicative: $N(z_1 z_2) = N(z_1)N(z_2)$.

We claim that the units are exactly ± 1. Indeed, if $r \in R^\times$, then $rs = 1$ for some element $s \in R$. Then, $N(r)N(s) = N(1) = 1$, so $N(r) = N(s) = 1$. But the only elements $r \in R$ with $N(r) = 1$ are $r = \pm 1$.

We will now show that the element $2 \in R$ is irreducible. Suppose $2 = rs$ for $r, s \in R$. By the multiplicative property of N, $N(2) = 4 = N(r)N(s)$ can only be satisfied by $N(r), N(s) \in \{1, 2, 4\}$. Since $a^2 + 5b^2 = 2$ has no integer solutions, R has no elements of norm 2. Hence, either r or s has unit norm and is thus a unit by the above discussion. We can show similarly that $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible, as there exist no elements of norm 3.

We can now compute directly that $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$, hence $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$. But $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$, which can be checked by taking norms. Hence, 2 is irreducible but not a prime.

Takeaways
So here is an example showing irreducible $\not\Longrightarrow$ prime
In order to construct this example, we have exhibited two factorisations of 6 into irreducibles: $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. Since $R^\times = \{\pm 1\}$, these irreducibles in the factorisations are not associates.

§10.2 Principal ideal domains

Definition 10.5 (Principal Ideal Domain)

An integral domain R is a **principal ideal domain** (PID) if all ideals are principal ideals. In other words, for all ideals $I \lhd R$, there exists an element r such that $I = (r)$.

Example 10.2

$\mathbb{Z}$ is a principal ideal domain by Lemma 8.3.

Proposition 10.1

In a principal ideal domain, all irreducible elements are prime.

Proof. Let $r \in R$ be irreducible, and suppose $r \mid ab$. If $r \mid a$, the proof is complete, so suppose $r \nmid a$.

Since R is a principal ideal domain, the ideal (a, r) is generated by a single element $d \in R$. In particular, since $r \in (d)$, we have $d \mid r$ so $r = cd$ for some $c \in R$.

Since r is irreducible, either c or d is a unit. If c is a unit, $(a, r) = (d) = (r)$, so in particular $r \mid a$, which contradicts the assumption that $r \nmid a$, so c cannot be a unit. Thus, d is a unit. In this case, $(a, r) = R$. By definition of (a, r), there exist $s, t \in R$ such that $1 = sa + tr$. Then, $b = sab + trb$. We have $r \mid sab$ since $r \mid ab$, and we know $r \mid trb$. Hence $r \mid b$ as required. □

Lemma 10.3

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

Proof. ($\implies$): Since r is not a unit, $(r) \neq R$.
Suppose $(r) \subseteq J \subseteq R$ where J is an ideal in R. Since R is a principal ideal domain, $J = (a)$ for some $a \in R$. In particular, $r = ab$ for some $b \in R$, since $(r) \subseteq J$. Since r is irreducible, either a or b is a unit. But if a is a unit, we have $J = R$. If b is a unit, then a and r are associates so they generate the same ideal. Hence, (r) is maximal.

($\impliedby$): Note that r is not a unit, since $(r) \neq R$. Suppose $r = ab$. Then $(r) \subseteq (a) \subseteq R$. But since (r) is maximal, either $(a) = (r)$ or $(a) = R$. If $(a) = (r)$, then b is a unit. If $(a) = R$, then a is a unit. Hence r is irreducible. □

Remark 25. 1. The converse direction doesn't depend on R being a PID only that it's an integral domain.

2. If R is a PID and $0 \neq r \in R$. Then, (r) is maximal iff r is irreducible (Lemma 10.3), which is true iff r is prime (Lemma 10.2 and proposition 10.1), which is equivalent to the fact that (r) is prime (Lemma 10.1). Hence, the maximal ideals are the nonzero prime ideals.

Definition 10.6 (Euclidean Domain)

An integral domain is a **Euclidean domain** if there exists a function $\varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that, for all $a, b \in R$.

1. If $a \mid b$ then $\varphi(a) \leq \varphi(b)$;
2. If $b \neq 0$ then $\exists\, q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.

Such a φ is called a **Euclidean function**.

Example 10.3

$\mathbb{Z}$ is a Euclidean domain, where the Euclidean function φ is the absolute value function.

Proposition 10.2

Euclidean domains are principal ideal domains.

Proof. Let R have Euclidean function φ. Let $I \lhd R$ be a nonzero ideal.
Let $b \in I \setminus \{0\}$ that minimises $\varphi(b)$. Then $(b) \subseteq I$.
For any element $a \in I$, we can use the Euclidean algorithm to show $a = bq + r$ where $r = 0$ or $\varphi(r) < \varphi(b)$. But since $r = a - bq \in I$, $\varphi(r)$ cannot be lower than the minimal element $\varphi(b)$. Thus $r = 0$, so $a = bq$. Hence, $I = (b)$, so all ideals are principal. □

Remark 26. In the above proof, only the second property of the Euclidean function was used. The first property is included in the definition since it will allow us to easily describe the units in the ring.

$$R^\times = \{u \in R : u \neq 0, \varphi(u) = \varphi(1)\}$$

It can be shown that, if there exists a function φ satisfying (ii), there exists a (possibly not unique) function φ' satisfying (i) and (ii).

Example 10.4

Let F be a field. Then $F[X]$ is a Euclidean domain with Euclidean function $\varphi(f) = \deg(f)$. The second property of Euclidean domains is proven using Proposition 7.1

whilst the first is easy to check.

So $F[X]$ is a PID by Proposition 10.2

Example 10.5

The ring $R = \mathbb{Z}[i]$ is a Euclidean domain with $\varphi(u + iv) = N(u + iv) = u^2 + v^2$. Since the norm is multiplicative, $N(zw) = N(z)N(w)$ which immediately gives property (i) in the definition.
Consider $z, w \in \mathbb{Z}[i]$ where $w \neq 0$. Consider $\frac{z}{w} \in \mathbb{C}$. This has distance less than 1 from the nearest element q of R, i.e. $|z/w - q| < 1$ as R is every complex point with integer components.
Let $r = z - wq \in R$. Then $z = wq + r$ where

$$\varphi(r) = |r|^2 = |z - wq|^2 < |w|^2 = \varphi(w)$$

So property (ii) is satisfied.

So $\mathbb{Z}[i]$ is a PID by Proposition 10.2

Example 10.6

Let A be a nonzero $n \times n$ matrix over a field F. Let $I = \{f \in F[X] : f(A) = 0\}$.

I is an ideal. Indeed, if $f, g \in I$, then $(f - g)(A) = f(A) - g(A) = 0$, and for $f \in I$ and $g \in F[X]$, we have $(f \cdot g)(A) = f(A) \cdot g(A) = 0$ as required.

Since $F[X]$ is a principal ideal domain, $I = (f)$ for some polynomial $f \in F[X]$. All units in $F[X]$ are the nonzero constant polynomials[a]. Hence, the polynomial of smallest degree in I is unique up to multiplication by a unit, so without loss of generality we may assume f is monic.

Then for $g \in F[X]$, $g(A) = 0 \iff g \in I = (f)$, i.e. $f \mid g$. Thus f is the minimal polynomial of A.

[a] Can check by looking at the first property of a Euclidean domain.

Example 10.7 (Field of order 8)

Let $\mathbb{F}_2$ be the finite field of order 2, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let $f(X)$ be the polynomial $X^3 + X + 1 \in \mathbb{F}_2[X]$.

We claim that f is irreducible. Suppose $f = gh$ where the degrees of g, h are positive. Since the degree of f is 3, one of g, h must have degree 1. Hence f has a root. But we can check that $f(0) = f(1) = 1$[a] so f has no root in $\mathbb{F}_2$. Hence f is irreducible as required.

Since $\mathbb{F}_2[X]$ is a principal ideal domain, we have that $(f) \triangleleft \mathbb{F}_2[X]$ is a maximal ideal by Lemma 10.3. Hence, $\mathbb{F}_2[X]/(f)$ is a field. We can verify that this field has order 8, using the Euclidean algorithm. Any element in this quotient is $aX^2+bX+c+(f)$ for $a, b, c \in \mathbb{F}_2$. We can show that all 8 of these possibilities yields different polynomials. So we have constructed a field of order 8. This technique will be explored further in Part II Galois Theory.

[a] Note you need to check $f(1) = f(3) = f(5) = \cdots = 0$ in $\mathbb{Z}$ i.e. $f(1) = 0$ in $\mathbb{F}_2$.

Example 10.8

The ring $\mathbb{Z}[X]$ is not a principal ideal domain. Consider the ideal $I = (2, X) \triangleleft \mathbb{Z}[X]$. We can write

$$I = \{2f_1(X) + Xf_2(X) : f_1, f_2 \in \mathbb{Z}[X]\} = \{f \in \mathbb{Z}[X] : 2 \mid f(0)\}$$

Suppose $I = (f)$ for some element f. Since $2 \in I$, we must have $2 = fg$ for some polynomial g. By comparing degrees, the degrees of f and g must be zero, since $\mathbb{Z}$ is an integral domain. Hence f is an integer, so $f = \pm 1$ or $f = \pm 2$. If $f = \pm 1$ then $I = \mathbb{Z}[X]$, and if $f = \pm 2$ then $I = 2\mathbb{Z}[X]$. These both lead to contradictions, since $1 \in I$ and $X \notin I$ respectively.

§10.3 Unique factorisation domains

Definition 10.7 (Unique Factorisation Domain)

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

1. Every nonzero, non-unit element is a product of irreducibles;
2. If $p_1 \cdots p_m = q_1 \cdots q_n$ where p_i, q_i are irreducible, then $m = n$, and p_i, q_i are associates, up to reordering.

GOAL: Show PID $\implies$ UFD.

Remark 27. Any field is a UFD as there are no non-unit elements.

Proposition 10.3

Let R be an integral domain satisfying property (1) above (every nonzero, non-unit element is a product of irreducibles). Then R is a unique factorisation domain iff every irreducible is prime.

Proof. ($\implies$): Let $p \in R$ be irreducible, and $p \mid ab$. Then $ab = pc$ for some $c \in R$. Writing a, b, c as products of irreducibles, it follows from uniqueness of factorisation (2) that $p \mid a$ or $p \mid b$. Hence p is prime.

($\impliedby$): Suppose $p_1 \cdots p_m = q_1 \cdots q_n$ where p_i, q_i are irreducible and hence prime. Since $p_1 \mid q_1 \cdots q_n$, we have $p_1 \mid q_i$ for some i. After reordering, we may assume that $p_1 \mid q_1$, so $p_1 u = q_1$ for $u \in R$. Since q_1 is irreducible, u is a unit since p_1 cannot be a unit. Hence p_1, q_1 are associates. Cancelling p_1 from both sides, we find $p_2 \cdots p_m = u q_2 \cdots q_n$. We may absorb this unit into q_2 without loss of generality. Inductively, all p_i and q_i are associates, for each i. Hence R is a unique factorisation domain. $\square$

Definition 10.8 (Noetherian)

Let R be a ring. Suppose, for all nested sequences of ideals in R written $I_1 \subseteq I_2 \subseteq \cdots$, $\exists\, N$ such that $I_n = I_{n+1}$ for all $n \geq N$. Then, we say that R is a **Noetherian** ring.

This condition is known as the 'ascending chain condition'. In other words, we cannot infinitely nest distinct ideals in a Noetherian ring.

Lemma 10.4

Principal ideal domains are Noetherian rings.

Proof. Let $I = \bigcup_{i=1}^{\infty} I_i$. Then, I is an ideal in R (Sheet 2). Since R is a principal ideal domain, $I = (a)$ for some $a \in R$. Then $a \in \bigcup_{i=1}^{\infty} I_i$, so in particular $a \in I_N$ for some N. But then for all $n \geq N$, $(a) \subseteq I_N \subseteq I_n \subseteq I_{n+1} \subseteq I = (a)$. So all inclusions are equalities, so in particular $I_n = I_{n+1}$. $\square$

Theorem 10.1

If R is a principal ideal domain, then it is a unique factorisation domain.

Proof. First, we verify property (1) of UFD, that every nonzero, non-unit element is a product of irreducibles. Let $x \neq 0$ be an element of R which is not a unit. Suppose x does not factor as a product of irreducibles. This implies that x is not irreducible. By definition of irreducibility, we can write x as the product of two elements x_1, y_1 where x_1, y_1 are not units. Then either x_1 or y_1 is not a product of irreducibles, so wlog we can suppose x_1 is not a product of irreducibles. We have $(x) \subseteq (x_1)$. This inclusion is strict, since y_1 is not a unit. Now, we can write $x_1 = x_2 y_2$ where x_2, y_2 are not units, and inductively we can create $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$. But R is Noetherian, so this is a contradiction to Lemma 10.4. So every nonzero, non-unit element is indeed a product of irreducibles.

By Proposition 10.3, it suffices to show that every irreducible is prime. This has already been shown previously by Proposition 10.1. Hence R is a unique factorisation domain. $\square$

Example 10.9

We have shown that ED $\implies$ PID $\implies$ UFD $\implies$ Integral Domain. We now provide examples for counterexamples to the converses.

The ring $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain since 2 is a zero divisor, hence it is not a ED, PID or UFD either.

The ring $\mathbb{Z}[\sqrt{-5}] \leq \mathbb{C}$ is integral, but not a unique factorisation domain and hence not ED or PID.

The ring $\mathbb{Z}[X]$ has been shown to be not a principal ideal domain. We can show using later results that this is a unique factorisation domain.

We can construct the ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, which can be shown to be not a Euclidean domain, but is a principal ideal domain. This will be proved in Part II Number Fields.

Finally, $\mathbb{Z}[i]$ is a Euclidean domain, and is hence a principal ideal domain, a unique factorisation domain, and an integral domain.

Definition 10.9 (Common Divisors and Multiples)

Let R be an integral domain.

1. $d \in R$ is a **common divisor** of $a_1, \ldots, a_n \in R$ if $d \mid a_i$ for all i;
2. $d \in R$ is a **greatest common divisor** of $a_1, \ldots, a_n$ if for all common divisors d', we have $d' \mid d$;
3. $m \in R$ is a **common multiple** of $a_1, \ldots, a_n$ if $a_i \mid m$ for all i;
4. $m \in R$ is a **least common multiple** of $a_1, \ldots, a_n$ if for all common multiples m', we have $m \mid m'$.

Warning 10.1

These do not need to exist in a given ring.

Remark 28. Greatest common divisors and lowest common multiples are unique up to associates, if they exist.

Proposition 10.4

In unique factorisation domains, greatest common divisors and least common multiples always exist.

Proof. Let $a_i = u_i \prod_j p_j^{n_{ij}}$ where the p_j are irreducible and pairwise non-associate, u_i is a unit, and $n_{ij} \in \mathbb{Z}_{\geq 0}$. We claim that $d = \prod_j p_j^{m_j}$, where $m_j = \min_{1 \leq i \leq n} n_{ij}$, is the greatest common divisor. Certainly d is a common divisor. If d' is a common divisor, then d' can be written as a product of irreducibles, which will be denoted $d' = w \prod_j p_i^{t_j}$ for a unit w. We can see that $t_j \leq n_{ij}$ for all i, so in particular, $t_j \leq m_j$. This implies $d' \mid d$. Hence d is a greatest common divisor. The argument for the least common multiple is similar, replacing minima with maxima. □

§11 Factorisation in polynomial rings

Theorem 11.1

Let R be a unique factorisation domain. Then $R[X]$ is also a unique factorisation domain.

The proof for this theorem will require a number of key lemmas. In this subsection, R will denote a unique factorisation domain, with field of fractions F. We have $R[X] \leq F[X]$. Since polynomial rings over fields are Euclidean domains, $F[X]$ is a principal ideal domain, and hence a unique factorisation domain. This does not immediately imply that $R[X]$ is a unique factorisation domain, however.

Definition 11.1 (Content)

The **content** of a polynomial $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ is $c(f) = \gcd\{a_0, \dots, a_n\}$. This is well-defined up to multiplication by a unit.

Definition 11.2 (Primitive)

We say that f is **primitive** if $c(f)$ is a unit.

Lemma 11.1

The product of primitive polynomials is primitive. Further, for $f, g \in R[X]$, $c(fg)$ and $c(f)c(g)$ are associates.

Proof. Let $f = \sum_{i=0}^n a_i X^i$ and $g = \sum_{i=0}^m b_i X^i$. Suppose fg is not primitive, so $c(fg)$ is not a unit. This implies that there exists a prime p such that $p \mid c(fg)$. Since f, g are primitive, $p \nmid c(f)$ and $p \nmid c(g)$.

p does not divide all of the a_k or the b_ℓ. Let k, ℓ be the smallest values such that $p \nmid a_k$ and $p \nmid b_\ell$. Then, the coefficient of $X^{k+\ell}$ in fg is given by

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

Thus $p \mid a_k b_\ell$ as $p \mid c(fg)$. This implies $p \mid a_k$ or $p \mid b_\ell$ as p prime $\lightning$.

To prove the second part, let $f = c(f) f_0$ for some $f_0 \in R[X]$. Here, f_0 is primitive. Similarly, $g = c(g) g_0$ for a primitive g_0. Thus $fg = c(f)c(g) f_0 g_0$. The expression $f_0 g_0$ is a primitive polynomial by the first part, so $c(fg)$ is equal to $c(f)c(g)$ up to associates. $\square$

Corollary 11.1

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

Proof. Since R is an integral domain, we have $R[X]^\times = R^\times$ [a], so p is not a unit. Let $f \in R[X]$. Then $p \mid f$ in $R[X] \iff p \mid c(f)$ in R. Thus, if $p \mid gh$ in $R[X]$, we have $p \mid c(gh) =$ [b] $c(g)c(h)$. In particular, since p is prime in R, we have $p \mid c(g)$ or $p \mid c(h)$, so $p \mid g$ or $p \mid h$. So p is prime in $R[X]$. $\square$

[a] Suppose $a, b \in R[X]$ s.t. $ab = 1$ then as degrees of polynomials add under multiplication $\deg a = \deg b = 0$ so $a, b \in R$.

[b] When we use equality with contents, we implicitly mean they are associates.

Lemma 11.2

Let $f, g \in R[X]$, where g is primitive. Then if $g \mid f$ in $F[X]$, then $g \mid f$ in $R[X]$.

Proof. Let $f = gh$, where $h \in F[X]$. We can find a nonzero $a \in R$, such that $ah \in R[X]$. In particular, we can multiply the denominators of the coefficients of h to form a. Now, $ah = c(ah) h_0$ where h_0 is primitive. Then $af = c(ah) h_0 g$. Since h_0 and g are primitive, so is $h_0 g$. Thus, taking contents, $a \mid c(ah)$. This implies $h \in R[X]$. Hence $g \mid f$ in $R[X]$. $\square$

Lemma 11.3 (Gauss' lemma)

Let $f \in R[X]$ be primitive. Then if f is irreducible in $R[X]$, we have that f is irreducible in $F[X]$.

Proof. Since $f \in R[X]$ is irreducible and primitive, its degree must be larger than zero[a]. Hence f is not a unit in $F[X]$.

Suppose f is not irreducible in $F[X]$, so $f = gh$ for $g, h \in F[X]$ with degrees larger than zero. Let $\lambda \in F^\times$ such that $\lambda^{-1} g \in R[X]$ is primitive. (For example, let $b \in R$ such that $bg \in R[X]$ clears out denominators, then $bg = c(bg)g_0$, giving $\lambda = c(bg)b^{-1}$.) Replacing g by $\lambda^{-1}g$ and h by λh, we still have a factorisation of f. Hence, we may assume without loss of generality that $g \in R[X]$ and is primitive. By Lemma 11.2, we have that $h \in R[X]$, and we already saw that $\deg h > 0$. This contradicts irreducibility $\lightning$. $\square$

[a]If $\deg f = 0$ and f primitive, f is a unit but this contradicts it being irreducible.

Remark 29. We will see that the reverse implication in Gauss' lemma also holds.

Lemma 11.4

Let $g \in R[X]$ be primitive. If g is prime in $F[X]$, then g is prime in $R[X]$.

Proof. It suffices to show that if $f_1, f_2 \in R[X]$, then $g \mid f_1 f_2$ implies $g \mid f_1$ or $g \mid f_2$. Since g is prime in $F[X]$, $g \mid f_1$ or $g \mid f_2$ in $F[X]$. By Lemma 11.2, $g \mid f_1$ or $g \mid f_2$ in $R[X]$ as required. $\square$

We can now prove Theorem 11.1, that polynomial rings over unique factorisation domains are unique factorisation domains.

Proof. Let $f \in R[X]$. Then, $f = c(f)f_0$ for f_0 primitive in $R[X]$. Since R is a unique factorisation domain, $c(f)$ is a product of irreducibles in R. If an element of R is irreducible, it is irreducible as an element of $R[X]$. Hence, it suffices to find a factorisation of f_0.

Suppose f_0 is not irreducible, so $f_0 = gh$ for $g, h \in R[X]$. Since f_0 is primitive, g and h are primitive and $\deg g, \deg h > 0$[a]. By induction on the degree, we can factor f_0 as a product of primitive irreducibles in $R[X]$. So property (1) of UFD is shown.

It now suffices to show uniqueness of the factorisation. By Proposition 10.3, it in fact suffices to show that every irreducible element of $R[X]$ is prime. Let f be irreducible. Write $f = c(f)f_0$, where f_0 is primitive. Since f is irreducible, either f_0 a unit so f must be constant or $c(f)$ a unit so f primitive.

Suppose f is constant. Since f is irreducible in $R[X]$, it must be irreducible in R. As R is a unique factorisation domain, f is prime in R. By Corollary 11.1, f is prime in $R[X]$.

Now, suppose f is primitive. Since f is irreducible in $R[X]$, we can use Gauss' lemma to show that f is irreducible in $F[X]$. Thus, f is prime in $F[X]$, as $F[X]$ is a unique factorisation domain. Finally, we can see that f is prime in $R[X]$ by Lemma 11.4. $\square$

[a] If $\deg g = 0$, as g primitive it must be a unit but we assume it is not.

Remark 30. By Lemma 10.2, we know that the prime elements in an integral domain are irreducible. This implies that the implications in the last paragraph above are in fact equivalences. In particular, in Gauss' lemma, the implication is an equivalence.

Example 11.1

Theorem 11.1 implies that $\mathbb{Z}[X]$ is a unique factorisation domain.

Example 11.2

Let $R[X_1, \ldots, X_n]$ be the ring of polynomials in n variables. Define inductively $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$. Applying Theorem 11.1 inductively $\implies$ $R[X_1, \ldots, X_n]$ is a UFD if R is.

§11.1 Eisenstein's criterion

Proposition 11.1 (Eisenstein's Criterion)

Let R be a unique factorisation domain, and $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ be a primitive polynomial. Let $p \in R$ be irreducible (or, equivalently, prime) such that

1. $p \nmid a_n$;
2. $p \mid a_i$ for all $i < n$; and
3. $p^2 \nmid a_0$.

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

Proof. Suppose $f = gh$ for $g, h \in R[X]$ not units. Since f is primitive, g, h must have positive degree. Let $g(X) = \sum_{i=0}^{k} r_i X^i$ and $h(X) = \sum_{i=0}^{\ell} s_i X^i$, so $k + \ell = n$. Then $p \nmid a_n = r_k s_\ell$, so $p \nmid r_k$ and $p \nmid s_\ell$. Further, $p \mid a_0 = r_0 s_0$ so $p \mid r_0$ or $p \mid s_0$. Wlog, we may assume $p \mid r_0$. There exists a minimal $j \leq k$ such that $p \mid r_i \; \forall \, i < j$ but $p \nmid r_j$.

$$a_j = \underbrace{r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1}_{p \mid r_i \, \forall \, i<j} + r_j s_0$$

By assumption, a_j is divisible by p since $j < n$. Further, the first j terms in the expansion are divisible by p. Thus, $p \mid r_j s_0$. By assumption, $p \nmid r_j$, so $p \mid s_0$, so $p^2 \mid r_0 s_0 = a_0$, contradicting the third criterion $\lightning$. $\square$

Example 11.3

Let $f(X) = X^3 + 2X + 5 \in \mathbb{Z}[X]$. We will show this is irreducible as a polynomial over $\mathbb{Q}$. If f is reducible in $\mathbb{Z}[X]$, then it factorises as $f(X) = (X + a)(X^2 + bX + c)$ up to multiplication by units. Here, $ac = 5$. But $\pm 1, \pm 5$ are not roots of f $\lightning$, so this is irreducible in $\mathbb{Z}[X]$. By Gauss' lemma, f is irreducible in $\mathbb{Q}[X]$, since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. In particular, $\mathbb{Q}[X]/(f)$ is a field by Lemma 10.3, since the ideal (f) is maximal.

Example 11.4

Let $p \in \mathbb{Z}$ be a prime, and let $f(X) = X^n - p$. By Eisenstein's criterion, f is irreducible in $\mathbb{Z}[X]$. It is then irreducible in $\mathbb{Q}[X]$ by Gauss' lemma.

Example 11.5

Consider $f(X) = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Z}[X]$, where p is prime. Eisenstein's criterion does not apply directly. Consider

$$f(X) = \frac{X^p - 1}{X - 1}; \quad Y = X - 1$$

By using this substitution of Y,

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

We can apply Eisenstein's criterion to this new polynomial, since $p \mid \binom{p}{i}$ for all $1 \leq i \leq p - 1$, and $p^2 \nmid \binom{p}{p-1} = p$. Thus, $f(Y+1)$ is irreducible in $\mathbb{Z}[Y]$, so $f(X)$ is irreducible in $\mathbb{Z}[X]$. Of course, $f(X)$ is therefore irreducible in $\mathbb{Q}[X]$ as before.

§12 Algebraic integers

§12.1 Gaussian integers

Recall the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$. There is a norm function $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ given by $a + bi \mapsto a^2 + b^2$, and $N(xy) = N(x)N(y)$. This norm is a Euclidean function, giving the Gaussian integers the structure of a Euclidean domain and hence a PID and UFD. So the primes are the irreducibles in $\mathbb{Z}[i]$. The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$, since they are the only elements of unit norm.

Example 12.1

2 is not irreducible in $\mathbb{Z}[i]$, since it factors as $(1+i)(1-i)$. 5 is not irreducible, since it factors as $(2+i)(2-i)$. These are nontrivial factorisations since the norms of the factors are not unit length.

3 is a prime, since it is irreducible. Indeed, $N(3) = 9$, so if 3 were reducible it would factor as ab where $N(a) = N(b) = 3$. But $\mathbb{Z}[i]$ has no elements of norm 3. Similarly, 7 is a prime.

Proposition 12.1

Let $p \in \mathbb{Z}$ be a prime. Then, the following are equivalent.

1. p is not prime in $\mathbb{Z}[i]$;
2. $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$;
3. $p = 2$ or $p \equiv 1 \mod 4$.

Proof. (1) $\implies$ (2): Let $p = xy$ for $x, y \in \mathbb{Z}[i]$ not units. Then, $p^2 = N(p) = N(x)N(y)$. Since x, y are not units, $N(x), N(y) > 1$ and in particular $N(x) = N(y) = p$. Writing $x = a + bi$ for $a, b \in \mathbb{Z}$, we have $p = N(x) = a^2 + b^2$, which is the condition in (2).

(2) $\implies$ (3): The only squares modulo 4 are 0 and 1. Since $p \equiv a^2 + b^2 \mod 4$, we have that p cannot be congruent to 3, modulo 4.

(3) $\implies$ (1): We have already observed above that 2 is not prime in $\mathbb{Z}[i]$. It hence suffices to consider the case where $p \equiv 1 \mod 4$. We have that $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ is cyclic of order $p - 1$ by Theorem 9.1. Hence, if $p \equiv 1 \mod 4$, we have that $4 \mid p - 1$, and hence $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ contains an element of order 4, i.e. $\exists\, x \in \mathbb{Z}$ with $x^4 \equiv 1 \mod p$, but $x^2 \not\equiv 1 \mod p$[a]. Then $x^2 \equiv -1 \mod p$, or in other words, $p \mid (x^2 + 1)$. But this factorises as $p \mid (x + i)(x - i)$. We can see that $p \nmid x + i$, $p \nmid x - i$, so p cannot

be prime. $\square$

[a]Otherwise x would be order 2

Remark 31. The proof that (iii) implies (i) is entirely nontrivial. It required lots of theory in order to reach the result, even though its statement did not require even the notion of a complex number.

Theorem 12.1

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

1. $a + bi$, where $a, b \in \mathbb{Z}$ and $a^2 + b^2 = p$[a] is a prime in $\mathbb{Z}$ with $p = 2$ or $p \equiv 1 \mod 4$; and
2. the primes p in $\mathbb{Z}$ satisfying $p \equiv 3 \mod 4$.

[a]Previous theorem implies p not prime in $\mathbb{Z}[i]$, but $a + bi \neq p$ and we care about $a + bi$.

Proof. First, we must check that all such elements are prime. For (1), note that $N(a + bi) = p$ is prime, so if $a + bi = uv$ then either $N(u)$ or $N(v) = 1$. Thus $a + bi$ is irreducible, hence prime.
(2) follows from Proposition 12.1.

It now suffices to show that any prime in the Gaussian integers satisfies one of the two above conditions. Let z be prime in $\mathbb{Z}[i]$. We note that $\overline{z}$ is also irreducible. Now, $N(z) = z\overline{z}$, which is a factorisation of the norm into irreducibles.
$N(z)$ a non-unit integer so let p be a prime in $\mathbb{Z}$ dividing $N(z)$.
If $p \equiv 3 \mod 4$, p is prime in $\mathbb{Z}[i]$. As $p \mid N(z) = z\overline{z}$, $p \mid z$ or $p \mid \overline{z}$ so p is associate to z or $\overline{z}$[a]. If p associate to $\overline{z}$ it is also associate to z by taking conjugates.
Otherwise, $p = 2$ or $p \equiv 1 \mod 4$ and $p = a^2 + b^2 = (a + bi)(a - bi)$ where $a \pm bi$ are irreducible in $\mathbb{Z}[i]$ as they have norm p. So we have $p = (a + bi)(a - bi) \mid z\overline{z}$, so z is an associate of $a + bi$ or $a - bi$ by uniqueness of factorisation. $\square$

[a]If two primes divide each other they must be associates.

Remark 32. In Theorem 12.1, if $p = a^2 + b^2$, $a + bi$ and $a - bi$ are not associate unless $p = 2$. [$(1 + i), (1 - i)$ are associates as $(1 + i) = (1 - i)i$ if $p = 2$ so $a + bi, a - bi$ are.]

Corollary 12.1

An integer $n \geq 1$ is the sum of two squares iff every prime factor p of n with $p \equiv 3 \mod 4$ divides n to an even power.

Proof. Suppose $n = a^2 + b^2$. So $n = N(a \pm bi)$. Factorising $a \pm bi$ into a product of primes then n is a product of norms of primes in the Gaussian integers. By

Theorem 12.1, those norms are

1. the primes $p \in \mathbb{Z}$ with $p \not\equiv 3 \mod 4$; and
2. squares of primes $p \in \mathbb{Z}$ with $p \equiv 3 \mod 4$.

The result follows. $\square$

Example 12.2

We can write $65 = 5 \cdot 13$ as the sum of two primes since $5, 13 \equiv 1 \mod 4$. We first factorise 5 and 13 into primes in the Gaussian integers.

$$5 = (2+i)(2-i); \quad 13 = (2+3i)(2-3i)$$

Thus, the factorisation of 65 into irreducibles in $\mathbb{Z}[i]$ is

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

This was dependent on the choice of grouping of terms. Alternatively,

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

§12.2 Algebraic integers

Definition 12.1 (Algebraic)

A number $\alpha \in \mathbb{C}$ is **algebraic** if α is a root of some nonzero polynomial $f \in \mathbb{Q}[X]$.

Definition 12.2 (Algebraic Integer)

$\alpha \in \mathbb{C}$ is an **algebraic integer** if it is a root of some monic polynomial $f \in \mathbb{Z}[X]$.

Notation. Let $R \leq S$, and $\alpha \in S$. We write $R[\alpha]$ to denote the smallest subring of S containing R and α. $R[\alpha]$ is the intersection of all subrings of S containing R and α. Further, $R[\alpha] = \operatorname{Im}\varphi$ where $\varphi : R[X] \to S$ is the homomorphism $g(X) \mapsto g(\alpha)$[1].

[1] We map polynomial g to $g(\alpha)$. The image is the smallest subring containing R and α as: $g(X) = c \in R[X]$ for $c \in R$ and $g(\alpha) = c$ so $R \subset \operatorname{Im}\varphi$; also $g(X) = X \in R[X]$ so $g(\alpha) = \alpha$ hence $\alpha \in \operatorname{Im}\varphi$. As we can add terms and multiply α by itself and any element in R, we can obtain any polynomial of α so $g(\alpha) \in R[\alpha]\ \forall\, g \in R[X]$.

Definition 12.3 (Minimal Polynomial)

Let α be an algebraic number. Consider the homomorphism $\varphi : \mathbb{Q}[X] \to \mathbb{C}$ where $g(X) \mapsto g(\alpha)$, $\mathbb{Q}[\alpha] = \operatorname{Im}\varphi$. Since $\mathbb{Q}[X]$ is a a principal ideal domain, $\ker\varphi = (f)$ for some $f \in \mathbb{Q}[X]$. This ideal contains a nonzero element since α is an algebraic number, hence f is nonzero. Multiplying f by a unit, we may assume f is monic without loss of generality.

This unique f is known as the **minimal polynomial** of α.

Corollary 12.2

All minimal polynomials are irreducible.

Proof. By the isomorphism theorem, $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha] \leq \mathbb{C}$. Any subring of a field is an integral domain. Hence (f) is a prime ideal in $\mathbb{Q}[X]$, and hence f is irreducible. In particular, this implies that $\mathbb{Q}[\alpha]$ is a field. □

Proposition 12.2

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

Remark 33. If α is an algebraic integer, then the polynomial in the definition can be taken to be minimal without loss of generality. $\mathbb{Z}[X]$ is not a principal ideal domain, so the previous argument cannot work verbatim.

Proof. Let f be the minimal polynomial of α. Let $\lambda \in \mathbb{Q}^\times$ such that λf has coefficients in $\mathbb{Z}$ and is primitive. Then $\lambda f(\alpha) = 0$, so $\lambda f \in \ker\theta$.

Let $g \in \ker\theta \triangleleft \mathbb{Z}[X]$, so in particular $g \in \mathbb{Z}[X]$. Then $g \in \ker\varphi$, and hence $\lambda f \mid g$ in $\mathbb{Q}[X]$. By Lemma 11.2, $\lambda f \mid g$ in $\mathbb{Z}[X]$. Thus, $\ker\theta = (\lambda f)$.

Now, since α is an algebraic integer, we know that there exists a monic polynomial $g \in \ker\theta$ such that $g(\alpha) = 0$. Then $\lambda f \mid g$ in $\mathbb{Z}[X]$, so $\lambda = \pm 1$ as both f, g are monic. Hence, $f \in \mathbb{Z}[X]$, and $(\lambda f) = (f) = \ker\theta$. □

Let $\alpha \in \mathbb{C}$ be an algebraic integer. Then, applying the isomorphism theorem to θ, $\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha]$.

Example 12.3

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

$$\begin{aligned}
\mathbb{Z}[X] \big/ (X^2+1) &\cong \mathbb{Z}[i] \\
\mathbb{Z}[X] \big/ (X^2-2) &\cong \mathbb{Z}\left[\sqrt{2}\right] \\
\mathbb{Z}[X] \big/ (X^2+X+1) &\cong \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] \\
\mathbb{Z}[X] \big/ (X^n-p) &\cong \mathbb{Z}[\sqrt[n]{p}]
\end{aligned}$$

Corollary 12.3

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

Proof. Let $\alpha \neq 0$, since the case where $\alpha = 0$ is trivial. Then the minimal polynomial of α has coefficients in $\mathbb{Z}$. Since α is rational, the minimal polynomial is $X-\alpha$. Hence $\alpha \in \mathbb{Z}$ as it is a coefficient of the minimal polynomial. □

§13 Noetherian rings

§13.1 Definition

Recall the definition of a Noetherian ring.

Definition 13.1 (Noetherian Ring)

A ring R is **Noetherian** if, for all sequences of nested ideals $I_1 \subseteq I_2 \subseteq \cdots$, there exists $N \in \mathbb{N}$ s.t. for all $n > N$, $I_n = I_{n+1}$.

Lemma 13.1

Let R be a ring. Then R satisfies the ascending chain condition (so R is Noetherian) iff all ideals in R are finitely generated.

We have already shown that principal ideal domains are Noetherian, since they satisfy this 'ascending chain' condition. This now will immediately follow from the lemma.

Proof. ($\Longleftarrow$): Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals. Consider $I = \bigcup_{i=1}^{\infty} I_i$, which is an ideal. By assumption, I is finitely generated, so $I = (a_1, \dots, a_n)$. These elements belong to a nested union of ideals. In particular, we can choose $N \in \mathbb{N}$ such that all a_i are contained within I_N. Then, for $n \geq N$, we find

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

So the inclusions are all equalities, so $I_N = I_n \;\forall\, n \geq N$.

($\implies$): Suppose that there exists an ideal $J \triangleleft R$ which is not finitely generated. Let $a_1 \in J$. Then since J is not finitely generated, $(a_1) \subset J$. We can therefore choose $a_2 \in J \setminus (a_1)$, and then $(a_1) \subset (a_1, a_2) \subset J$. Continuing inductively, we contradict the ascending chain condition. $\square$

§13.2 Hilbert's basis theorem

Theorem 13.1 (Hilbert's Basis Theorem)

Let R be a Noetherian ring. Then $R[X]$ is Noetherian.

Proof. Suppose there exists an ideal $J \triangleleft R[X]$ that is not finitely generated. Let $f_1 \in J$ be an element of minimal degree. Then $(f_1) \subsetneq J$. So we can choose $f_2 \in J \setminus (f_1)$, which is also of minimal degree, then $(f_1, f_2) \subsetneq J$. Inductively we can construct a sequence $f_1, f_2, \dots$, where the degrees are non-decreasing. Let

a_i be the leading coefficient of f_i, for all i. We then obtain a sequence of ideals $(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$ in R. Since R is Noetherian, there exists $m \in \mathbb{N}$ such that for all $n \geq m$, we have $a_n \in (a_1, \ldots, a_m)$. Let $a_{m+1} = \sum_{i=1}^{m} \lambda_i a_i$, since a_{m+1} lies in the ideal $(a_1, \ldots, a_m)$. Now we define

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

The degree of g is equal to the degree of f_{m+1}, and they have the same leading coefficient a_{m+1}. Then, consider $f_{m+1} - g \in J$ and $\deg(f_{m+1} - g) < \deg f_{m+1}$. By minimality of the degree of f_{m+1}, $f_{m+1} - g \in (f_1, \ldots, f_m)$, hence $f_{m+1} \in (f_1, \ldots, f_m)$. This contradicts the choice of f_{m+1}, so J is in fact finitely generated. $\square$

Corollary 13.1

$\mathbb{Z}[X_1, \ldots, X_n]$ is Noetherian. Similarly, $F[X_1, \ldots, X_n]$ is Noetherian for any field F, since fields satisfy the ascending chain condition.

Example 13.1

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

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

where $\mathscr{F} \subseteq R$ is a (possibly infinite) set of polynomials. Such a set is referred to as an **algebraic variety**. Let

$$I = \left\{ \sum_{i=1}^{m} \lambda_i f_i : m \in \mathbb{N}, \lambda_i \in R_i, f_i \in \mathscr{F} \right\}$$

We can check that $I \lhd R$. Since R is Noetherian, $I = (g_1, \ldots, g_r)$. Hence

$$V = \{(a_1, \ldots, a_n) \in \mathbb{C}^n : g(a_1, \ldots, a_n) = 0, \forall g \in I\}$$

Lemma 13.2

Let R be a Noetherian ring, and $I \lhd R$. Then ${}^{R}\!/_{I}$ is Noetherian.

Proof. Let $J_1' \subseteq J_2' \subseteq \cdots$ be a chain of ideals in ${}^{R}\!/_{I}$. By the ideal correspondence, J_i' corresponds to an ideal J_i that contains I, so $J_i' = {}^{J_i}\!/_{I}$. So $J_1 \subseteq J_2 \subseteq \cdots$ is a chain of ideals in R. Since R is Noetherian, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, we have $J_N = J_n$, and so $J_N' = J_n'$. Hence ${}^{R}\!/_{I}$ satisfies the ascending chain condition. $\square$

Example 13.2

The ring of Gaussian integers $\mathbb{Z}/(X^2+1)$ is Noetherian.

Example 13.3

If $R[X]$ is Noetherian, then $R[X]/(X) \cong R$ is Noetherian. This is a converse to the Hilbert basis theorem.

Example 13.4

The ring of polynomials in countably many variables is not Noetherian.

$$\mathbb{Z}[X_1, X_2, \dots] = \bigcup_{n\in\mathbb{N}} \mathbb{Z}[X_1, \dots, X_n]$$

In particular, consider the ascending chain $(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots$.

Example 13.5

Let $R = \{f \in \mathbb{Q}[X] : f(0) \in \mathbb{Z}\} \leq \mathbb{Q}[X]$. Even though $\mathbb{Q}[X]$ is Noetherian, R is not. Indeed, consider $(X) \subset \left(\frac{1}{2}X\right) \subset \left(\frac{1}{4}X\right) \subset \left(\frac{1}{8}X\right) \subset \cdots$. These inclusions are strict, since $2 \in R$ is not a unit.

Part III
Modules

§14 Modules

§14.1 Definitions

Definition 14.1 (Module)
Let R be a ring. A **module over R** is a triple $(M, +, \cdot)$ consisting of a set M and two operations $+ : M \times M \to M$ and $\bullet : R \times M \to M$, that satisfy

1. $(M, +)$ is an abelian group with identity $0 = 0_M$;
2. $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$;
3. $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$;
4. $r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \cdot m$;
5. $1_R \cdot m = m$;

Remark 34. Closure is implicitly required by the types of the $+$ and $\cdot$ operations.

Example 14.1
A module over a field is precisely a vector space.

Example 14.2
A $\mathbb{Z}$-module is precisely the same as an abelian group, since

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

Example 14.3
Let F be a field, and V be a vector space over F. Let $\alpha : V \to V$ be an endomorphism.

We can turn V into an $F[X]$-module by

$$\bullet : F[X] \times V \to V; \quad f \cdot v = (f(\alpha))(v)$$

E.g. $(X^2+1) \cdot v = (\alpha^2 + 1_V)(v)$.

Note that the structure of the $F[X]$-module depends on the choice of α. We can write $V = V_\alpha$ to disambiguate.

Example 14.4

For any ring R, we can consider R^n as an R-module via

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

In particular, the case $n = 1$ shows that any ring R can be considered an R-module where the scalar multiplication in the ring and the module agree.

Example 14.5

For an ideal $I \triangleleft R$, we can regard I as an R-module, since I is preserved under multiplication by elements in R. The quotient ring ${}^{R}\!/_{I}$ is also an R-module, defining multiplication as $r \cdot (s + I) = rs + I$.

Example 14.6

Let $\varphi : R \to S$ be a ring homomorphism. Then any S-module can be regarded as an R-module. We define $r \cdot m = \varphi(r) \cdot m$. In particular, this applies when R is a subring of S, and φ is the inclusion map. So any module over a ring can be viewed as a module over any subring.

Definition 14.2 (Submodule)

Let M be an R-module. Then $N \subseteq M$ is an **R-submodule of M**, written $N \leq M$, if $(N, +) \leq (M, +)$, and $rn \in N$ for all $r \in R$ and $n \in N$.

Example 14.7

By considering R as an R-module, a subset of R is an R-submodule iff it is an ideal.

Example 14.8

If $R = F$ is a field, then a module is equivalent to a vector space and a submodule a vector subspace.

Definition 14.3 (Quotient)

Let $N \leq M$ be R-modules. Then, the **quotient** ${}^{M}\!/_{N}$ is defined as the quotient of groups under addition, and with scalar multiplication defined as $r \cdot (m+N) = rm+N$. This is well-defined, since N is preserved under scalar multiplication. This makes ${}^{M}\!/_{N}$ an R-module.

Remark 35. Submodules are analogous both to subrings and to ideals.

Definition 14.4 (Homomorphism)

Let M, N be R-modules. Then $f : M \to N$ is a **R-module homomorphism** if it is a homomorphism of $(M, +)$ and $(N, +)$, and scalar multiplication is preserved: $f(r \cdot m) = r \cdot f(m) \ \forall\, r \in R, m \in M$.

Definition 14.5 (Isomorphism)

An **R-module isomorphism** is an R-module homomorphism that is a bijection.

Example 14.9

If $R = F$ is a field, F-module homomorphisms are exactly linear maps.

Theorem 14.1 (First Isomorphism Theorem)

Let $f : M \to N$ be an R-module homomorphism. Then

1. $\ker f = \{m \in M : f(m) = 0\} \leq M$;
2. $\operatorname{Im} f = \{f(m) \in N : m \in M\} \leq N$;
3. ${}^{M}\!/_{\ker f} \cong \operatorname{Im} f$.

Proof. Similar to before, left as an exercise. $\square$

Theorem 14.2 (Second Isomorphism Theorem)

Let $A, B \leq M$ be R-submodules. Then

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

2. $A \cap B \leq M$;
3. $^{A}/_{A \cap B} \cong {}^{(A+B)}/_{B}$.

Proof. Apply first iso thm to the composite map $A \to M \to {}^{M}/_{B}$ by $a \mapsto a \mapsto a+B$. Left as an exercise. $\square$

For $N \leq M$, there is a bijection between submodules of $^{M}/_{N}$ and submodules of M containing N.

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

$$^{M/N}/_{L/N} \cong {}^{M}/_{L}$$

Note that these results apply to vector spaces; for example, the first isomorphism theorem immediately gives the rank-nullity theorem.

§14.2 Finitely generated modules

Definition 14.6 (Generated Submodule)
Let M be an R-module. If $m \in M$, then we write $Rm = \{rm : r \in R\}$. This is an R-submodule of M, known as the submodule **generated by** m.

Definition 14.7 (Sum of Submodules)
If $A, B \leq M$, we can define $A + B = \{a + b : a \in A, b \in B\}$, known as the **sum of submodules**. In particular, this sum is commutative.

Definition 14.8 (Cyclic)
M is **cyclic** if $M = Rm$ for some $m \in M$.

Definition 14.9 (Finitely Generated)
A module M is **finitely generated** if it is the sum of finitely many cyclic submodules. In other words, $M = Rm_1 + \cdots + Rm_n$.

This is the analogue of finite dimensionality in linear algebra.

Lemma 14.1

M is cyclic $\iff$ $M \cong {}^{R}\!/_{I}$ for some $I \lhd R$.

Proof. ($\implies$): Suppose $M = Rm$, then there is a surjective R-module homomorphism

$$\begin{aligned} R &\to M \\ r &\mapsto rm. \end{aligned}$$

Its kernel is an R-submodule of R, i.e. an ideal. First iso thm implies that ${}^{R}\!/_{I} \cong M$.

($\impliedby$): ${}^{R}\!/_{I}$ is generated as an R-module by $1_R + I$. □

Lemma 14.2

An R-module M is finitely generated iff there exists a surjective R-module homomorphism $f : R^n \to M$ for some n.

Proof. ($\implies$): We have $M = Rm_1 + \cdots + Rm_n$. We define $f : R^n \to M$ by $(r_1, \ldots, r_n) \mapsto r_1 m_1 + \cdots + r_n m_n$. This is surjective as $M = Rm_1 + \cdots + Rm_n$ also you can check other properties to find it is a R-module homomorphism.

($\impliedby$): Let $e_i = (0, \ldots, 1, \ldots, 0)$ be the element of R^n with all entries zero except for 1 in the ith place. Given f, let $m_i = f(e_i)$. Then, since f is surjective, any element $m \in M$ is contained in the image of f, so is of the form $f(r_1, \ldots, r_n) = f(\sum_{i=1}^n r_i e_i) = \sum_{i=1}^n r_i f(e_i) = \sum_{i=1}^n r_i m_i$. Thus $M = Rm_1 + \cdots = Rm_n$. □

Corollary 14.1

Let $N \leq M$ be a R-submodule. If M is finitely generated then ${}^{M}\!/_{N}$ is finitely generated.

Proof. There exists a surjective R-module homomorphism $f : R^n \to M$. Then $q \circ f$, where q is the quotient map, is also a surjective homomorphism. So ${}^{M}\!/_{N}$ is finitely generated. □

Example 14.10

It is not always the case that a submodule of a finitely generated module is finitely generated. Let R be a non-Noetherian ring, and I an ideal in R that is not finitely generated (in the ring sense). R is a finitely generated R-module, since $R1 = R$. I

is a submodule of R, which is not finitely generated (in the module sense).

Remark 36. If R is Noetherian, it is always the case that submodules of finitely generated R-modules are finitely generated (Sheet 4).

Lemma 14.3

Let R be an integral domain. Every submodule of a cyclic R-module is cyclic iff R is a PID.

Proof. ($\implies$): R is a cyclic R-module. Saying its submodule are cyclic precisely means that every ideal is principal.

($\impliedby$): If M is a cyclic R-module its isomorphic to R/I, $I \lhd R$ by Lemma 14.1. Any submodule of R/I is of the form J/I for some ideal $J \lhd R$ and $I \subseteq J$. R a PID implies J is principal so J/I is cyclic. $\square$

§14.3 Torsion

Definition 14.10 (Torsion)

Let M be an R-module.

1. $m \in M$ is **torsion** if there exists $0 \neq r \in R$ such that $rm = 0$;
2. M is a **torsion module** if every element is torsion;
3. M is a **torsion-free module** if 0 is the only torsion element.

Example 14.11

The torsion elements in a $\mathbb{Z}$-module (which is an abelian group) are precisely the elements of finite order. If F is a field, any F-module is torsion-free.

§14.4 Direct sums

Definition 14.11 (Direct Sum)

Let $M_1, \ldots, M_n$ be R-modules. Then the **direct sum** of $M_1, \ldots, M_n$, written $M_1 \oplus \cdots \oplus M_n$, is the set $M_1 \times \cdots \times M_n$, with the operations of addition and scalar multiplication defined componentwise. We can show that the direct sum of (finitely many) R-modules is an R-module.

Example 14.12

$R^n = R \oplus \cdots \oplus R$, where we take the direct sum of n copies of R.

Lemma 14.4

Let $M = \bigoplus_{i=1}^n M_i$, and for each M_i, let $N_i \leq M_i$. Then $N = \bigoplus_{i=1}^n N_i$ is a submodule of M. Further,

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

Proof. First, we can see that this N is a submodule. Applying the first isomorphism theorem to the surjective R-module homomorphism $M \to \bigoplus_{i=1}^n M_i/N_i$ given by $(m_1, \dots, m_n) \mapsto (m_1 + N_1, \dots, m_n + N_n)$, the result follows as required, since the kernel is N. □

§14.5 Free modules

Definition 14.12 (Independent)

Let $m_1, \dots, m_n \in M$. The set $\{m_1, \dots, m_n\}$ is **independent** if $\sum_{i=1}^n r_i m_i = 0$ implies that the r_i are all zero.

Definition 14.13 (Generates Freely)

A subset $S \subseteq M$ **generates M freely** if:

1. S generates M, so for all $m \in M$, we can find finitely many entries $s_i \in S$ and coefficients $r_i \in R$ such that $m = \sum_{i=1}^k r_i s_i$;
2. any function $\psi : S \to N$, where N is an R-module, extends to an R-module homomorphism $\theta : M \to N$.

Remark 37. In (ii), such an extension θ is always unique if it exists, by (i).

Definition 14.14 (Free)

An R-module M freely generated by some subset $S \subseteq M$ is called **free**. We say that S is a **free basis** for M.

Remark 38. Free bases in the study of modules are analogous to bases in linear algebra. All vector spaces are free modules, but not all modules are free.

Proposition 14.1

For a finite subset $S = \{m_1, \dots, m_n\} \subseteq M$, the following are equivalent.

1. S generates M freely;
2. S generates M and S is independent;
3. Every element of M can be written uniquely as $r_1 m_1 + \dots + r_n m_n$ for some $r_i \in R$;
4. The R-module homomorphism $R^n \to M$ given by $(r_1, \dots, r_n) \mapsto r_1 m_1 + \dots + r_n m_n$ is bijective, so is an isomorphism.

Proof. Not all implications are shown, but they are similar to arguments found in Part IB Linear Algebra.

(i) $\implies$ (ii) Let S generate M freely. Suppose S is not independent. Then there exist r_i such that $\sum_{i=1}^n r_i m_i = 0$ but not all r_i are zero. Let $r_j \neq 0$. Since S generates M freely, consider the module homomorphism $\psi : S \to R$ given by

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

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

$$0 = \theta(0) = \theta\left(\sum_{i=1}^n r_i m_i\right) = \sum_{i=1}^n r_i \theta(m_i) = r_j \neq 0$$

This is a contradiction, so S is independent.

To show (ii) $\implies$ (iii), it suffices to show uniqueness. If there exist two ways to write an element as a linear combination, consider their difference to find a contradiction from (ii).

We can show (iii) $\implies$ (i). Then it remains to show (iii) $\iff$ (iv). $\square$

Example 14.13

A non-trivial finite abelian group is not a free $\mathbb{Z}$-module.
This is because given non-trivial element x, we know $\exists nx = 0$ for some n, e.g. n is the order of the group. So x cannot be in an independent set.

Example 14.14

The set $\{2, 3\}$ generates $\mathbb{Z}$ as a $\mathbb{Z}$-module. This is not a free basis, since they are not independent: $2 \cdot 3 - 3 \cdot 2 = 0$. Furthermore no subset is a free basis, $\{2\}, \{3\}$ do not generate.

This is different to vector spaces, where we can always construct a basis from a subset of a spanning set.

Proposition 14.2 (Invariance of Dimension)

Let R be a nonzero 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. We define $IM = \{\sum a_i m_i : a_i \in I, m_i \in M\} \leq M$. Since I is an ideal, we can show that IM is a submodule of M. The quotient module M/IM is an R-module, but we can also show that it is an R/I-module, by defining scalar multiplication as

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

We can check that this is well-defined; this follows from the fact that for $b \in I$, $b \cdot (m + IM) = bm + IM$, but $b \in I$ so $bm \in IM$.

Now, suppose that $R^m \cong R^n$. Then let $I \lhd R$ be a maximal ideal in R[a]. By Lemma 14.4, we find an isomorphism of R/I-modules

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

This is an isomorphism of vector spaces over R/I which is a field, since I is maximal. Hence, using the corresponding result from linear algebra, $n = m$. □

[a] We can prove the existence of such an ideal under the assumption of the axiom of choice, and in particular using Zorn's lemma. With Noetherian Rings this is quite easy to prove by just picking an ideal and if its not maximal then there is one containing it and so on till we have a constant ideal and so it must be maximal

§15 The structure theorem and applications

We will assume that R is a Euclidean domain in this section, and let φ be a Euclidean function for R.

§15.1 Row and column operations

We will consider an $m \times n$ matrix with entries in R.

Definition 15.1 (Elementary Row Operations)

The **elementary row operations** on a matrix are

1. (ER1) Add $\lambda \in R$ times the jth row to the ith row, where $i \neq j$;
2. (ER2) Swap the ith row and the jth row;
3. (ER3) Multiply the ith row by $u \in R^{\times}$.

Remark 39. Each of these operations can be realised by left-multiplication by some $m \times m$ matrix. These operations are all invertible, so their matrices are all invertible.

We can define elementary column operations in an analogous way (EC1-3), using right-multiplication by an $n \times n$ matrix instead.

Definition 15.2 (Equivalent)

Two $m \times n$ matrices A, B are **equivalent** if there exists a sequence of elementary row and column operations that transforms one matrix into the other. If they are equivalent, then there exist invertible matrices P, Q such that $B = QAP$.

Definition 15.3 (Minor)

A $k \times k$ **minor** of an $m \times n$ matrix A is the determinant of a $k \times k$ submatrix of A, which is a matrix of A produced by removing $m - k$ rows and $n - k$ columns.

Definition 15.4 (Fitting Ideal)

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

Lemma 15.1

The kth fitting ideal of a matrix is invariant under elementary row and column operations, i.e. for equivalent A, B $\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)\ \forall\, k$.

Proof. It suffices by symmetry to show that the elementary row operations do not change the Fitting ideal.

For the first elementary row operation, ER1, on a matrix A, suppose we add $\lambda \in R$ multiplied by the jth row to the ith row, yielding a matrix A'. In particular, $a_{ik} \mapsto a_{ik} + \lambda a_{jk}$ for all k. Let C be a $k \times k$ submatrix of A and C' the corresponding submatrix of A'.

If row i was not chosen in C, then C and C' are the same matrix. Hence $\det C = \det C'$.

If row i and row j were both chosen in C, we have that C, C' differ by a row operation. Since the determinant is invariant under this elementary row operations thus $\det C = \det C'$.

If row i was chosen but row j was not chosen, by expanding the determinant along the ith row, we find

$$\det C' = \det C \pm \lambda \det D$$ [a]

where we can show that D is a $k \times k$ submatrix of A that includes row j but not row i. By definition, $\det D \in \mathrm{Fit}_k(A)$ and $\det C \in \mathrm{Fit}_k(A)$, so certainly $\det C' \in \mathrm{Fit}_k(A)$. Hence $\mathrm{Fit}_k(A') \subseteq \mathrm{Fit}_k(A)$. By the invertibility of the elementary row operations, $\mathrm{Fit}_k(A') \supseteq \mathrm{Fit}_k(A)$.

The proofs for the other elementary row operations are left as an exercise. □

[a] Expanding the det along the ith row is $(a_{i1} + \lambda a_{j1}) \det E - (a_{i2} + \lambda a_{j2}) \det F + \cdots \pm (a_{in} + \lambda a_{jn}) \det Z = (a_{i1} \det E - a_{i2} \det F + \cdots \pm a_{in} \det Z) + \lambda(a_{j1} \det E - a_{j2} \det F + \cdots \pm a_{jn} \det Z) = \det C \pm \lambda \det D$.

§15.2 Smith normal form

Theorem 15.1 (Smith Normal Form)

An $m \times n$ matrix $A = (a_{ij})$ over a Euclidean domain R is equivalent to a matrix of the form, with $d_i \neq 0$

$$\begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_t & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}; \quad d_1 \mid d_2 \mid \cdots \mid d_t$$

The d_i are known as *invariant factors*, and they are unique up to associates.

Proof. If $A = 0$, the matrix is already in Smith normal form. Otherwise, we can swap columns and rows such that $a_{11} \neq 0$. We will reduce $\varphi(a_{11})$ as much as possible until it divides every other element in the matrix, using the following algorithm.

STEP 1: If $a_{11} \nmid a_{1j}$ for some $j \geq 2$, then $a_{1j} = qa_{11} + r$ where $q, r \in R$ and $\varphi(r) < \varphi(a_{11})$. We can subtract q multiplied by column 1 from column j. Swapping these columns leaves $a_{11} = r$.

STEP 2: If $a_{11} \nmid a_{i1}$ for some $i \geq 2$, then repeat the above process using row operations.

STEP 1 and 2 decrease $\varphi(a_{11})$, so we repeat until $a_{11} \mid a_{1j}, a_{i1}$ for all $j \geq 2, i \geq 2$. We only need to repeat finitely many times as the Euclidean function takes values in $\mathbb{Z}_{\geq 0}$ and $\varphi(a_{11})$ strictly decreases in each iteration.

Now, we can subtract multiples of the first row to clear out the first column and multiples of the first column to clear out the first row to give

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

STEP 3: If $a_{11} \nmid a_{ij}$ for $i, j \geq 2$, then add the ith row to the first row. There is now an element in the first row, a_{ij}, that a_{11} does not divide. We can then perform column operations as in step 1 to decrease $\varphi(a_{11})$.

We will then restart the algorithm. After finitely many steps, this algorithm will terminate and a_{11} will divide all elements a_{ij} of the matrix.

$$A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}; \quad a_{11} \equiv d_1 \mid a_{ij}$$

We can now apply the algorithm to A', since column and row operations not including the first row or column do not change whether $a_{11} \mid a_{ij}$.

We now demonstrate uniqueness of the invariant factors. Suppose A has Smith normal form with invariant factors d_i where $d_1 \mid \cdots \mid d_t$. Then, for all k, $\mathrm{Fit}_k(A)$ can be evaluated in Smith normal form by invariance of the Fitting ideal under row and column operations. Hence $\mathrm{Fit}_k(A) = (d_1 d_2 \cdots d_k) \lhd R$. Thus, the product $d_1 \cdots d_k$ depends only on A, and is unique up to associates. Cancelling, we can see that each d_i depends only on A, up to associates. $\square$

Example 15.1

Consider the matrix over $\mathbb{Z}$ given by

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

Using elementary row and column operations,

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \xrightarrow{c_1 \mapsto c_1 + c_2} \begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix} \xrightarrow{c_2 \mapsto c_1 + c_2} \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix} \xrightarrow{r_2 \mapsto -3r_1 + r_2} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

This is in Smith normal form as $1 \mid 5$.

Alternatively, (d_1) is all the 1×1 minors, i.e. $(2, -1, 1, 2) = (1)$. So $d_1 = \pm 1$. Further, $(d_1 d_2) = (\det A) = (5)$. So $d_1 d_2 = \pm 5$ and hence $d_2 = \pm 5$.

§15.3 The structure theorem

Lemma 15.2

Let R be a Euclidean domain with Euclidean function φ (or, indeed, a principal ideal domain). Any submodule of the free module R^m is generated by at most m elements.

Proof. The $m = 1$ case was lemma 14.3.

Let $N \leq R^m$. Consider

$$I = \{r \in R : \exists\, r_2, \dots, r_m \in R,\ (r, r_2, \dots, r_m) \in N\}$$

Since N is a submodule, this is an ideal. Since R is a principal ideal domain, $I = (a)$ for some $a \in R$. Let $n = (a, a_2, \dots, a_m) \in N$. For $(r_1, \dots, r_m) \in N$, we have $r_1 = ra$ for some r. Hence $(r_1, \dots, r_m) - rn = (0, r_2 - ra_2, \dots, r_m - ra_m)$, which lies in $N' = N \cap (\{0\} \times R^{m-1}) \leq R^{m-1}$, hence $N = Rn + N'$. By induction, N' is generated by $n_2, \dots, n_m$, hence $\{n, n_2, \dots, n_m\}$ generate N. $\square$

Theorem 15.2

Let R be a Euclidean domain, and $N \leq R^m$. Then 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 $d_i \in R$ and $t \leq m$, and such that $d_1 \mid \cdots \mid d_t$.

Proof. By Lemma 15.2, we have $N = Ry_1 + \cdots + Ry_n$ for some $y_i \in R^m$ for some $n \leq m$. Each y_i belongs to R^m so we can form the $m \times n$ matrix A which has columns y_i. A is equivalent to a matrix A' in Smith normal form with invariant factors $d_1 \mid \cdots \mid d_t$.

A' is obtained from A by elementary row and column operations. Switching row i and row j in A corresponds to reassigning the standard basis elements e_i and e_j to each other. Adding a multiple of row i to row j corresponds to replacing $e_1, \ldots, e_m$ with a linear combination of these basis elements which is a free basis. In general, each row operation simply changes the choice of free basis used for R^m. Analogously, each column operation changes the set of generators y_i for N.

Hence, after applying these row and column operations, the free basis e_i of R^m is converted into $x_1, \ldots, x_m$, and N is generated by $d_1x_1, \ldots, d_tx_t$. □

Theorem 15.3 (Structure Theorem for finitely generated modules over Euclidean domains)

Let R be a Euclidean domain, and M a finitely generated module over R. Then

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

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

Proof. Since M is finitely generated, there exists a surjective R-module homomorphism $\varphi : R^m \to M$ for some m by Lemma 14.1. By the first isomorphism theorem, $M \cong {}^{R^m}\!/_{\ker\varphi}$. By Theorem 15.2, there exists a free basis $x_1, \ldots, x_m$ for R^m such that $\ker\varphi \leq R^m$ is generated by $d_1x_1, \ldots, d_tx_t$ where $d_1 \mid \cdots \mid d_t$. Then,

$$\begin{aligned} M &\cong \frac{\overbrace{R \oplus \ldots R}^{}_{m \text{ copies}}}{d_1R \oplus \cdots \oplus d_tR \oplus \underbrace{0 \oplus \cdots \oplus 0}_{m-t \text{ copies}}} \\ &\cong {}^{R}\!/_{(d_1)} \oplus \cdots \oplus {}^{R}\!/_{(d_t)} \oplus \underbrace{R \oplus \cdots \oplus R}_{m-t \text{ copies}} \quad \text{by Lemma 14.4} \end{aligned}$$

□

Remark 40. After deleting those d_i which are units, the invariant factors of M are unique up to associates. The proof is omitted.

Corollary 15.1

Let R be a Euclidean domain. Then any finitely generated torsion-free module is free.

Proof. Since M is torsion-free, there are no submodules of the form ${}^{R}\!/_{(d)}$ with d nonzero, since then multiplying an element of M by d would give zero. Hence, by the structure theorem, $M \cong R^m$ for some m. □

Example 15.2

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

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

which has Smith normal form $d_1 = 1$ and $d_2 = 5$. Hence, by changing basis for $\mathbb{Z}^2$, we can let N be generated by $(1, 0)$ and $(0, 5)$. Hence,

$$G \cong {}^{\mathbb{Z} \oplus \mathbb{Z}}\!/_{\mathbb{Z} \oplus 5\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$$

§15.4 Primary decomposition theorem

More generally, applying the structure theorem to $\mathbb{Z}$-modules, we obtain the structure theorem for finitely generated abelian groups:

Theorem 15.4 (Structure Theorem for finitely generated abelian groups)

Let G be a finitely generated abelian group. Then

$$G \cong C_{d_1} \times \dots \times C_{d_t} \times \mathbb{Z}^r$$

where $d_1 \mid \dots \mid d_t$ in $\mathbb{Z}$, and $r \geq 0$.

Proof. Take $R = \mathbb{Z}$ in structure theorem for modules. We have replaced the submodule notation ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ and $\oplus$ with the group notation C_n and $\times$. □

Remark 41. The special case of G finite means $r = 0$ and was quoted as Theorem 6.2.

We have also seen that any finite abelian group can be written as a product of cyclic groups of prime power order. This also has a generalisation for modules. The previous result relied on the lemma $C_{mn} \cong C_m \times C_n$ where m and n are coprime. There is an analogous result for principal ideal domains.

Lemma 15.3

Let R be a principal ideal domain, and $a, b \in R$ with $\gcd = 1$. Then, treating these quotients as R-modules,

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

Note. The case of $R = \mathbb{Z}$ was Lemma 6.1.

Proof. Since R is a principal ideal domain, $(a, b) = (d)$ for some $d \in R$. The greatest common divisor of a, b is a unit, so d is a unit, giving $(a, b) = R$. Hence, there exist $r, s \in R$ such that $ra + sb = 1$. This is a generalisation of Bézout's theorem.

Now, we define an R-module homomorphism $\psi : R \to R/(a) \oplus R/(b)$ by $\psi(x) = (x + (a), x + (b))$. Then $\psi(sb) = (sb + (a), sb + (b)) = (1 - ra + (a), sb + (b)) = (1 + (a), (b))$, and similarly $\psi(ra) = ((a), 1 + (b))$. Hence, $\psi(sbx + ray) = (x + (a), y + (b))$ so ψ is surjective.

Clearly we have $(ab) \subset \ker \psi$, so it suffices to show the converse. If $x \in \ker \psi$, then $x \in (a)$ and $x \in (b)$, so $x \in (a) \cap (b)$. Since $x = x(ra + sb) = r\underbrace{(ax)}_{\in (ab)} + s\underbrace{(bx)}_{\in (ab)}$, $x \in (ab)$. Hence $\ker \psi = (ab)$, and the result follows from the first isomorphism theorem for modules. □

Lemma 15.4 (Primary Decomposition Theorem)

Let R be a Euclidean domain and M a finitely generated R-module. Then

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

where the quotients are considered as R-modules, where p_i are primes in R, which are not necessarily distinct, and where $m \geq 0$.

Proof. By the structure theorem,

$$M \cong R/(d_1) \oplus \dots \oplus R/(d_t) \oplus \underbrace{R \oplus \dots \oplus R}_{m \text{ copies}} \cong R/(d_1) \oplus \dots \oplus R/(d_t) \oplus R^m$$

where $d_1 \mid \dots \mid d_t$. So it suffices to show that each $R/(d_i)$ can be written as a product of factors of the form $R/(p_j^{n_j})$. Since R is a unique factorisation domain and a principal ideal domain, d_i can be written as a product $up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where u is a unit and the p_j are pairwise non-associate primes. By Lemma 15.3,

$$R/(d_i) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_r^{\alpha_r})$$

□

§15.5 Rational canonical form

See tartarus for a good explainer of what $F[X]$ modules are and what is going on.

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

Lemma 15.5

If V is finite-dimensional as a vector space, then V_α is finitely generated as an $F[X]$-module.

Proof. Consider a basis $v_1, \dots, v_n$ of V, so $v_1, \dots, v_n$ generate V as an F-vector space. Then, these vectors generate V_α as an $F[X]$-module, since $F \leq F[X]$[a]. □

[a] Any element in V can be written as $\sum \lambda_i v_i$ for $\lambda_i \in F$. As $F \leq F[X]$, $\lambda_i \in F[x]$ so any element in V is a linear combination of the v_i in $F[X]$.

Example 15.3

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

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

Example 15.4

Suppose $V_\alpha \cong F[X]/(X-\lambda)^n$ as an $F[X]$-module. Consider the basis $1, X-\lambda, (X-$

$\lambda)^2, \ldots, (X-\lambda)^{n-1}$ for ${F[X]}/{(X-\lambda)^n}$ as an F-vector space. Here, $\alpha - \lambda\,\mathrm{id}$ has matrix $(*)$ from the previous example. Hence, α has matrix $(*) + \lambda I$.

Example 15.5

Suppose $V_\alpha \cong {F[X]}/{(f)}$ where $f \in F[X]$ as an $F[X]$-module, such that f is monic. Let

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

With respect to basis $1, X, \ldots, X^{n-1}$, α has matrix

$$C(f) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

since f is monic and the last column represents X^n. The above matrix is known as the *companion matrix* of the monic polynomial.

Theorem 15.5 (Rational canonical form)

Let F be a field, V be a finite-dimensional F-vector space, and $\alpha : V \to V$ be a linear map. Then the $F[X]$-module V_α decomposes as

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

for some monic polynomials $f_i \in F[X]$, and $f_1 \mid \cdots \mid f_t$. Moreover, with respect to a suitable basis, α has matrix

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

Proof. We know that V_α is finitely generated as an $F[X]$-module, since V is finite-dimensional by Lemma 15.5. Since $F[X]$ is a Euclidean domain, the structure theorem applies, and

$$V_\alpha \cong {}^{F[X]}\!\big/_{(f_1)} \oplus \cdots \oplus {}^{F[X]}\!\big/_{(f_t)} \oplus F[X]^m$$

for some m, where $f_1 \mid \cdots \mid f_t$. Since V is finite-dimensional as an F vector space, $m = 0$ as $F[X]$ is infinite-dimensional. As F is a field, wlog we may multiply each f_i by a unit to ensure that they are monic.

Then, using the previous example, we can construct the companion matrices for each polynomial and obtain the matrix as required. □

Remark 42.

1. If α is represented by an $n \times n$ matrix A, there exists a change of basis matrix P such that PAP^{-1} has form $(**)$ as stated in the theorem. Any square matrix over a field is similar to $(**)$.
2. Note further that $(**)$ can be used to find the minimal and characteristic polynomials of α; the minimal polynomial is f_t as if $f_i \mid f_j$ then $f_j = 0 \implies f_i = 0$. So $f_t = 0 \implies f_1 = f_2 = \cdots = f_{t-1} = 0$.
3. The characteristic polynomial is $f_1 \cdots f_t$.
4. In particular, the minimal polynomial divides the characteristic polynomial, and this implies the Cayley-Hamilton theorem.

Example 15.6

Consider $\dim V = 2$. Then, $\sum \deg f_i = 2$, so there are two cases: one polynomial of degree two, or two polynomials of degree one. Consider $V_\alpha \cong {}^{F[X]}\!\big/_{(X-\lambda)} \oplus {}^{F[X]}\!\big/_{(X-\mu)}$. Since one of the f_i must divide the other, we have $\lambda = \mu$. If we have one polynomial of degree two, we have $V_\alpha \cong {}^{F[X]}\!\big/_{(f)}$, where f is the characteristic polynomial of α.

Corollary 15.2

Let A, B be invertible 2×2 non-scalar matrices over a field F. Then A, B are similar iff their characteristic polynomials are equal.

Proof. ($\implies$): If A, B are similar they have the same characteristic polynomial, which is proven in Part IB Linear Algebra.

($\impliedby$): If the matrices are non-scalar, the modules V_α, V_β are of the form ${}^{F[X]}\!\big/_{(f)}$ by the previous example, so they are both similar to the companion matrix of f, where f is the characteristic polynomial of A or B. □

Definition 15.5 (Annihilator)
The **annihilator** of an R-module M is

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

Example 15.7
Let $I \lhd R$. Then the annihilator of ${}^{R}\!/\!_{I}$ is $\mathrm{Ann}_R\left({}^{R}\!/\!_{I}\right) = I$.

Example 15.8
Let A be a finite abelian group. Then, considering A as a $\mathbb{Z}$-module, $\mathrm{Ann}_{\mathbb{Z}}(A) = (e)$ where e is the *exponent* of the group, which is the lowest common multiple of the orders of elements in the group.

Example 15.9
Let V_α be as above. Then $\mathrm{Ann}_{F[X]}(V_\alpha) = (f)$ where f is the minimal polynomial of α.

§15.6 Jordan normal form

Jordan normal form concerns matrix similarity in $\mathbb{C}$. The following results are therefore restricted to this particular field.

Lemma 15.6
The primes (or equivalently, irreducibles) in $\mathbb{C}[X]$ are the polynomials $X - \lambda$ for $\lambda \in \mathbb{C}$, up to associates.

Proof. By the fundamental theorem of algebra, any non-constant polynomial with complex coefficients has a complex root. By the Euclidean algorithm, we can show that having a root λ is equivalent to having a linear factor $X - \lambda$. Hence the irreducibles have degree one, and thus are $X - \lambda$ exactly, up to associates. □

Theorem 15.6 (Jordan Normal Form)
Let $\alpha : V \to V$ be an endomorphism of a finite-dimensional $\mathbb{C}$-vector space V. Let V_α be the set V as a $\mathbb{C}[X]$-module, where scalar multiplication is defined by

$f \cdot v = f(\alpha)(v)$. Then, there exists an isomorphism of $\mathbb{C}[X]$-modules

$$V_\alpha \cong {}^{\mathbb{C}[X]}\big/_{((X-\lambda_1)^{n_1})} \oplus \cdots \oplus {}^{\mathbb{C}[X]}\big/_{((X-\lambda_t)^{n_t})}$$

where $\lambda_i \in \mathbb{C}$ are not necessarily distinct. In particular, there exists a basis for this vector space such that α has matrix in block diagonal form

$$\begin{pmatrix} J_{n_1}(\lambda_1) & & & \\ & J_{n_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{n_t}(\lambda_t) \end{pmatrix}$$

where each *Jordan block* $J_{n_i}(\lambda_i)$ is an $n_i \times n_i$ matrix of the form

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

Proof. Note $\mathbb{C}[X]$ is a Euclidean domain using the degree function, and V_α is finitely generated as a $\mathbb{C}[X]$-module by Lemma 15.5. These are the assumptions of the primary decomposition theorem so we can apply it, finding the module decomposition as required, noting that the primes in $\mathbb{C}[X]$ are the linear polynomials as in Lemma 15.6. Note that the free factor $\mathbb{C}[X]$ cannot appear in the decomposition since V is finite-dimensional.

We have already seen that for a module $W_\alpha \cong {}^{F[X]}\big/_{((X-\lambda)^n)}$, multiplication by X is represented by the matrix $J_n(\lambda)$ with respect to the basis $1, (X-\lambda), \dots, (X-\lambda)^{n-1}$. Hence the result follows by considering the union of these bases. $\square$

Remark 43.

1. If α is represented by a matrix A, then A is similar to a matrix in Jordan normal form. This is the form of the result often used in linear algebra.
2. The Jordan blocks are uniquely determined up to reordering. This can be proven by considering the dimensions of the *generalised eigenspaces*, which are $\ker((\alpha - \lambda\,\mathrm{id})^m)$ for some $m \in \mathbb{N}$.
3. The minimal polynomial of α is $\prod_\lambda (X-\lambda)^{c_\lambda}$ where c_λ is the size of the largest λ-block.
4. 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.
5. The number of λ-blocks is the dimension of the eigenspace of λ.

§15.7 Modules over principal ideal domains (non-examinable)

The structure theorem above was proven for Euclidean domains. This also holds for principal ideal domains. Some of the ideas relevant to this proof are illustrated in this subsection.

Theorem 15.7

Let R be a principal ideal domain. Then any finitely generated torsion-free R-module is free.

If R is a Euclidean domain, this was proven as a corollary to the structure theorem, Corollary 15.1.

Lemma 15.7

Let R be a principal ideal domain and M be an R-module. Let $r_1, r_2 \in R$ be not both zero, and let d be their greatest common divisor. Then,

1. there exists $A \in SL_2(R)$ such that

$$A \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

2. if $x_1, x_2 \in M$, then there exist $x_1', x_2' \in M$ 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 principal ideal domain, $(r_1, r_2) = (d)$. Hence, by definition, $d = \alpha r_1 + \beta r_2$ for some $\alpha, \beta \in R$. Let $r_1 = s_1 d$ and $r_2 = s_2 d$. Then $\alpha s_1 + \beta s_2 = 1$. Now, let

$$A = \begin{pmatrix} \alpha & \beta \\ -s_2 & s_1 \end{pmatrix} \implies \det A = 1; \quad A \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

as required.

For the second part, let $x_1' = s_1x_1 + s_2x_2$ and $x_2' = -\beta x_1 + \alpha x_2$. Then $Rx_1' + Rx_2' \subseteq Rx_1 + Rx_2$. The matrix defining x_1', x_2' in terms of x_1, x_2 is invertible since its determinant is a unit; we can solve for x_1, x_2 in terms of x_1', x_2'. So $Rx_1' + Rx_2' = Rx_1 + Rx_2$. Then by direct computation we can see that $r_1x_2 + r_2x_2 = dx_1' + 0 \cdot x_2'$. □

The structure theorem for principal ideal domains follows the same method; it is deduced for Smith normal form. That theorem also holds for principal ideal domains. The above lemma allows one to prove Smith normal form for principal ideal domains. In a Euclidean domain, we used the Euclidean function for a notion of size in order to perform induction; in a principal ideal domain we can count the irreducibles in a factorisation.

Proof of theorem. Let $M = Rx_1 + \dots + Rx_n$ where n is minimal. If $x_1, \dots, x_n$ are independent, then M is free as required. Suppose that the x_i are not independent, so there exists r_i such that $\sum r_i x_i = 0$ but not all of the r_i are zero. By reordering, we can suppose that $r_1 \neq 0$. By using part (ii) of the previous lemma, after replacing x_1 and x_2 by suitable x_1', x_2', we may assume that $r_1 \neq 0$ and $r_2 = 0$. By repeating this process with x_1 and x_i for all $i \geq 2$, we obtain $r_1 \neq 0$ and $r_2 = \dots = r_n = 0$, so $r_1 x_1'' = 0$ for some nonzero $x_1'' \in M$. But M is torsion-free, so r_1 must be zero, and this is a contradiction. □