Part IB — GRM

Based on lectures by Dr R Zhou

Lent 2022

Contents

§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 $\cdot \colon G \times G \to G$ 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 $|G| = |H| \cdot [G \colon H]$, where $[G \colon H]$ is the number of left cosets of H in G. $[G \colon H]$ 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 $g_1H \cdot g_2H = (g_1 \cdot g_2)H$. This can be shown to be well-defined.

§0.5 Homomorphisms

Let G, H be groups. A function $\varphi\colon G \to H$ 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 $\ker\varphi = \{g \in G \colon \varphi(g) = 1\}$, and the *image* of φ is $\operatorname{Im}\varphi = \{\varphi(g) \colon g \in G\}$. 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 $\varphi\colon G \to H$ is an isomorphism, we say that G and H are isomorphic, written $G \cong H$. Isomorphism is an equivalence relation. The isomorphism theorems are

1. if $\varphi\colon G \to H$, then ${}^{G}\!/_{\ker\varphi} \cong \operatorname{Im}\varphi$;
2. if $H \leq G$ and $N \trianglelefteq G$, then $H \cap N \trianglelefteq H$ and ${}^{H}\!/_{H \cap N} \cong {}^{HN}\!/_{N}$;
3. if $N \leq M \leq G$ such that $N \trianglelefteq G$ and $M \trianglelefteq G$, then ${}^{M}\!/_{N} \trianglelefteq {}^{G}\!/_{N}$, and ${}^{G/N}\!/_{M/N} = {}^{G}\!/_{M}$.

§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 3. 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 the correspondence theorem. □

§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 $\mathrm{Sym}(\{1, \dots, n\})$, 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 $\alpha \colon G \times X \to X$ 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 $\varphi \colon G \to \mathrm{Sym}(X)$.

Proof. For all $g \in G$, we can define $\varphi_g \colon X \to X$ 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

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

This is a homomorphism.

Conversely, any group homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$ 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. $\square$

Definition 2.4 (Permutation Representation)

The homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$ 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 $\mathrm{Orb}_G(x) = \{g * x \colon g \in G\} \subseteq X$;
2. the **stabiliser** of $x \in X$ is $G_x = \{g \in G \colon g * x = x\} \leq G$.

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 4. 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 5. 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 $\varphi\colon G \to \mathrm{Sym}(X)$ 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 $\mathrm{Im}\, \varphi = \mathrm{id}$, which is a contradiction since G acts transitively on X and $|X| > 1$. Thus $\ker \varphi = 1$, and $G \cong \mathrm{Im}\, \varphi \leq S_n$.

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

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

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. $\square$

§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 6. $\varphi\colon G \to G$ 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 $\varphi\colon G \to \mathrm{Sym}(G)$ 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 $\{g \in G\colon gHg^{-1} = H\} = N_G(H)$, 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

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, $|\mathrm{ccl}(g)||C(g)| = p^n$. In particular, $|\mathrm{ccl}(g)|$ 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 $\mathrm{ccl}_G(g) = \{g\}$. $\square$

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, hence $G \cong C_p$. $\square$

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 that any group G has a composition series $1 = G_1 \triangleleft \dots \triangleleft G_N = G$ 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 $r \in \{0, \dots, n\}$. $\square$

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. $\square$

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. $\square$

§4.2 Sylow theorems

Theorem 4.2

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 subsets 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 $0 \leq k < p^a$, 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 $G \curvearrowright \Omega$ by left-multiplication, so $g * X = \{gx \colon x \in X\}$. For any $X \in \Omega$, the orbit-stabiliser theorem can be applied to show that

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

By the above, 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 $|G| \leq |\mathrm{orb}_G(X)| \cdot |X|$, giving $|G_X| = \frac{|G|}{|\mathrm{orb}_G(X)|} \leq |X| = p^a$.

Combining with the above, 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. We claim that if P is a Sylow p-subgroup and $Q \leq G$ is a p-subgroup, then $Q \leq gPg^{-1}$ 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. 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 $Q \leq gPg^{-1}$ 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. Suppose $\{Q\}$ is another orbit of size 1, so Q is a Sylow p-subgroup which is preserved under conjugation by P. P normalises Q, so $P \leq N_G(Q)$. 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 $P = Q$ since $Q \trianglelefteq N_G(Q)$. Thus, $|P|$ is the unique orbit of size 1, so $n_p \equiv 1 \mod p$ as required.

$\square$

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. $\square$

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 $n_{11} = 12$. 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 $G \curvearrowright \mathrm{Syl}_3(G)$ by conjugation, and this generates a group homomorphism $\varphi\colon G \to S_4$. But the kernel of this homomorphism is a normal subgroup of G, so $\ker\varphi$ is trivial or G itself. 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, which is impossible.

Thus $n_3 = 22$. This means that G has $22 \cdot (3 - 1) = 44$ elements of order 3, 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.

§5 Matrix groups

§5.1 Definitions

Definition 5.1

Let F be a field, such as $\mathbb{C}$ or ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Let $GL_n(F)$ be set of $n \times n$ invertible matrices over F, which is called the *general 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*. $SL_n(F)$ is the kernel of the determinant homomorphism on $GL_n(F)$, so $SL_n(F) \triangleleft GL_n(F)$.

Let $Z \triangleleft GL_n(F)$ denote the subgroup of *scalar matrices*, the group of nonzero multiples of the identity. The group $PGL_n(F) = {}^{GL_n(F)}\!/_{Z}$ is called the *projective general linear group*. Let $PSL_n(F) = {}^{SL_n(F)}\!/_{Z \cap SL_n(F)}$. 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 $A \in G$ if and only if 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

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

Since the scalar matrices act trivially, we obtain an action on the projective general linear group instead of the general linear group. 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 the example above,

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

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

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

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,

$$Z \cap SL_2\left(\mathbb{Z}/p\mathbb{Z}\right) = \{\pm 1\}$$

and the elements 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. □

Example 5.2

Let $G = PSL_2\left(\mathbb{Z}/5\mathbb{Z}\right)$. Then by the previous lemma, $|G| = 60$. Let $G \curvearrowright \mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ by Möbius transformations. The permutation representation $\varphi\colon G \to \mathrm{Sym}(\{0,1,2,3,4,\infty\})$ is injective, since the permutation representation of $PGL_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ is known to be injective by a previous lemma.

We claim that $\operatorname{Im}\varphi \subseteq A_6$. Let $\psi = \operatorname{sgn}\circ\varphi$. If we can show ψ is trivial, $\operatorname{Im}\varphi \subseteq A_6$. Let $h \in G$, and suppose h has order $2^n m$ for odd m. 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 the second Sylow theorem, 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 $\ker\psi$ is normal 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 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 $\langle (g, h) \rangle = C_m \times C_n$. □

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 $n = p_1 a^1 \cdots p^r a^r$ where the p_i are distinct primes, then applying the above lemma inductively gives C_n 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. □

Later, we will prove the following refinement of this theorem.

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 7. The integers $n_1, \dots, n_k$ in the corollary above are unique up to ordering. The integers $d_1, \dots, d_t$ are also unique, assuming that $d_1 > 1$. The proofs will be omitted.

Example 6.1

The abelian groups of order 8 are exactly C_8, $C_2 \times C_4$, and $C_2 \times C_2 \times C_2$. The abelian groups of order 12 are, using the corollary above, $C_2 \times C_2 \times C_3$, $C_4 \times C_3$, and using the above theorem, $C_2 \times C_6$ 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

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 6.2

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

Corollary 6.2

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. □

§7 Rings

§7.1 Definitions

Definition 7.1

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 8. For all $x \in R$,

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

Further,

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

Definition 7.2

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

Remark 9. 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 $\mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. This is known as the ring of Gaussian integers. The set $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\right\}$ is a subring of $\mathbb{R}$.

Example 7.2

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

Example 7.3

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

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

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

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

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

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

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

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

Example 7.4

${\mathbb{Z}}/{n\mathbb{Z}}$ is a field only if n is a prime.

Remark 10. 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 the degree of r is less than the degree of g.

Remark 11. This is the Euclidean algorithm for division, adapted to polynomial rings.

Proof. Let n be the degree of f and m be the degree of g, so

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

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 $f_1 = f - a_n b_m^{-1} g X^{n-m}$. 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 12. 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 7.5

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 7.6

Let R be a ring. Then the *power series ring* $R[\![X]\!]$ is the set of power series on X. 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 7.7

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

§7.3 Homomorphisms

Definition 7.6

Let R and S be rings. A function $\varphi\colon R \to S$ 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).

A ring homomorphism is an *isomorphism* if it is bijective. The *kernel* of a ring homomorphism is $\ker \varphi = \{r \in R : \varphi(r) = 0\}$.

Lemma 7.1

Let R, S be rings. Then a ring homomorphism $\varphi\colon R \to S$ is injective if and only if $\ker \varphi = \{0\}$.

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

§7.4 Ideals

Definition 7.7

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

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

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

Lemma 7.2

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

Proof. We know that $\ker\varphi$ is a subgroup by the equivalent fact from groups. 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 13. 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 7.3

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

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. 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 $r \in \{0, 1, \dots, n-1\}$. 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 7.8

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

Definition 7.9

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

§7.5 Quotients

Theorem 7.1

Let $I \trianglelefteq R$. Then the set ${}^{R}\!/_{I}$ of cosets 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.

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

$$r_1' r_2' = (r_1 + a_1)(r_2 + a_2) = r_1 r_2 + a_1 r_2 + r_1 a_2 + a_1 a_2$$

Hence $(r_1' r_2') + I = (r_1 r_2) + I$. The remainder of the proof is trivial. $\square$

Example 7.8

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 $n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$. Addition and multiplication behave like in modular arithmetic modulo n.

Example 7.9

Consider the ideal (X) inside the polynomial ring $\mathbb{C}[X]$. This ideal is the set of polynomials with zero constant term. Let $f(X) = a_n X^n + \dots + a_0$ be an arbitrary element of $\mathbb{C}[X]$. 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 7.10

Consider $(X^2 + 1) \triangleleft \mathbb{R}[X]$. For $f(X) = a_n X^n + \dots + a_0 \in \mathbb{R}[X]$, we can apply the Euclidean algorithm to write $f(X)$ as $q(X)(X^2 + 1) + r(X)$ where the degree of r is less than two. Hence $r(X) = a + bX$ for some real numbers a and b. 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 $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

§7.6 Isomorphism theorems

Theorem 7.2 (first isomorphism theorem)
Let $\varphi\colon R \to S$ be a ring homomorphism. Then,

$$\ker\varphi \lhd R; \quad \operatorname{Im}\varphi \leq S; \quad R/\ker\varphi \cong \operatorname{Im}\varphi$$

Proof. We have $\ker\varphi \lhd R$ from above. 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 $\Phi\colon R/K \to \operatorname{Im}\varphi$ 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.

$$\Phi(1_R+K) = \varphi(1_R) = 1_S; \quad \Phi((r_1+K)(r_2+K)) = \Phi(r_1r_2+K) = \varphi(r_1r_2) = \varphi(r_1)\varphi(r_2)$$

The result follows as required. □

Theorem 7.3 (second isomorphism theorem)
Let $R \leq S$ and $J \lhd S$. Then,

$$R \cap J \lhd R; \quad R + J = \{r + a \colon r \in R, a \in J\} \leq S; \quad {}^{R}\!/_{R \cap J} \cong {}^{R+J}\!/_{J} \leq {}^{S}\!/_{J}$$

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 $1_S \in R \cap J$. If $r_1, r_2 \in R$ and $a_1, a_2 \in J$, we have

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

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

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

Remark 14. If $I \lhd R$, there exists a bijection between ideals in ${}^{R}\!/_{I}$ and the ideals of R containing I. Explicitly,

$$K \mapsto \{r \in R \mid r + I \in K\}; \quad J \mapsto {}^{J}\!/_{I}$$

Theorem 7.4 (third isomorphism theorem)
Let $I \lhd R$ and $J \lhd R$ with $I \subseteq J$. Then,

$${}^{J}\!/_{I} \lhd {}^{R}\!/_{I}; \quad {}^{R/I}\!/_{J/I} \cong {}^{R}\!/_{J}$$

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

Remark 15. ${}^{J}\!/_{I}$ is not a quotient ring, since J is not in general a ring; this notation should be interpreted as a set of cosets.

Example 7.11

Consider the surjective ring homomorphism $\varphi\colon \mathbb{R}[X] \to \mathbb{C}$ 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, yielding $\ker\varphi = (X^2+1)$. Applying the first isomorphism theorem, we immediately find $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Example 7.12

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

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

This inductively defines

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

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

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

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 $0 = 1$. The number n is known as the *characteristic* of R.

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.

§7.7 Integral domains

Definition 7.10

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 $b = 0$. 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 if and only if it has no zero divisors.

Example 7.13

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

Example 7.14

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

Lemma 7.4

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. □

Lemma 7.5

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

Proof. Exercise on the example sheets. □

Theorem 7.5

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 a previous structure theorem for finite abelian groups to show that there exists $H \leq G$ such that $H \cong C_{d_1} \times C_{d_1}$ 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. □

Example 7.15

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

Proposition 7.2

Any finite integral domain is a field.

Proof. Let $0 \neq a \in R$, where R is an integral domain. Consider the map $\varphi\colon R \to R$ given by $x \mapsto ax$. If $\varphi(x) = \varphi(y)$, then $a(x-y) = 0$. But $a \neq 0$, hence $x - y = 0$. Hence φ is injective. Since R is finite, φ is a bijection, hence it has an inverse φ^{-1}, which yields the multiplicative inverse of a by considering $\varphi^{-1}(a)$. This may be repeated for all a. □

Theorem 7.6

Any integral domain R is a subring of a field F, and 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 $S = \{(a,b) \in R\colon b \neq 0\}$. We can define an equivalence relation

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

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

$$\begin{aligned}
(a,b) \sim (c,d) \sim (e,f) &\implies ad = bc;\ cf = de \\
&\implies adf = bcf = bde \\
&\implies af = be \\
&\implies (a,b) \sim (e,f)
\end{aligned}$$

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 $\frac{a}{b} \cdot \frac{b}{a} = 1$. Hence F is a field.

We can identify R with the subring of F given by $\frac{r}{1}$ for all $r \in R$. This is clearly isomorphic to R. Further, any element of F can be written as $\frac{a}{b} = ab^{-1}$ as required. $\square$

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

Example 7.16

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

§7.8 Maximal ideals

Definition 7.11

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

Lemma 7.6

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

Proof. 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. Hence $I = R$.

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. $\square$

Proposition 7.3

Let $I \triangleleft R$. Then I is maximal if and only if ${R}/{I}$ is a field.

Proof. ${R}/{I}$ is a field if and only if its ideals are either zero, denoted ${I}/{I}$, or ${R}/{I}$ itself. By the correspondence theorem, I and R are the only ideals in R which contain I. Equivalently, $I \triangleleft R$ is maximal. $\square$

§7.9 Prime ideals

Definition 7.12

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 7.17

The ideals in the integers are (n) for some $n \geq 0$. $n\mathbb{Z}$ is a prime ideal if and only if 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 $p \mid b$. 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 7.4

Let $I \triangleleft R$. Then I is prime if and only if ${}^{R}\!/_{I}$ 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. $\square$

Remark 16. If I is a maximal ideal, then ${}^{R}\!/_{I}$ is a field. A field is an integral domain. Hence any maximal ideal is prime.

Remark 17. 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. 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).