

Groups, Rings and Modules

ADAM KELLY

February 13, 2021

This set of notes is a work-in-progress account of the course ‘Groups, Rings and Modules’, originally lectured by Dr Tom Fisher in Lent 2020 at Cambridge. These notes are not a transcription of the lectures, but they do roughly follow what was lectured (in content and in structure).

These notes are my own view of what was taught, and should be somewhat of a superset of what was actually taught. I frequently provide different explanations, proofs, examples, and so on in areas where I feel they are helpful. Because of this, this work is likely to contain errors, which you may assume are my own. If you spot any or have any other feedback, I can be contacted at ak2316@cam.ac.uk.

Contents

1	Groups	4
1.1	Groups	4
1.1.1	Definitions	4
1.1.2	Isomorphism Theorems	6
1.1.3	Simple Groups	8
1.2	Group Actions	9
1.2.1	Definitions	9
1.2.2	Orbits and Stabilisers	10
1.2.3	Using Group Actions	10
1.3	Alternating Groups	13
1.3.1	Conjugacy Classes & Simplicity of A_n	13
1.4	p -Groups and p -Subgroups	15
1.4.1	Basic Properties of p -Groups	15
1.4.2	Sylow Theorems	16
1.5	Some Groups	18
1.5.1	Matrix Groups	18
1.5.2	Finite Abelian Groups	20
2	Rings	22
2.1	Rings	22
2.1.1	Definitions	22
2.1.2	Constructing Rings	23
2.1.3	Units and Fields	24

1 Groups

§1.1 Groups

The first algebraic object that we shall consider in this course is one you are likely familiar with – a group.

§1.1.1 Definitions

We will begin by defining what a group is.

Definition 1.1.1 (Group)

A **group** is a pair $(G, *)$ consisting of a set G and a binary operation $^a *: G \times G \rightarrow G$ satisfying the axioms:

- *Identity.* There is an element $e \in G$ such that $e * g = g * e = g$ for all $g \in G$,
- *Inverses.* For every element $g \in G$, there is an element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.
- *Associativity.* The operation $*$ is associative.

^aSome texts include an additional *closure* axiom, but this is implied by $*$ being a binary operation on G .

Remark. We will usually either use additive or multiplicative notation for groups, and in these cases we will often write 0 or 1 for the identity respectively.

Definition 1.1.2 (Subgroup)

A subset $H \subseteq G$ is a **subgroup** of G , written $H \leq G$, if it is a group with respect to the operation $*$ defined on $H \times H$.

There is a way to test the conditions needed for a subset to be a subgroup in just a few lines, but it does have limited utility.

Lemma 1.1.3 (Fast Subgroup Checking Lemma)

A nonempty subset $H \subseteq G$ is a subgroup if $a, b \in H$ implies $a * b^{-1} \in H$.

Proof Sketch. Check that this implies the definition. □

Example 1.1.4 (Examples of Groups)

The following are all examples of groups.

- The additive groups $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
- The cyclic group of order n , C_n .

- (iii) The dihedral group D_{2n} of the symmetries of a regular n -gon.
- (iv) The symmetric group S_n and alternating group A_n , where S_n is the group of permutations of $\{1, 2, \dots, n\}$ and $A_n \leq S_n$ is the group of even permutations.
- (v) The quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = ijk = -1$.
- (vi) The matrix groups over some field F , $\text{GL}_n(F)$ of all $n \times n$ matrices over F with non-zero determinant, and $\text{SL}_n(F) \leq \text{GL}_n(F)$, the subgroup of matrices with determinant 1.

Definition 1.1.5 (Direct Product)

The **direct product** of groups G and H is $G \times H$ with operation $(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

For a subgroup $H \leq G$, the **left cosets** of H in G are the sets $gH = \{gh \mid h \in H\}$ where $g \in G$. Recall that these partition G , and each has the same cardinality as H . From this we deduce Lagrange's theorem.

Theorem 1.1.6 (Lagrange's Theorem)

Let G be a finite group, and H be a subgroup. Then $|G| = |H| \cdot |G : H|$ where $|G : H|$ is the **index** of H in G , the number of left cosets of H in G .

It is natural to wonder whether there is a converse to Lagrange's theorem, and it turns out that the converse is *not* true in general. There is a partial converse however.

Theorem 1.1.7 (First Sylow Theorem)

If G is a group with $|G| = p^a m$ where p is a prime and $p \nmid m$, then there exists $H \leq G$ with $|H| = p^a$.

We will prove this theorem later on.

Definition 1.1.8 (Order of an Element)

Let G be a group and $g \in G$. 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 g has infinite order.

Remark. If g has order d , then $g^n = 1 \iff d \mid n$. The proof follows from the division algorithm. Also, $\{1, g, g^2, \dots, g^{d-1}\} \leq G$ and so if G is finite, then by Lagrange, $d \mid |G|$.

Definition 1.1.9 (Normal Subgroup)

A subgroup $H \leq G$ is **normal** if $g^{-1}Hg = H$ for all $g \in G$. We write $H \trianglelefteq G$ in this case.

Proposition 1.1.10 (Quotient Group)

If $H \trianglelefteq G$, then the set G/H of left cosets of H in G is a group called the **quotient group** with the operation $g_1 H * g_2 H = (g_1 g_2) H$.

Proof. We must check that $*$ is well defined. Suppose that $g_1H = g'_1H$ and $g_2H = g'_2H$. Then $g'_1 = g_1h_1$ and $g'_2 = g_2h_2$ for some $h_1, h_2 \in H$. Then we get $g'_1g'_2H = g_1h_1g_2h_2H = g_1h_1g_2H$. This is equal to g_1g_2H if and only if $(g_1g_2)^{-1}g_1h_1g_2 \in H$, that is, if $g_2^{-1}h_1g_2 \in H$, which follows from the normality of H . Now to check the group axioms, note that associativity is inherited, we have the coset H being the identity, and the inverse of gH being $g^{-1}H$. Thus G/H is a group. \square

§1.1.2 Isomorphism Theorems

We will now review the isomorphism theorems, beginning by defining a homomorphism.

Definition 1.1.11 (Group Homomorphism)

If G, H are groups, a function $\phi : G \rightarrow H$ is a **group homomorphism** if $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$.

Definition 1.1.12 (Kernel/Image)

The **kernel** of a group homomorphism ϕ is $\ker(\phi) = \{g \in G \mid \phi(g) = e\}$. The **image** of ϕ is $\text{img}(\phi) = \{\phi(g) \mid g \in G\}$. Also $\ker(\phi) \leq G$ and $\text{img}(\phi) \leq H$.

If we have some homomorphism $\phi : G \rightarrow H$, then the kernel is a normal subgroup of G . Indeed, if $a \in \ker(\phi)$ and $g \in G$, then $\phi(g^{-1}ag) = \phi(g)^{-1}\phi(a)\phi(g) = e$, so $g^{-1}ag \in \ker(\phi)$ too, hence $\ker(\phi) \trianglelefteq G$.

Definition 1.1.13 (Group Isomorphism)

A **group isomorphism** is a group homomorphism that is also a bijection. We say G and H are **isomorphic**, written $G \cong H$, if there exists an isomorphism $\phi : G \rightarrow H$.

Remark. If $\phi : G \rightarrow H$ is a group isomorphism, then so is ϕ^{-1} .

We now come to the isomorphism theorems.

Theorem 1.1.14 (First Isomorphism Theorem)

Let $\phi : G \rightarrow H$ be a group homomorphism. Then $\ker(\phi) \trianglelefteq G$, and $G/\ker(\phi) \cong \text{img}(\phi)$.

Proof. Let $K = \ker(\phi)$. We already checked that $K \trianglelefteq G$. Now define $\Phi : G/K \rightarrow \text{img}(\phi)$ by $gK \mapsto \phi(g)$.

We first check Φ is well defined and injective. We have

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

Then we check that Φ is a group homomorphism, with

$$\begin{aligned}\Phi(g_1 K g_2 K) &= \Phi(g_1 g_2 K) \\ &= \phi(g_1 g_2) \\ &= \phi(g_1) \phi(g_2) \\ &= \Phi(g_1 K) \Phi(g_2 K).\end{aligned}$$

Lastly we check that it is surjective. Let $x \in \text{img}(\phi)$, say $x = \phi(g)$ for some $g \in G$. Then $x = \Phi(gK) \in \text{img}(\Phi)$. \square

Example 1.1.15 (Using the First Isomorphism Theorem)

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

We find that $\ker(\phi) = \{z \in \mathbb{C} \mid e^z = 1\} = 2\pi i\mathbb{Z}$, and $\text{img}(\phi) = \mathbb{C}^*$. Thus $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^*$.

With the first isomorphism theorem, it is not enough to know the statement and proof – you have to know when to employ it. For example, if asked to prove $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^*$, you should be able to think of a strategy similar to the one used above.

The first isomorphism theorem is sometimes just called the ‘isomorphism theorem’, and it tends to be more important than the corollaries that we will state.

Corollary 1.1.16 (Second Isomorphism Theorem)

Let $H \leq G$ and $K \trianglelefteq G$. Then $HK = \{hk \mid h \in H, k \in K\} \leq G$ and $H \cap K \trianglelefteq H$, moreover $HK/K \cong H/H \cap K$.

Proof. Let $h_1 k_1, h_2 k_2 \in HK$. We have

$$\begin{aligned}h_1 k_1 (h_2 k_2)^{-1} &= h_1 k_1 k_2^{-1} h_2^{-1} \\ &= h_1 h_2^{-1} h_2 k_1 k_2^{-1} h_2^{-1} \\ &= (h_1 h_2^{-1}) (h_2 k_1 k_2^{-1} h_2^{-1}) \in HK,\end{aligned}$$

thus $HK \leq G$, as required.

Now let $\phi : H \mapsto G/K$ with $h \mapsto hK$. This is the composite of the inclusion $H \hookrightarrow G$ and the quotient map $G \rightarrow G/K$, thus ϕ is a group homomorphism.

We note $\ker(\phi) = \{h \in H \mid hK = K\} = H \cap K \trianglelefteq H$, and $\text{img}(\phi) = \{hK \mid h \in H\} = HK/K$. Thus by the first isomorphism theorem, $H/H \cap K \cong HK/K$. \square

Before we state the third isomorphism theorem, consider the following motivation. Suppose $K \trianglelefteq G$. There is a bijection

$$\{\text{subgroups of } G/K\} \longleftrightarrow \{\text{subgroups of } G \text{ containing } K\},$$

obtained by considering the maps $x \mapsto \{g \in G \mid gK \in X\}$ and $H \mapsto H/K$. This restricts to a bijection between

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

Corollary 1.1.17 (Third Isomorphism Theorem)

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

$$(G/K)/(H/K) \cong G/H.$$

Proof. Let $\phi : G/K \rightarrow G/H$ with $gK \mapsto gH$. If $g_1K = g_2K$, then $g_2^{-1}g_1 \in K \leq H$, so $g_1H = g_2H$, and thus ϕ is well defined. Also ϕ is a surjective group homomorphism with kernel $\ker(\phi) = H/K$. Then apply the first isomorphism. \square

§1.1.3 Simple Groups

If $K \trianglelefteq G$, then studying the groups K and the quotient group G/K gives some information about G . However, this approach is not always available.

Definition 1.1.18 (Simple Group)

A group G is **simple** if $\{e\}$ and G are its only normal subgroups.

Lemma 1.1.19 (Abelian Simple Groups)

An abelian group is simple if and only if it is isomorphic to C_p for some prime p .

Proof. By Lagrange's theorem, a subgroup $H \leq C_p$ has order dividing $|C_p| = p$, which is a prime. Hence H has order 1 or p , and H is either $\{e\}$ or $H = G$.

Now let G be an abelian simple group, and $g \in G$ with $g \neq e$. Note that any subgroup of an abelian group is normal, and thus G must have no subgroups other than G and $\{e\}$. But then G has subgroup $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$. Since G is simple, this must be the whole group, that is, G is cyclic.

If G is the infinite cyclic group, then $G \cong (\mathbb{Z}, +)$, which is not simple (as $2\mathbb{Z} \trianglelefteq \mathbb{Z}$). Thus $G \cong C_n$ for some n . Let g be a generator for C_n . If $m \mid n$, then $\langle g^{n/m} \rangle$ is a subgroup of order m , but G is simple thus $m = 1$ or n , hence n must be prime. \square

Lemma 1.1.20 (Composition Series of Finite Groups)

If G is a finite group then G has a composition series $\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{m-1} \triangleleft G_m = G$, with each quotient G_i/G_{i-1} is simple.

[Note that G_i need not be normal in G .]

Proof. We induct on $|G|$. If $|G| = 1$ we are done. If $|G| > 1$, then let G_{m-1} be a normal subgroup of largest possible order (not $|G|$). Then G/G_{m-1} is simple, and by induction on G_{m-1} , we are done. \square

§1.2 Group Actions

A useful way to study a group is by studying how it ‘acts’ on some set. The way we look at this mathematically is through the lense of group actions.

§1.2.1 Definitions

We will begin by looking at groups of permutations of a set.

Definition 1.2.1 ($\text{Sym}(X)$)

For a set X , let $\text{Sym}(X)$ be the group of all bijections $X \rightarrow X$ under composition. We let the identity of this group be id .

Definition 1.2.2 (Permutation Group)

A group G is a **permutation group** (of degree n) if $G \leq \text{Sym}(X)$ (where $|X| = n$).

Example 1.2.3 (Examples of Permutation Groups)

The group $S_n = \text{Sym}(\{1, 2, \dots, n\})$ is a permutation group of degree n , as is the alternating group $A_n \leq S_n$.

The group D_n , the symmetries of a regular n -gon, is a permutation group as it is a subgroup of $\text{Sym}(\{\text{vertices of an } n\text{-gon}\})$.

We can now generalize the notion of a permutation group to the idea mentioned before – a group acting on a set. Slightly more useful (and general) than permutation groups is the notion of a group acting on a set.

Definition 1.2.4 (Group Action)

An action of a group G on a set X is a function $* : G \times X \rightarrow X$ satisfying

- (i) $e * x = x$ for all $x \in X$.
- (ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G$ and $x \in X$.

We also think about group actions in the following way, and switching between the points of view can be quite helpful.

Proposition 1.2.5

An action of a group G on a set X is equivalent to specifying a group homomorphism $\phi : G \rightarrow \text{Sym}(X)$.

Proof. For each $g \in G$, there is a function $\phi_g : X \rightarrow X$ given by $x \mapsto g * x$. We have $\phi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \phi_{g_1}(\phi_{g_2}(x))$. Thus $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}$.

In particular, $\phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \phi_e = \text{id}$. Thus ϕ_g is a bijection, and $\phi_g \in \text{Sym}(X)$. We define $\phi : G \rightarrow \text{Sym}(X)$ with $g \mapsto \phi_g$. Then this is a group homomorphism by the above.

Conversely, let $\phi : G \rightarrow \text{Sym}(X)$ be a group homomorphism. Then defining $*$: $G \times X \rightarrow X$ with $(g, x) \mapsto \phi(g)(x)$, we have that this is a group action since $e * x = \phi(e)(x) = \text{id}(x) = x$ and $(g_1 g_2) * x = \phi(g_1 g_2)(x) = \phi(g_1)(\phi(g_2)(x)) = g_1 * (g_2 * x)$. \square

Definition 1.2.6 (Permutation Representation)

We say $\phi : G \rightarrow \text{Sym}(X)$ is a **permutation representation** of G .

§1.2.2 Orbits and Stabilisers

A useful notion is that of *orbits* and *stabilisers*. Informally, the orbit of an element x in a set S acted on by a group G is all of the elements that can be reached by applying elements of G . The stabiliser of x is the set of elements in G so that when we apply them, we still have the element x .

Definition 1.2.7 (Orbits and Stabilisers)

Let G act on a set X . The **orbit** of an element $x \in X$ is $\text{Orb}_G(x) = \{g * x \mid g \in G\}$, which is a subset of X . The **stabiliser** of $x \in X$ is $\text{Stab}_G(x) = \{g \in G \mid g * x = x\}$, which is a subgroup of G .

The orbits partition the set X . If there is only one orbit then we say that the group action is **transitive**. We recall the Orbit-Stabiliser theorem.

Theorem 1.2.8 (Orbit-Stabiliser Theorem)

There is a bijection between $\text{Orb}_G(x)$ and the set of left cosets of $\text{Stab}_G(x)$ in G . In particular, if G is finite, then

$$|G| = |\text{Orb}_G(x)| \cdot |\text{Stab}_G(x)|.$$

Remark. The kernel of ϕ can be thought of as $\ker \phi = \bigcap_{x \in X} \text{Stab}_G(x)$ is called the **kernel of the group action**. Also $\text{Stab}_G(g * x) = g \text{Stab}_G(x) g^{-1}$, so if $x, y \in X$ belong to the same orbit then their stabilisers are conjugate subgroups of G .

§1.2.3 Using Group Actions

In many cases, the choosing the right group action can help make progress on a problem. With this in mind, it's helpful to have a list of standard group actions that you can apply.

Example 1.2.9 (Examples of Group Actions)

The following are all group actions.

- (i) Let G act on itself by left multiplication, with $g * x = gx$. The kernel of this action is $\{g \in G \mid gx = x\} = \{e\}$, and thus G injects into $\text{Sym}(G)$. This proves Cayley's theorem, that any finite group G is isomorphic to a subgroup of S_n for some n (say $n = |G|$).
- (ii) Let $H \leq G$. Then G acts on the left cosets of H in G by left multiplication. This group action is transitive, with $\text{Stab}_H(x) = \{g \in G \mid gxH = xH\} =$

xHx^{-1} . We have the kernel $\ker(\phi) = \bigcap_{x \in G} xHx^{-1}$, which is the largest normal subgroup of G contained in H .

- (iii) Let G act on itself by conjugation, so $g * x = gxg^{-1}$. Here, the orbits and stabilisers are $\text{Orb}_G(x) = \{gxg^{-1} \mid g \in G\} = \text{ccl}_G(x)$, the **conjugacy class** of x in G . The stabilisers are $\text{Stab}_G(x) = \{g \in G \mid gx = xg\} = C_G(x) \leq G$, the **centraliser** of x . The kernel of this action is the **center**, $Z(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$.

G also acts by conjugation on any normal subgroup.

- (iv) Let X be the set of all subgroups of G . Then G acts on X by conjugation. That is, $g * H = gHg^{-1} \leq G$. The stabiliser of H is $\{g \in G \mid gHg^{-1} = H\} = N_G(H)$ is the **normaliser** of H in G . This is the largest subgroup of G to contain H as a normal subgroup. In particular $H \trianglelefteq G \iff N_G(H) = G$.

Of this last, the frequently useful actions (that you should readily reach for) are the left multiplication of cosets, conjugation of elements and subgroups.

To see how we can apply group actions to proving a theorem, consider the following result (and mainly it's proof). Here we will use the action of G on the left cosets of a subgroup H .

Theorem 1.2.10

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

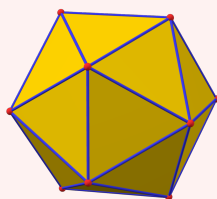
Proof. Let G act on X , the set of left cosets of H in G , by left multiplication, and let $\phi : G \rightarrow \text{Sym}(X)$ be the associated permutation representation. Then $\text{Sym}(X) = S_n$. As G is simple, we know that $\ker \phi = \{e\}$ or G . If $\ker \phi = G$, then $\text{img } \phi = \{e\}$, contradicting that G acts transitively on X (since $n > 1$). Thus $\ker \phi$ is trivial, and $G \cong \text{img } \phi \leq S_n$.

Since $G \leq S_n$ and $A_n \trianglelefteq S_n$, the second isomorphism theorem gives $G \cap A_n \trianglelefteq G$ and $G/G \cap A_n \leq S_n/A_n \cong C_2$. But G is simple so $G \cap A_n = \{e\}$ or G . If $G \cap A_n = \{e\}$, then $G \hookrightarrow C_2$, which contradicts that G is non-abelian. Otherwise, $G \cap A_n = G$, and $G \leq A_n$. Finally if $n \leq 4$, then A_n has no non-abelian simple subgroups (by listing them), so $n \geq 5$. \square

Another example, looking at the rotational symmetries of an icosahedron, is given below.

Example 1.2.11 (Rotational Symmetries of an Icosahedron)

Let G be the group of rotations of an icosahedron, as pictured.



In this shape, there is 20 faces, 12 vertices and 30 edges. We want to know the possible orders of elements in this group, and the number of elements of each order.

Order	Number of Elements in G
1	1
2	15
3	20
5	24

This gives us a total of 60 elements. We can verify this with the orbit-stabiliser theorem. For G acting on the vertices, and some vertex v , we have $|G| = |\text{Orb}(v)| \cdot |\text{Stab}(v)| = 12 \cdot 5 = 60$.

To consider the conjugacy classes, we note that two elements are conjugate if they 'look the same up to relabelling the icosahedron'.

The elements of order 2 are all conjugate, as are those by order 3. The elements of order 5 split into two conjugacy classes of equal size (12), as the rotations by $\pm \frac{2\pi}{5}$ are all conjugate and rotations by $\pm \frac{4\pi}{5}$ are all conjugate, but not to each-other.

We can use this to deduce G is simple. If $H \leq G$, then $|H| = 1 + 15a + 20b + 12c$ for $a, b \in \{0, 1\}$ and $c \in \{0, 1, 2\}$, but as $|H| \mid 60$ by Lagrange, we get $|H| = 1$ or 60. Thus G is simple.

In fact, G is isomorphic to A_5 . We will show that the sets $H \leq \{1\}$ for $H \leq G$ a subgroup of order 4 partitions the 15 elements of order 2 into 5 sets of 3.

1. If $|H| = 4$, then $H \cong C_2 \times C_2$ or $H \cong C_4$. But there is no elements of order 4 in G , so $H \cong C_2 \times C_2$. Note that this has three elements of order 2.
2. If $g \in G$ has order 2, then $g \in C_G(g)$ and $|C_G(g)| = \frac{|G|}{|\text{cl}_G(g)|} = \frac{60}{15} = 4$.
3. Suppose $e \neq g \in H \cap K$ where H and K are distinct subgroups of order 4. Then $|C_G(g)| \geq |H \cup K|$ since H and K are abelian, and $|H \cup K| > 4$.

This proves the claim. Now let G act on the set X of subgroups of order 4 by conjugation. We obtain a group homomorphism $\phi : G \rightarrow \text{Sym}(X) = S_5$. Then G simple implies either $\ker \phi = \{e\}$ or G . If it was G , then we would get that there is a normal subgroup of order 4m, which is a contradiction. Thus the kernel is trivial, and $G \cong S_5$. Then exactly as before, either $G \cong C_2$ or $G \leq A_5$, and thus $|G| = |A_5| = 60$, so $G \cong A_5$.

§1.3 Alternating Groups

We know from the ‘Groups’ course that two permutations in S_n are conjugate if and only if they have the same cycle type.

Example 1.3.1 (Conjugacy Classes in S_5)

In S_5 , we have the following:

Cycle Type	Number of Elements	Sign
1, 1, 1, 1, 1	1	+
2, 1, 1, 1	10	−
2, 2, 1	15	+
3, 1, 1	20	+
3, 2	20	−
4, 1	30	−
5	24	+

Thus we know the sizes of the conjugacy classes in S_5 . The same method works in general for S_n .

We want to think about the conjugacy classes of A_n .

§1.3.1 Conjugacy Classes & Simplicity of A_n

One way to think about conjugacy classes is to say that the group acts on itself by conjugation. Then the conjugacy classes correspond to orbits and centralizers correspond to stabilisers.

So it’s going to be useful to think about the centralisers of elements in A_n . Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. We have then got two cases.

- If there exists an odd permutation commuting with g , then $|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)|$, and $|\text{ccl}_{A_n}(g)| = |\text{ccl}_{S_n}(g)|$.
- Otherwise, $|C_{A_n}(g)| = |C_{S_n}(g)|$ and $|\text{ccl}_{A_n}(g)| = \frac{1}{2}|\text{ccl}_{S_n}(g)|$.

Example 1.3.2 (Conjugacy Classes in A_5)

We can now investigate the conjugacy classes in A_5 . Note that $(1\ 2)(3\ 4)$ commutes with the odd permutation $(1\ 2)$ and $(1\ 2\ 3)$ commutes with $(4\ 5)$. But if $h \in C_{S_5}(g)$ where $g = (1\ 2\ 3\ 4\ 5)$, then

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

Thus $h \in \langle g \rangle$, and $|\text{ccl}_{A_5}(g)| = \frac{1}{2}|\text{ccl}_{S_5}(g)| = 12$. Thus A_5 has conjugacy classes of size 1, 15, 20, 12, 12. By the same argument as before, this implies that A_5 is simple.

Lemma 1.3.3 (Generators of A_n)

A_n is generated by 3-cycles.

Proof. We know that each $\sigma \in A_n$ is the product of an even number of transpositions. So it suffices to write the product of any two transpositions as the product of 3-cycles.

For a, b, c, d distinct, we have $(a\ b)(b\ c) = (a\ b\ c)$, and $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$. \square

Lemma 1.3.4 (3-Cycles are Conjugate in A_n)

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

Proof. We claim that every 3-cycle is conjugate to $(1\ 2\ 3)$. Indeed, if $(a\ b\ c)$ is a 3-cycle, then $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \notin A_n$, then replace σ with $\sigma(4\ 5)$. \square

Theorem 1.3.5 (A_n is Simple)

The alternating group A_n is simple for all $n \geq 5$.

Proof. Let $N \trianglelefteq A_n$ be a non-trivial subgroup of A_n . It suffices to show that N contains a 3-cycle.

We take some $\sigma \in N$ with $\sigma \neq e$, and write σ as the product of disjoint cycles.

- *Case 1.* σ contains a cycle of length $r \geq 4$.

Without loss of generality, let $\sigma = (1\ 2\ 3 \cdots r)\tau$. Let $\delta = (1\ 2\ 3)$, then $\delta^{-1}\sigma\delta \in N$, and $\sigma^{-1}\delta^{-1}\sigma\delta \in N$. This can be written $(r \cdots 2\ 1)(1\ 3\ 2)(1\ 2 \cdots r)(1\ 2\ 3) = (2\ 3\ r)$, which is a three cycle. Then N contains a three cycle.

- *Case 2.* σ contains two 3-cycles.

Again, without loss of generality say $\sigma = (1\ 2\ 3)(4\ 5\ 6)\tau$. Then let $\delta = (1\ 2\ 4)$, and $\sigma^{-1}\delta^{-1}\sigma\delta = (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 2\ 3)(4\ 6\ 5)(1\ 2\ 3) = (1\ 2\ 4\ 3\ 6)$. Then we can apply case 1, and N contains a three cycle.

- *Case 3.* σ contains two 2-cycles.

Without loss of generality, say $\sigma = (1\ 2)(3\ 4)\tau$. Then let $\delta = (1\ 2\ 3)$. Then $\sigma^{-1}\delta^{-1}\sigma\delta = (1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3)$. Calling this π , and letting $\epsilon = (2\ 3\ 5)$, then $\pi^{-1}\epsilon^{-1}\pi\epsilon = (1\ 4)(2\ 3)(2\ 5\ 3)(1\ 4)(2\ 3)(2\ 3\ 5) = (2\ 5\ 3)$, so N contains a 3-cycle. Note that we use $n \geq 5$ here.

It remains to consider σ where it is a three-cycle. But then N contains a 3-cycle. \square

Definition 1.3.6 (Automorphism)

An **automorphism** of a group G is an isomorphism $G \rightarrow G$.

The automorphisms of a group form a subgroup $\text{Aut}(G) \leq \text{Sym}(G)$.

§1.4 p -Groups and p -Subgroups

Throughout this section, p will denote a fixed prime number.

Definition 1.4.1 (p -group)

A finite group G is a p -group if $|G| = p^n$ for $n \in \mathbb{N}$ where p is a prime.

§1.4.1 Basic Properties of p -Groups

We will now state some basic properties of p -groups that will be used in the following sections.

Theorem 1.4.2 (p -groups Have Non-trivial Centers)

If G is a p -group, then $Z(G) \neq \{e\}$.

Proof. For $g \in G$, we have $|\text{ccl}_G(g)| \cdot |C_G(g)| = |G| = p^n$. So each conjugacy class has size that is a power of p . Since G is a union of its conjugacy classes,

$$\begin{aligned} |G| &\equiv \#(\text{conj. classes of size 1}) \pmod{p} \\ \implies 0 &\equiv |Z(G)| \pmod{p}. \end{aligned}$$

In particular, $|Z(G)| > 1$. □

Corollary 1.4.3 (Simple p -groups)

The only simple p -group is C_p .

Proof. Let G be a simple p -group. Since $Z(G) \leq G$, we have either $Z(G) = \{e\}$ or $Z(G) = G$. The center cannot be trivial by the previous theorem, thus $Z(G) = G$, and the only abelian simple groups are C_p . □

Corollary 1.4.4

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

Proof. We know that any finite group G has a composition series $\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{m-1} \triangleleft G_m = G$, with each quotient G_i/G_{i-1} simple. Then G is a p -group implies G_i/G_{i-1} is a p -group, and thus $G_i/G_{i-1} \cong C_p$. Then $|G_i| = p^i$ for all $0 \leq i \leq m$, and $m = n$. □

Lemma 1.4.5

For G a group, if $G/Z(G)$ is cyclic, then G is abelian, and $G/Z(G)$ is trivial.

Proof. Let $gZ(G)$ be a generator for $G/Z(G)$. Then each coset is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$. Thus $G = \{g^r z \mid r \in \mathbb{Z}, z \in Z(G)\}$. Then $(g^{r_1} z_1)(g^{r_2} z_2) =$

$g^{r_1+r_2}z_1z_2$ since z_1 is in the center. We can also write this as $g^{r_1+r_2}z_2z_1 = (g^{r_2}z_2)(g^{r_1}z_1)$, since z_2 is also in the center. Thus G is abelian. \square

We can now start to consider what various p -groups actually look like. We know that a group of order p is cyclic, so we will begin with groups of order p^2 .

Corollary 1.4.6 (Groups of Order p^2)

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

Proof. The center of G is non-trivial, and by thus by Lagrange, $|Z(G)|$ is either p or p^2 . If the order was p^2 , then we would be done. So consider the case $|Z(G)| = p$. Then $|G/Z(G)|$ must have order p , but then it is cyclic and contradicts our previous lemma. \square

We will leave considering groups of order p^3 as an exercise.

§1.4.2 Sylow Theorems

Let G be a finite group, and write $|G| = p^a m$ where p is a prime with $p \nmid m$.

Theorem 1.4.7 (First Sylow Theorem)

The set $\text{Syl}_p(G) = \{P \leq G \mid |P| = p^a\}$ of **Sylow p -subgroups** is non-empty.

Proof. We wish to show that G has a subgroup of order p^a . Let Ω be the set of all subsets of G of size p^a . We have

$$|\Omega| = \binom{p^a m}{p^a} = \frac{p^a m}{p^2} \cdot \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 1}{1}.$$

For $0 \leq k < p^a$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same power of p . Thus $|\Omega|$ is coprime to p .

Let G act on Ω by left multiplication, where for $g \in G$ and $X \in \Omega$, we put $g * X = \{gx \mid x \in X\} \in \Omega$. For any $X \in \Omega$, we have $|\text{Stab}_G(X)| \cdot |\text{Orb}_G(X)| = |G| = p^a m$. But by the coprimality described above, we can pick X such that $|\text{Orb}_G(X)|$ is coprime to p . Therefore $p^a \mid |\text{Stab}_G(X)|$.

On the other hand, if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$. Therefore $G = \bigcup_{g \in G} g * X$. Thus $|G| \leq |\text{Orb}_G(X)| \cdot |X|$, and thus $|\text{Stab}_G(X)| = \frac{|G|}{|\text{Orb}_G(X)|} \leq |X| = p^a$. So $|\text{Stab}_G(X)| = p^a$, and is thus a Sylow p -subgroup. \square

Theorem 1.4.8 (Second Sylow Theorem)

All elements of $\text{Syl}_p(G)$ are conjugate.

Proof. We claim that if $P \in \text{Syl}_p(G)$ and $Q \leq G$ is a p -subgroup then $Q \leq gPg^{-1}$ for some $g \in G$.

Let Q act on the set of left cosets of G by left multiplication, where $q * gP = qgP$. The orbit stabiliser theorem implies each orbit has size dividing $|Q|$, so it is either 1 or a multiple of p .

Since $|G : P| = m$ is coprime to p , there exists an orbit of size 1. Thus there exists $g \in G$ such that $qgP = gP$ for all $q \in Q$, and we get $g^{-1}qg \in P$, so $Q \subseteq gPg^{-1}$. \square

Theorem 1.4.9 (Third Sylow Theorem)

The number $n_p = |\text{Syl}_p(G)|$ of Sylow p -subgroups satisfies $n_p \equiv 1 \pmod{p}$, and $n_p \mid G$.

Proof. Let G act on $\text{Syl}_p(G)$ by conjugation. The second Sylow theorem implies that this action is transitive. So by the orbit stabiliser theorem, $n_p = |\text{Syl}_p(G)|$ divides $|G|$.

Now let $P \in \text{Syl}_p(G)$. P acts on $\text{Syl}_p(G)$ by conjugation. Then the orbits have size dividing $|P|$, so they are either 1 or a multiple of p .

To show $n_p \equiv 1 \pmod{p}$, it suffices to show that $\{P\}$ is the unique orbit of size 1. If $\{Q\}$ is an orbit of size 1, then P normalizes Q , so $P \leq N_G(Q)$. Now P and Q are Sylow p -subgroups of $N_G(Q)$. Hence by the second Sylow theorem, they are conjugate in $N_G(Q)$, and equal since $Q \trianglelefteq N_G(Q)$. Thus $\{P\}$ is the unique orbit of size 1. \square

Applications of the Sylow Theorems

We will now look at how the Sylow theorems can be use to prove some facts about certain groups.

Corollary 1.4.10

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

Proof. Let $g \in G$ and $P \in \text{Syl}_p(G)$. Then $gPg^{-1} \leq G$ is another Sylow p -subgroup, so we must have $gPg^{-1} = P$, for all $g \in G$. Then $P \trianglelefteq G$. \square

Example 1.4.11 (No Simple Groups of Order 1000)

Let $|G| = 1000 = 2^3 \cdot 5^3$. Then $n_5 \equiv 1 \pmod{5}$, and $n_5 \mid 8$. Checking, we find that $n_5 = 1$, and the unique Sylow 5-subgroup is normal. Then G is not simple.

Example 1.4.12 (No Simple Groups of Order 132)

Let $|G| = 132 = 2^2 \cdot 3 \cdot 11$. Then $n_{11} \equiv 1 \pmod{11}$, and $n_{11} \mid 12$. Then $n_{11} = 1$ or 12.

Suppose G was simple. Then $n_{11} \neq 1$, so $n_{11} = 12$. Now $n_3 \equiv 1 \pmod{3}$, and $n_3 \mid 44$, so $n_3 = 1, 4$ or 22. But G is simple, and either $n_3 = 4$ or 22. Supposing $n_3 = 4$, then letting G act on $\text{Syl}_3(G)$ by conjugation, we get a group homomorphism $\phi : G \rightarrow S_4$. Then $\ker(\phi) \trianglelefteq G$ implies $\ker(\phi) = \{e\}$ or G . It cannot be G by the

second Sylow theorem, thus ϕ is injective. But then $G \hookrightarrow S_4$, and $132 \leq 24$, which is a contradiction.

Thus $n_3 = 22$, and $n_1 = 12$. But then counting the G has $22 \cdot (3-1) = 44$ elements of order 3, and $12 \cdot (11-1) = 120$ elements of order 11. But then $120 + 44 = 164 > 132$, which is a contradiction. Thus there does not exist a simple group of order 132.

§1.5 Some Groups

We are going to finish the section on groups by looking at some Matrix groups, along with some finitely generated abelian groups.

§1.5.1 Matrix Groups

Let F be a field (for example \mathbb{C} or $\mathbb{Z}/p\mathbb{Z}$). Recall the groups $\mathrm{GL}_n(F)$ of $n \times n$ invertible matrices over F , and $\mathrm{SL}_n(F) = \ker(\mathrm{GL}_n \xrightarrow{\det} F^\times) \trianglelefteq \mathrm{GL}_n(F)$. Also let $Z \trianglelefteq \mathrm{GL}_n(F)$ be the group of scalar matrices (scalar multiples of the identity matrices).

We define the *projective general/special linear groups* as follows.

Definition 1.5.1 (Projective General Linear Group)

The **projective general linear group** $\mathrm{PGL}_n(F)$ is defined to be $\mathrm{GL}_n(F)/Z$.

Definition 1.5.2 (Projective Special Linear Group)

The **projective special linear group** $\mathrm{PSL}_n(F)$ is the group $\mathrm{SL}_n(F)/(Z \cap \mathrm{SL}_n(F))$, which is isomorphic to $Z \cdot \mathrm{SL}_n(F)/Z$, by the second isomorphism theorem.

Example 1.5.3

Let $G = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. A list of n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ are the columns of some $A \in G$ if and only if they are linearly independent. Thus

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

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

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

Indeed there are $\binom{n}{2}$ entries $*$, each which can take p values, so the order is $p^{\binom{n}{2}}$.

Just as $\mathrm{PGL}_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ via Möbius maps, $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. Indeed, $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ acts as

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

and since scalar matrices act trivially, this is an action of $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 1.5.4

The permutation representation of $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \rightarrow S_{p+1}$ is injective (and is an isomorphism if $p = 2$ or 3).

Proof. Suppose $\frac{az+b}{cz+d} = z$ for all $z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. Putting $z = 0$ shows $b = 0$. Putting $z = \infty$ shows $c = 0$. Putting $z = 1$ shows $a = d$, and thus this is a scalar matrix. \square

Lemma 1.5.5

If p is an odd prime, then $|\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})| = \frac{p(p-1)(p+1)}{2}$.

Proof. By the previous example, $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = p(p-1)(p^2-1)$. Then consider the group homomorphism $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p\mathbb{Z})^\times$. This is surjective, since we have

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mapsto a,$$

so $|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|}{p-1} = p(p-1)(p+1)$.

Then counting the number of scalar matrices, if

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}),$$

then $\lambda^2 \equiv 1 \pmod{p}$ implies $p \mid (\lambda-1)(\lambda+1)$, so $\lambda \equiv \pm 1 \pmod{p}$. So there are two such scalar matrices, and $|\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})| = \frac{1}{2} |\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| = \frac{p(p-1)(p+1)}{2}$. \square

Example 1.5.6

Let $G = \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$. Then $|G| = 60 = 2^2 \cdot 3 \cdot 5$.

Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ via Möbius maps. By our previous lemma, there is an injective group homomorphism $\phi : G \rightarrow \mathrm{Sym}(\{0, 1, \dots, 4, \infty\}) \cong S_6$.

Claim. $\mathrm{img}(\phi) \leq A_6$, that is, $\psi : G \rightarrow S_6 \xrightarrow{\mathrm{sgn}} \{\pm 1\}$ is trivial.

If m is odd, then $\psi(g) = e \iff \psi(g)^m = e \iff \psi(g^m) = e$. So it suffices to consider $g \in G$ with order a power of 2. We showed in the proof of the Sylow theorems that every such element belongs to a Sylow 2-subgroup. So it suffices to check that $\psi(H) = e$, where H is a Sylow 2-subgroup (using that we have any two Sylow 2-subgroups are conjugate, and ψ maps to an abelian group).

We take $H = \left\{ \pm \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \leq G$. We compute:

$$\begin{aligned} \phi \left(\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \right) &= (1 \ 4)(2 \ 3) \\ \phi \left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right) &= (0\infty)(1 \ 4). \end{aligned}$$

These are even permutations, so $\psi(H)$ is trivial, and our claim is true.

§1.5.2 Finite Abelian Groups

Later in this course, we will prove the following theorem.

Theorem 1.5.7 (The Fundamental Theorem of Finite Abelian Groups)

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

Remark (Non-Uniqueness). While this is possible, such a decomposition is not unique. For example, you may recall from IA groups that if m and n are coprime, then $C_m \times C_n \cong C_{mn}$.

Lemma 1.5.8

If m and n are coprime, then $C_{mn} = C_m \times C_n$.

Proof. Let g and h be generators of C_m and C_n . Then we have $(g, h) \in C_m \times C_n$, and $(g, h)^r = (g^r, h^r)$. In particular, $(g, h)^r = e$ if and only if $m \mid r$ and $n \mid r$, that is, if $mn \mid r$ since they are coprime. Thus (g, h) has order mn , which is $|C_m \times C_n|$. \square

Corollary 1.5.9

Let G be a finite abelian group. Then $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ where each n_i is a prime power.

Proof. If $n = p_1^{a_1} \cdots p_r^{a_r}$, with p_i prime, then we can (by the previous lemma) write $C_n \cong C_{p_1^{a_1}} \times \cdots \times C_{p_r^{a_r}}$. Writing each of the cyclic groups in the fundamental theorem of abelian groups then gives the result. \square

In fact, we will prove the following refinement of the the fundamental theorem of finite abelian groups.

Theorem 1.5.10

Let G be a finite abelian group. Then

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

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

Remark. The integers n_1, \dots, n_k in the previous corollary and d_1, \dots, d_t in the previous theorem are uniquely determined by G . The proof (which we omit) works by counting the number of elements of each prime power order.

Example 1.5.11 (Abelian Groups of Order 8)

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

Example 1.5.12 (Abelian Groups of Order 12)

The abelian groups of order 12 are $C_2 \times C_6 \cong C_2 \times C_2 \times C_3$, $C_4 \times C_3 \cong C_{12}$.

Definition 1.5.13 (Exponent)

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

Example 1.5.14

A_4 has exponent 6.

Corollary 1.5.15

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

Proof. If $G \cong C_{d_1} \times \dots \times C_{d_t}$ with $d_1 \mid d_2 \mid \dots \mid d_t$, then every $g \in G$ has order dividing d_t , and if $h \in C_{d_t}$ is a generator, then $(1, 1, 1, \dots, h) \in G$ has order d_t . So G has exponent d_t . \square

2 Rings

§2.1 Rings

We will now move on to another central algebraic object in this course – *rings*.

§2.1.1 Definitions

Let's start with a definition.

Definition 2.1.1 (Ring)

A **ring** is a triple $(R, +, \cdot)$ consisting of a set R and two binary operations^a $+, \cdot : R \times R \rightarrow R$, referred to as *addition* and *multiplication*, that satisfy

- $(R, +)$ is an abelian group, with identity 0.
- Multiplication is associative and has an identity 1.
- *Distributivity*. For $x, y, z \in R$, we have $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$.

^aAgain this has an implicit *closure* axiom

Remark (Notation). For $x \in R$, we write $-x$ for its inverse under addition, and we abbreviate $x + (-y) = x - y$.

We note that in the definition we require $(R, +)$ to be an abelian group, but the fact that it is abelian is deducible from the other axioms. This means that if we talk about a ring being commutative, we must be referring to the multiplication.

Definition 2.1.2 (Commutative Ring)

A ring R is **commutative** if $x \cdot y = y \cdot x$ for all $x, y \in R$.

In this course, we will *only consider* commutative rings. So whenever we refer to an arbitrary ring, we will be referring to a commutative ring.¹

We can define subrings in the natural way.

Definition 2.1.3 (Subrings)

A subset $S \subset R$ is a **subring**, written $S \leq R$, if it is a ring under the same operations $+$ and \cdot , with the same identity elements 0 and 1.

Example 2.1.4 (Examples of Rings and Subrings)

The following are examples of rings and subrings.

¹There are some notable non-commutative rings such as ones made up of matrices, but they will not be considered in this course.

- (i) We have the subrings $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, under addition and multiplication as normal.
- (ii) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a ring, and $\mathbb{Z}[i] \leq \mathbb{C}$.
- (iii) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \leq \mathbb{R}$.
- (iv) $\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{m}{p^n} \mid m \in \mathbb{Z}, n \geq 0\right\} \leq \mathbb{Q}$.
- (v) $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n , is a ring of order n .

§2.1.2 Constructing Rings

Similar to the direct product of groups, there is a natural way to combine rings.

Definition 2.1.5 (Product Ring)

If R and S are rings, then their **product ring** $R \times S$ is a ring via $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$.

We have $0_{R \times S} = (0_R, 0_S)$ and $1_{R \times S} = (1_R, 1_S)$.

Remark. Note that $R \times \{0\}$ is *not* a subring of $R \times S$ – this doesn't have the same identity elements.

There are some other interesting ways to construct rings from other rings. First of all, we could consider functions from some set onto R .

Definition 2.1.6

If R is a ring and X is a set, then the set of all functions $X \rightarrow R$ is a ring under pointwise operations, $(f + g)(x) = f(x) + g(x)$, and $(f \cdot g)(x) = f(x) \cdot g(x)$.

Other interesting examples appear as subrings. For example, the continuous functions $\mathbb{R} \rightarrow \mathbb{R}$.

We can also construct the *ring of polynomials*

Definition 2.1.7 (Ring of Polynomials)

Let R be a ring and define S to be the set of all sequences (a_0, a_1, \dots) with $a_i \in R$ with $a_i = 0$ for all $i \geq N$ for some N . Then defining addition and multiplication as

$$\begin{aligned} (a_0, a_1, \dots) + (b_0, b_1, \dots) &= (a_0 + b_0, a_1 + b_1, \dots) \\ (a_0, a_1, \dots) \cdot (b_0, b_1, \dots) &= (c_0, c_1, \dots), \end{aligned}$$

where $c_n = \sum_{i=0}^n a_i b_{n-i}$ gives us $R[X]$, the **ring of polynomials in X with coefficients in R** .

Note that if we define $X = (0, 1, 0, \dots)$, then $X^n = (\underbrace{0, 0, \dots, 0}_{n \text{ times}}, 1, 0, \dots)$, and

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

This is why this is known as the polynomial ring.

You may wonder why we defined things in this way, and the answer is that we are not thinking about polynomials as functions, but as sequences of coefficients. To see why this matters, consider $R = \mathbb{Z}/p\mathbb{Z}$ with p prime and $f(x) = X^p - X$. Then the function $x \mapsto f(x)$ is identically zero, but the polynomial $X^p - X$ is non-zero.

So we can restate our definition in a clearer and more general way.

Definition 2.1.8 (Ring of Polynomials)

If R is a ring then $R[X_1, \dots, X_n]$ is the *ring of polynomials* in X_1, \dots, X_n with coefficients in R .

Remark. We can define this inductively as $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$ using our careful construction for $R[X]$ above.

Some extensions of this are the following rings.

Definition 2.1.9 (Power Series and Laurent Polynomials)

The **power series ring** is the ring $R[[X]] = \{a_0 + a_1X + a_2X^2 + \dots \mid a_i \in R\}$ and the **ring of Laurent polynomials** is $R[X, X^{-1}] = \{\sum_{i \in \mathbb{Z}} a_i X^i \mid a_i \in R, \text{ and only finitely many } a_i \neq 0\}$.

§2.1.3 Units and Fields

We now introduce an important definition. Recall that not every element ring necessarily has an inverse under multiplication. When an element *does* have one, we call it a *unit*.

Definition 2.1.10 (Unit)

An element $r \in R$ is a **unit** if it has an inverse under multiplication. That is, if there exists $s \in R$ such that $r \cdot s = 1$.

The units in a ring R form a group (R^\times, \cdot) under multiplication. For example, $\mathbb{Z}^\times = \{\pm 1\}$, and $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

When every non-zero element in a ring is a unit, we call that ring a *field*.

Definition 2.1.11 (Field)

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

Examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

Remark. Note that we require $0 \neq 1$ in the definition of a field. If we did not have this, then if $0 = 1$, $x = 1 \cdot x = 0 \cdot x = 0$, for all $x \in R$. So if a ring has $0 = 1$, then it is the trivial ring $R = \{0\}$. And we don't want this to be a field.

The notion of a ring allows us to do some interesting things.

Lemma 2.1.12 (Polynomial Division Algorithm)

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

Proof. We induct on the degree of f . If the degree is n , then we write $f(X) = a_n X^n + \cdots + a_1 X + a_0$ with $a_n \neq 0$, and $g(X) = b_m X^m + \cdots + b_1 X + b_0$, where $b_m \in R^\times$.

If $n < m$, put $q = 0$ and $r = f$, and we are done. Otherwise, we put $f_1(X) = f(X) - a_n b_m^{-1} X^{n-m} g(X)$. Then the coefficient of X^n is 0, and $\deg(f_1) < n$, and we apply the induction hypothesis to get $f_1(X) = q_1(X)g(X) + r(X)$, with $\deg(r) < \deg(g)$.

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

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