PATRICK ORSON

GROUPS AND RINGS

ABSTRACT ALGEBRA I

Contents

Introduction

These are the class notes for the one-semester course Abstract Algebra I. They are a work in progress, subject to editing and improvement. I welcome your corrections and comments.

Most of the results stated here are given without proof in the notes. During the course, we will prove some of the results in the classroom, while other results will be set for you to prove during homework.

I hope you enjoy the course!

1 Groups

Groups – definitions

Here is the formal definition of a group, which must be memorised in order to write rigorous arguments. But to really understand groups one must build the intuition for them via the concept of symmetry.

Definition 1.1. A *binary operation* $\cdot$ on a set X is a function

$$\cdot : X \times X \to X; \qquad (x, y) \mapsto x \cdot y.$$

Our binary operation notation "$\cdot$" resembles multiplication, but is meant to be an all-purpose stand-in that could represent familiar operations you have seen before, for example: $+$, $\times$, $\circ$, ...

Definition 1.2. A *group* is a triple $(G, \cdot, e)$, consisting of a set G, a binary operation $\cdot$ and an element $e \in G$ such that

(i) For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. ASSOCIATIVITY

(ii) For all $a \in G$, we have $a \cdot e = a$. IDENTITY

(iii) For all $a \in G$, there exists $b \in G$ such that $a \cdot b = e$. INVERSE

WARNING! Some authors include "CLOSURE" as an axiom of a group. This means $a \cdot b \in G$ for all $a, b \in G$. This is redundant because our definition of binary operation includes this concept. BUT when you are checking you have a group, you need to check your proposed binary operation really does produce a new element in your set. See Example 1.12 for an example of this problem.

The IDENTITY and INVERSE axioms are surprisingly powerful and can be used to generate several important results that one would intuitively expect.

Proposition 1.3. *Let $(G, \cdot, e)$ be a group.*

(i) ELEMENTS COMMUTE WITH THEIR INVERSE
If $a, b \in G$ are such that $a \cdot b = e$ then $b \cdot a = e$.

(ii) RIGHT IDENTITIES ARE ALSO LEFT IDENTITIES
If $a \in G$ then $e \cdot a = a$.

(iii) INVERSES ARE UNIQUE
If $a, b, b' \in G$ are such that $a \cdot b = e$ and $a \cdot b' = e$ then $b = b'$.

(iv) IDENTITIES ARE UNIQUE
If $e' \in G$ is such that $a \cdot e' = a$ for some $a \in G$, then $e' = e$.

If we have a set with a binary operation $(G, \cdot)$ satisfying ASSOCIATIVITY, and assume an identity element $e \in G$ *exists*, then we now know it is unique. So in fact it is redundant to include e in the notation $(G, \cdot, e)$. However, we will continue to do so, for clarity.

Because inverses are unique, we can now assign them a notation.

Definition 1.4. Given $(G, \cdot, e)$ and $a \in G$, write $a^{-1} \in G$ for the unique element such that $a \cdot a^{-1} = e$, and call this *the inverse of a*.

Notation 1.5. Given $n \in \mathbb{Z}^{\geq 1}$, write

$$a^n := \underbrace{a \cdot \ldots \cdot a}_{n} \qquad a^{-n} := (a^{-1})^n \qquad a^0 := e.$$

Exercise 1.1. Given $(G, \cdot, e)$, $a \in G$, and $n, m \in \mathbb{Z}$, show that

$$a^n \cdot a^m = a^{n+m} \qquad \text{and} \qquad (a^n)^m = a^{nm}.$$

You will have seen examples of non-commutative binary operations before, for example multiplication of square matrices. When the binary operation does commute we give the group a special name.

Definition 1.6. A group $(G, \cdot, e)$ is called *abelian* if the binary operation is commutative, that is, if $a \cdot b = b \cdot a$ for all $a, b \in G$.

Definition 1.7. A group $(G, \cdot, e)$ is *finite* if the set G is a finite set. We call the number of elements $|G|$ of a finite group the *order* of the group.

Figure 1.1: Niels Abel (1802-1829). Algebraist, most famous for proving there is no formula for solving a general degree 5 polynomial equation in terms of radicals. He lends his name to this important condition on a group, and also one of the most prestigious prizes in mathematics: the Abel Prize.

Groups – examples

We give some basic examples of groups and non-groups.

Example 1.8. The *trivial group* is $(\{e\}, \cdot, e)$, consisting of the single $\{e\}$, with the operation $e \cdot e = e$, and identity e.

Example 1.9. $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ are all abelian groups.

Example 1.10. $(\mathbb{Z}^{\geq 0}, +, 0)$ is not a group because it does not satisfy the INVERSE axiom. For example, there is no $n \in \mathbb{Z}^{\geq 0}$ such that $1 + n = 0$.

Example 1.11. $(\mathbb{Z}, -, 0)$ is not a group because it does not satisfy the ASSOCIATIVE axiom. For example, $(1 - 1) - 1 = -1 \neq 1 - (1 - 1)$.

Example 1.12. Let G be the set of integers that are perfect cubes. Then $(G, +, 0)$ is not a group. In fact "associativity", "identity" and "inverse" are all satisfied, but $+$ combines elements of G to produce elements outside of G, e.g. $1^3 + 1^3 = 2 \notin G$. So $+$ is not actually a binary operation on this set. We say "G is not closed under $+$".

Example 1.13. $(\mathbb{Q} \setminus \{0\}, \times, 1)$, $(\mathbb{R} \setminus \{0\}, \times, 1)$, $(\mathbb{C} \setminus \{0\}, \times, 1)$ are abelian groups.

Example 1.14. $(\mathbb{Q}^{>0}, \times, 1)$, $(\mathbb{R}^{>0}, \times, 1)$ are abelian groups.

Example 1.15. $(\mathbb{Z}, \times, 1)$ is not a group because it does not satisfy the INVERSE axiom. For example, there is no $n \in \mathbb{Z}$ such that $2 \times n = 1$.

Example 1.16. $(\mathbb{Q}, \times, 1)$ is not a group because it does not satisfy the INVERSE axiom. There is no $q \in \mathbb{Q}$ such that $0 \times q = 1$.

Example 1.17. Write $S^1 := \{z \in \mathbb{C} \mid |z| = 1\} \subseteq \mathbb{C}$. Then $(S^1, \times, 1)$ is an abelian group.

Example 1.18. Let $n \in \mathbb{Z}^{>0}$. Then

$$C_n := (\{z \in \mathbb{C} \mid z^n = 1\}, \times, 1\})$$

is a finite abelian group. The order of the group is n as this is the number of nth roots of unity. For example

$$\begin{aligned} C_1 &= \{1\} \\ C_2 &= \{1, -1\} \\ C_3 &= \{1, \tfrac{1}{2}(-1 + i\sqrt{3}), \tfrac{1}{2}(-1 - i\sqrt{3})\} \\ C_4 &= \{1, i, -1, -i\} \end{aligned}$$

Example 1.19. Let $n \in \mathbb{Z}^{>0}$. Let $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. Define a binary operation by setting $a +_n b$ to be the remainder when $a + b$ is divided by n. Then $(\mathbb{Z}_n, +, 0)$ is a finite abelian group. The order of the group is n.

Example 1.20. The *Klein* 4*-group* (Kleinviergruppe) is the group $V := (\{e, a, b, c\}, \cdot, e)$ with the binary operation defined by the multiplication table

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The group is finite of order 4. The multiplication table is symmetric about the diagonal, meaning the group is abelian. An interesting feature: the e's on the diagonal show that $x \cdot x = e$ for every element x of the group, which is not true of C_4 or $\mathbb{Z}_4$, the other order 4 groups we introduced. So this one is fundamentally different!

Figure 1.2: Felix Klein (1949-1925). Prolific mathematician, who's *Erlangen Program* synthesised geometry, complex analysis and group theory to classify geometric spaces by their symmetries.

All the examples of groups we have given above are abelian. However, most groups are not abelian. Here are some examples of non-abelian groups.

Example 1.21. Let $\mathrm{GL}_2(\mathbb{R})$ be the set of all invertible 2×2 matrices with real entries. Then $(\mathrm{GL}_2(\mathbb{R}), \times, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$ is a non-abelian group.

Of course, $(\mathrm{GL}_2(\mathbb{R}), +, \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right))$ is also a group. In contrast, it is abelian. Indeed the set $\mathrm{Mat}_n(\mathbb{R})$ of all $n \times n$ matrices is an abelian group under addition $(\mathrm{Mat}_n(\mathbb{R}), +, 0\text{-matrix})$.

Example 1.22. A function $f \colon \mathbb{R} \to \mathbb{R}$ is an *isometry* if it is length-preserving, that is, if $|x - y| = |f(x) - f(y)|$ for all $x, y \in \mathbb{R}$. Let $\mathrm{Isom}(\mathbb{R})$ be the set of isometries. Then $(\mathrm{Isom}(\mathbb{R}), \circ, \mathrm{Id})$ is a group.

It is not abelian. For example, $r(x) := -x$ and $t(x) := x + 1$ are isometries, but

$$(t \circ r)(x) = t(r(x)) = -x + 1 \neq -x - 1 = r(t(x)) = (r \circ t)(x).$$

Subgroups

Definition 1.23. We say a group $(H, \cdot_H, e_H)$ is a *subgroup* of $(G, \cdot_G, e_G)$, and use the notation $(H, \cdot_H, e_H) \leq (G, \cdot_G, e_G)$, if

(i) H is a subset of G

(ii) $e_H = e_G$

(iii) For all $a, b \in H$, we have $a \cdot_G b = a \cdot_H b$.

In other words, H is a subset of G and has the same group operation and identity element as G. This can be used as a way of generating subgroups.

Proposition 1.24. *Given a group $(G, \cdot_G, e_G)$ and a subset $H \subseteq G$, if $a \cdot_G b \in H$ for all $a, b \in H$ then there is a unique group structure $(H, \cdot_H, e_H)$ on H such that $(H, \cdot_H, e_H)$ is a subgroup of $(G, \cdot_G, e_G)$.*

In other words, if you can check a subset is closed under the binary operation, it is a subgroup in a unique way. The unique way is "use the identity and binary operation from G".

Here are some examples of subgroups and non-subgroups.

Example 1.25. For any group $(G, \cdot, e)$, we always have the subgroups

- $(G, \cdot, e) \leq (G, \cdot, e)$ and
- $(\{e\}, \cdot, e) \leq (G, \cdot, e)$.

These are called the *improper subgroups*. Any other subgroup is called a *proper* subgroup.

Example 1.26. $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0)$

Example 1.27. $(\mathbb{Q}^{>0}, \times, 1)$ is a subgroup of $(\mathbb{Q} \setminus \{0\}, \times, 1)$ because $\mathbb{Q}^{>0} \subseteq \mathbb{Q} \setminus \{0\}$ and the multiplications and identities agree.

Example 1.28. Suppose $n, m \in \mathbb{Z}^{\geq 0}$ and n divides m. Then we claim we have a subgroup $C_n \leq C_m$ (recall Example 1.18). To see this, we just need to show the subset condition. We have that $m = nq$ for some $q \in \mathbb{Z}^{\geq 0}$. Then if $z \in \mathbb{C}$ is such that $z^n = 1$, we have $z^m = (z^n)^q = 1^q$. This shows nth roots of unity are also mth roots of unity.

Example 1.29. Let $\mathrm{SL}_2(\mathbb{R})$ be the set of all 2×2 matrices with real entries and determinant 1. As $\det(AB) = \det(A)\det(B)$, the product of any two such matrices also has determinant 1. Hence

$$(\mathrm{SL}_2(\mathbb{R}), \times, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) \leq (\mathrm{GL}_2(\mathbb{R}), \times, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)).$$

Notation 1.30. Let $n \in \mathbb{Z}$ then $n\mathbb{Z} := \{kn \in \mathbb{Z} \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$, the set of all multiples of the number n.

Proposition 1.31. *The subgroups of $(\mathbb{Z}, +, 0)$ are exactly the subsets determined by $n\mathbb{Z} \subseteq \mathbb{Z}$ for all $n \in \mathbb{Z}$.*

CONVENTION

From now on we will stop specifying the full triple $(G, \cdot, e)$ unless it is not clear from context which identity and group operation we are using.

The group $(G, \cdot, e)$ will be simply written "G".

Example. We will simply write $\mathbb{Z}$ to indicate the integers together with addition and the identity element 0.

Symmetries of geometric objects

The word "symmetry" is used fairly broadly in mathematics and we want to give a general definition. We then move on to specify the sort of symmetry we mean when we are talking about reflections/rotations of polygons and polyhedra.

Permutation groups

"Symmetry" should capture the idea of taking an object and moving it around so that afterwards you just have to same object back.

The terms "symmetry", "permutation", "bijection" and "invertible function" all mean the same thing and are used fairly interchangeably.

Definition 1.32. A *symmetry/permutation* of a set X is an invertible function

$$f \colon X \to X.$$

The *symmetry group/permutation group* of a set X is the set $\mathrm{Sym}(X)$ of all symmetries of the set X, where the group operation is composition and the identity element is the identity map.

Exercise 1.2. Verify that $(\mathrm{Sym}(X), \circ, \mathrm{Id}_X)$ is indeed a group.

The most common symmetry group to study in this generality is the following. We will study this in great detail later in the course.

Definition 1.33. For $n \in \mathbb{Z}^{\geq 1}$, the *symmetric group on n letters* is $S_n := \mathrm{Sym}(X)$ where $X = \{1, 2, 3, \ldots, n\}$. In other words

$$S_n := \{\sigma \mid \sigma \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \text{ is a bijection}\}.$$

Exercise 1.3. Show that S_n is a finite group of order $n!$.

Example 1.34. • $S_1 = \{\mathrm{Id}\}$, which is the trivial group.

- $S_2 = \{\mathrm{Id}, \sigma\}$ where σ is the permutation that switches 1 and 2.
- S_3 has $3! = 6$ elements. Let's show S_3 is generated by just 2 elements under composition. Here are the proposed elements.

  You should quickly scribble down the 6 permutations of $\{1,2,3\}$ to check you can do so.

  $$\varphi\colon \{1,2,3\} \to \{1,2,3\}; \qquad \varphi(1) = 2,\ \varphi(2) = 3,\ \varphi(3) = 1$$

  and

  $$\psi\colon \{1,2,3\} \to \{1,2,3\}; \qquad \psi(1) = 2,\ \psi(2) = 1,\ \psi(3) = 3.$$

  Exercise 1.4. Explicitly write out the permutations:

  $$\varphi^2, \qquad \varphi \circ \psi, \qquad \varphi^2 \circ \psi$$

  and hence show that

  $$S_3 = \{\ \mathrm{Id},\ \varphi,\ \varphi^2,\ \psi,\ \varphi \circ \psi,\ \varphi^2 \circ \psi\ \}$$

  because these are the six distinct permutations of $\{1,2,3\}$.

  Prove that $\psi \circ \varphi = \varphi^2 \circ \psi$.

Regular polygons

For now, let's loosely define a *geometric object* to be a subset $X \subseteq \mathbb{R}^n$ for some n. One might insist that "symmetry" should preserve more than just the set X, but should also preserve the nice geometric features of X. This is captured by the following.

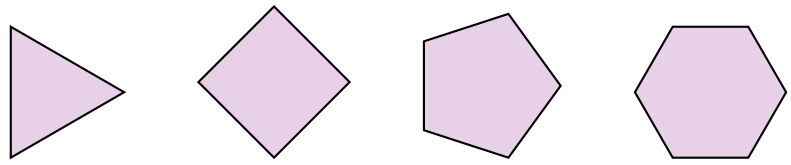
Definition 1.35. If $X \subseteq \mathbb{R}^n$ then a bijection $f\colon X \to X$ is called an *isometry* if it preserves the distance between any two points; precisely, if $||x - y|| = ||f(x) - f(y)||$ for all $x, y \in X$.

Exercise 1.5. The set $\mathrm{Isom}(X)$ of isometries of a subset $X \subseteq \mathbb{R}^n$ is a subgroup of $\mathrm{Sym}(X)$.

Let's define some "nice" geometric objects.

Definition 1.36. For $n \geq 0$, the *regular n-gon* is the polygon in $\mathbb{R}^2$ with vertices, located at $(x_k, y_k) = (\cos(k\theta), \sin(k\theta))$ for $k = 0, 1, \ldots, n-1$.

One could define the regular n-gon as "any polygon in $\mathbb{R}^2$ with n vertices and equal internal angles", but the subsequent discussion is easier if we just pick a specific one, as we do here.



Remark 1.37. Just to be clear, our convention is that the polygon (as a subset of $\mathbb{R}^2$) is not just the edge of the shape, but includes the region in the middle.

Definition 1.38. The *nth dihedral group* D_{2n} is the isometry group of the regular n-gon.

Theorem 1.39. *The dihedral group* D_{2n} *has* $2n$ *elements*

$$D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\},$$

where $e = \mathrm{Id}$, r *is the anti-clockwise rotation around the origin of* $\frac{2\pi}{n}$ *radians and* s *is reflection in the x-axis.*

This theorem explains the notation D_{2n}, but the notation is still a potential source of confusion, so stay sharp! For example, an equilateral triangle has 3 sides, but the isometry group is D_6.

Proposition 1.40. *The dihedral group* D_{2n} *is abelian for* $n = 1, 2$ *and non-abelian for* $n \geq 3$.

The proof of Theorem 1.39 shows that the "rules" $r^n = e$, $s^2 = e$ and $rs = sr^{-1}$ are enough to reduce any composition of r, s and r^{-1} to one of the $2n$ elements in the displayed set for D_{2n}. This suggests a very compact notation for describing some groups in which, or example,

$$D_{2n} = \langle r, s \,|\, r^n = e, s^2 = e, rs = sr^{-1} \rangle.$$

Observe that D_6 and S_3 each have 6 elements and each have the same generators and relations. So they are the "same" group. This is explained by the fact every permutation of the vertices of an equilateral triangle (which we could label 1, 2, and 3) can be achieved using isometries of the triangle. This is not true for any other n-gon, for example, there is no isometry of a square that leaves diagonally opposite vertices adjacent to each other afterwards.

The formal development of this notation is somewhat involved, so we will introduce it somewhat informally for now.

Notation 1.41. Suppose G is a finite group of order N and each element of G can be written as a composition of elements on a finite list $S = \{x_1, \ldots, x_m\}$, together with their inverses, and that a finite list of "rules" $r_1, \ldots, r_n$ is enough to reduce arbitrary compositions of S and the inverses to a preferred representative list of elements of G. Then we write

$$G = \langle x_1, \ldots, x_m \,|\, r_1, \ldots, r_n \rangle.$$

Example 1.42. The Klein 4-group is

$$V = \langle a, b \,|\, a^2 = e,\ b^2 = e,\ ab = ba \rangle.$$

Setting $c = ab$, we see the multiplication table is indeed satisfied. We need to check any combination of e, a, b, a^{-1}, b^{-1} can be reduced to e, a, b, or ab using the rules. First note $a^{-1} = a$ and $b^{-1} = b$. Here is an example of how to reduce:

$$aababbabbabba = aaaaaabbbbbbb = a^6b^6b = e^3e^3b = b.$$

This can be polished up to an algorithm, proving the reduction statement.

Platonic solids

There are exactly five regular convex polyhedra.

A "polyhedron" is a *solid*, meaning we are including the points inside as part of the set.

- The tetrahedron 24 isometries.

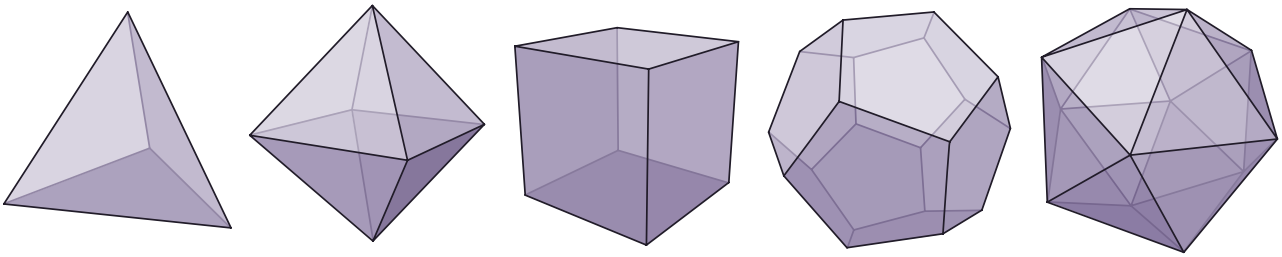


Figure 1.3: The five Platonic solids

- The octahedron 48 isometries.
- The cube 48 isometries.
- The dodecahedron 120 isometries.
- The icosohedron 120 isometries.

We will deduce these are indeed the number of isometries a little later in the course, when we have developed some more technology.

Homomorphisms

A key way to study groups is to study the functions between them that respect the group structures.

Definition 1.43. A function $\varphi\colon H \to G$ between groups is called a *homomorphism* if $\varphi(a \cdot_H b) = \varphi(a) \cdot_G \varphi(b)$ for all $a, b \in H$.

An invertible homomorphism $\varphi\colon H \to G$ is called an *isomorphism*. If there exists an isomorphism between H and G, we call these groups *isomorphic* and write $H \cong G$.

Example 1.44. The identity map $\mathrm{Id}_G\colon G \to G$ is always a homomorphism (indeed, an isomorphism).

Example 1.45. Given groups H and G, the function $\varphi\colon H \to G$ given by $\varphi(a) = e_G$ for all $a \in H$ is always a homomorphism, called the *trivial* homomorphism.

Example 1.46. If $H \leq G$ is a subgroup then the inclusion map $i\colon H \to G$, given by $i(a) = a$ for all $a \in H$, is a homomorphism.

Example 1.47. If n divides m, then $\varphi\colon C_m \to C_n$, given by $\varphi(z) = z^{m/n}$, is a homomorphism.

Example 1.48. The function $\exp\colon \mathbb{R} \to \mathbb{R}^{>0}$ given by $\exp(x) = e^x$ is a homomorphism from an additive group to a multiplicative group

$$\exp\colon (\mathbb{R}, +, 0) \to (\mathbb{R}^{>0}, \times, 1).$$

Example 1.49. Let V, W be a vector spaces (e.g. $V = \mathbb{R}^n$ and $W = \mathbb{R}^m$). These are groups using the binary operation of vector addition and identity is the 0-vector. Then a linear map $T\colon V \to W$ is in particular a group homomorphism.

Lemma 1.50. *Let $\varphi\colon H \to G$ be a homomorphism. Then*

(i) $\varphi(e_H) = e_G$ *and*

(ii) $\varphi(a)^{-1} = \varphi(a^{-1})$ *for all* $a \in H$.

Exercise 1.6. Confirm that the composition $\varphi \circ \psi\colon K \to G$ of two homomorphisms $\psi\colon K \to H$ and $\varphi\colon H \to G$ is a homomorphism.

Definition 1.51. Let $\varphi\colon H \to G$ be a homomorphism.

(i) The *image* of φ is

$$\mathrm{im}(\varphi) := \{g \in G \mid g = \varphi(h) \text{ for some } h \in H\} \subseteq G$$

(ii) The *kernel* of φ is

$$\ker(\varphi) := \{h \in H \mid \varphi(h) = e_G\} \subseteq H.$$

Proposition 1.52. *Let $\varphi\colon H \to G$ be a homomorphism. Then* $\mathrm{im}(\varphi) \leq G$ *and* $\ker(\varphi) \leq H$ *are subgroups.*

In principle, to detect a homomorphism is an isomorphism, we need to show it is both surjective and injective. The group structure provides us with a lovely shortcut for this.

You may recognise a version of this condition from a linear algebra course. Linear maps are additive group homomorphisms, so the linear algebra version is a special case of this.

Lemma 1.53. *A homomorphism $\varphi\colon H \to G$ is an isomorphism if and only if* $\mathrm{im}(\varphi) = G$ *and* $\ker(\varphi) = e_H$.

Cyclic groups

An example we have seen already is

$$C_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

This is a finite group. Writing $\xi = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ the group has elements

$$\begin{aligned} C_n &= \{1, \xi, \xi^2, \ldots, \xi^{n-1}\} \\ &= \langle \xi \mid \xi^n = 1 \rangle. \end{aligned}$$

We give a name to this type of group.

Definition 1.54. A group G is called *cyclic* if there exists $x \in G$ such that every element in G is equal to x^k for some $k \in \mathbb{Z}$. We call any such x a *generator* of G.

A cyclic group may have more than one generator. For example in $C_4 = \{1, i, -1, -i\}$, both i and $-i$ are generators.

Example 1.55. The groups C_n described above are cyclic, and any *primitive* nth root of unity is a generator, where primitive means $\xi = \cos\theta + \sin\theta$ for $\theta = \frac{2\pi k}{n}$, for k coprime to n.

Example 1.56. The groups $\mathbb{Z}_n$ from Example 1.19. Each number $x \in \{0, 1, \ldots, n-1\}$ is of the form $x = 1 + \cdots + 1 = kn$.

Example 1.57. The group $\mathbb{Z}$ is cyclic, with each $x\mathbb{Z}$ of the form $x = 1 + \cdots + 1 = kn$ or $x = (-1) + \cdots + (-1) = -kn$.

Theorem 1.58. *If a group G is cyclic, it is isomorphic to C_n for some $n > 0$ or to $\mathbb{Z}$.*

Definition 1.59. Let G be a group and let $g \in G$. The *order* of the element g is the least integer $k \in \mathbb{Z}^{>0}$ such that $g^k = e$ (provided one exists), and in this case write $\mathrm{ord}(g) = k$. If no such k exists, then we say g is of *infinite order* and write $\mathrm{ord}(g) = \infty$.

By definition, a subgroup generated by a single element is cyclic and the order of the subgroup is the order of the element. By Theorem 1.58 the subgroup generated by any element is isomorphic to one of C_n or $\mathbb{Z}$.

Definition 1.60. Given $g \in G$, we write

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} \subseteq G$$

and call this *the subgroup generated by g*.

2 *Quotient groups and the First Isomorphism Theorem*

To study any object in mathematics, we can try to break it into smaller objects and categorise the "atomic" or "building block" objects. There are many ways this can be made precise in group theory. We start this section with the idea of finding natural partitions of a group into subsets called "cosets". We then generalise the idea of modular arithmetic, by making precise when we can "quotient out" by a subgroup to pass to a smaller group, like passing from $\mathbb{Z}$ to $\mathbb{Z}_n$.

Cosets

Definition 2.1. Let $H \leq G$ be a subgroup. A *left coset of H in G* is

$$gH := \{a \in G \mid a = g \cdot h \text{ for some } h \in H\}.$$

You can think of gH as the set of all group elements you can "create" by multiplying elements of H on the left by g.

The set of all the left cosets of H in G is written

$$G/H := \{gH \mid g \in G\}.$$

Definition 2.2. Let $H \leq G$ be a subgroup. A *right coset of H in G* is an orbit of the left regular action of H on G. That is,

$$Hg := \{a \in G \mid a = h \cdot g \text{ for some } h \in H\}.$$

You can think of Hg as the set of all group elements you can "create" by multiplying elements of H on the right by g.

The set of all the right cosets of H in G is written

$$H\backslash G := \{Hg \mid g \in G\}.$$

Notation 2.3. As $eH \subseteq G$ and $He \subseteq G$ are both just the set $H \subseteq G$, we will often just write H for these cosets.

WARNING! The only coset of H in G that is a subgroup is $eH = H$ itself. This is because no other coset will contain the identity element.

Remark 2.4. Here is a way to check whether two cosets are the same subset of G.

$$\begin{aligned} gH = g'H &\iff g \in g'H \\ &\iff g' = gh \text{ for some } h \in H \\ &\iff g^{-1}g' \in H. \end{aligned}$$

The reader can deduce the corresponding statements for right cosets.

Example 2.5. Consider the subgroup $H = 2\mathbb{Z} \leq \mathbb{Z}$ of even integers. Then integers n and m are in the same coset of $2\mathbb{Z}$ whenever their difference is even $m - n \in 2\mathbb{Z}$. There are thus two cosets: the odd integers and the even integers. As we are in an additive group, it is common to switch to additive notation for the left cosets $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

We could just have well have written the cosets as $4 + 2\mathbb{Z}$ and $-3 + 2\mathbb{Z}$; any representative will do.

Example 2.6. For a similar kind of example, we have the $3\mathbb{Z} \leq \mathbb{Z}$ has three left cosets $3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$, and two integers are in the same coset if they leave the same remainder on division by 3.

Example 2.7. The isometries of the equilateral triangle form the dihedral group $D_6 = \{e, r, r^2, s, rs, r^2s\}$.

- Let's think about the cosets of the subgroup $R = \{e, r, r^2\}$ generated by r. Recall that in this group we have $sr = r^{-1}s = r^2s$. The left cosets are

$$R = \{e, r, r^2\} \quad \text{and} \quad sR = \{s, sr, sr^2\} = \{s, r^2s, rs\}.$$

  The right cosets are

$$R = \{e, r, r^2\} \quad \text{and} \quad Rs = \{s, rs, r^2s\} = \{s, r^2s, rs\}.$$

  So each left coset is also a right coset. This is not always the case.

- Let's think about the cosets of the subgroup $S = \{e, s\}$ generated by s. The left cosets are

$$S = \{e, s\}, \quad rS = \{r, rs\}, \quad \text{and} \quad r^2S = \{r^2, r^2s\}.$$

  The right cosets are

$$S = \{e, s\}, \quad Sr = \{r, sr\} = \{r, r^2s\}, \quad \text{and} \quad Sr^2 = \{r^2, sr^2\} = \{r^2, rs\}.$$

  In this case most left cosets were not right cosets and vice versa.

The reader will noticed that in all the examples above, the set of left cosets is a partition of the group. This is generally true.

Proposition 2.8. *Given $H \leq G$, the set of left cosets is a partition of G.*

Similarly for right cosets.

Here is a rephrasing of the previous proposition.

Corollary 2.9. *Given $H \leq G$ the relation*

Similarly for right cosets.

$$g \sim g' \iff gH = g'H$$

is an equivalence relation on G, with equivalence classes the left cosets.

Lagrange's Theorem

You may have noticed in the examples above that, for a given $H \leq G$ every left coset is the same size/cardinality as every other left coset. This is easily proved: let $g \in G$, then the functions

$$\begin{array}{ccc} H & \to & gH \\ h & \mapsto & gh \end{array} \quad \text{and} \quad \begin{array}{ccc} gH & \to & H \\ x & \mapsto & g^{-1}x \end{array}$$

are inverses of each other. So every left coset of H is in bijection with H. The similar statement is true for the right cosets. As we now have G partitioned by equally sized sets, the following is straightforward to prove.

Recall that G/H is the set of all left cosets, so $|G/H|$ just means number of left cosets.

Theorem 2.10 (Lagrange's theorem)**.** *Let G be a finite group and let $H \leq G$ be a subgroup. Then $|G| = |H||G/H|$. In particular the order of a subgroup divides the order of the group.*

Remark 2.11. Of course the similar statement is true using right cosets $|G| = |H||G\backslash H|$. Equating the left and right coset versions, and dividing by $|H|$ we get that there are the same number of left and right cosets $|H\backslash G| = |G/H|$.

Definition 2.12. Given $H \leq G$, the *index of H in G* is the number of left cosets $|G/H|$, provided that number is finite. If G/H is infinite, we say H has infinite index in G. The index of H in G is written $|G : H|$.

Remark 2.13. Another way of stating Lagrange's Theorem is to say that if G is a finite group and $H \leq G$ then

$$|G : H| = \frac{|G|}{|H|}.$$

Lagrange's Theorem has many lovely corollaries.

Corollary 2.14. *If G is a finite group, then the order of any element of G divides the order of G.*

Corollary 2.15. *If G is a finite group then for any $g \in G$, we have $g^{|G|} = e$.*

Corollary 2.16. *If $|G|$ is prime then G is cyclic and generated by any non-identity element.*

One of the most striking applications of Lagrange's Theorem is a reproof of a classical number-theoretic result. At a first pass, we have the following result of Fermat.

Figure 2.1: Joseph-Louis Lagrange (1736-1813). It is difficult to overstate Lagrange's contributions to Analysis, Number Theory, Algebra and celestial mechanics. Perhaps just check out the Wikipedia page "List of things named after Joseph-Louis Lagrange", which includes a crater on the moon.

Figure 2.2: A truly marvellous picture of Pierre de Fermat (1601 - 1665), which this margin is too narrow to contain.

Theorem 2.17 (Fermat's Little Theorem)**.** *For any prime $p \in \mathbb{Z}$, and any non-zero integer a, we have $a^{p-1} \equiv 1 \pmod{p}$.*

This result was generalised by Euler to work for any modular arithmetic n, not just for primes p. To describe the generalisation, we need the *Euler totient function*

$$\varphi\colon \mathbb{Z}^{\geq 1} \to \mathbb{Z}^{\geq 1}$$

where $\varphi(n)$ is the number of integers in the set $\{1, \ldots, n-1\}$ that are relatively prime to n.

Example 2.18. If $n = p$ is prime then all the integers in the set $\{1, \ldots, p-1\}$ are relatively prime to p, so $\varphi(p) = p - 1$.

Theorem 2.19 (Euler-Fermat)**.** *For any positive integer n, and any integer a coprime to n, we have $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Normal subgroups and quotient groups

The idea now is to turn the set of cosets ITSELF into a group. You have already seen an example of this, but let's see it again.

Example 2.20. Let $G = \mathbb{Z}$, $n \in \mathbb{N}$ and consider the subgroup $n\mathbb{Z} \leq \mathbb{Z}$. This has cosets

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &= \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + \mathbb{Z}, \ldots, (n-1) + \mathbb{Z}\} \\ &= \{k + n\mathbb{Z} \mid k = 0, 1, \ldots, n-1\}. \end{aligned}$$

There is a binary operation on $\mathbb{Z}/n\mathbb{Z}$

$$(k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) := (k + \ell) + n\mathbb{Z}.$$

It turns out this makes $\mathbb{Z}/n\mathbb{Z}$ into a group (we'll check this later).

How could the approach above FAIL to make a group?

Let $H \leq G$ be a subgroup. We have a notation for the set of left cosets

$$G/H := \{gH \mid g \in G\}.$$

The natural candidate for the group operation is to propose a binary operation on G/H

$$(g_1 H) \cdot (g_2 H) := (g_1 \cdot g_2) H.$$

The potential issue is that gH is not uniquely represented by the element g. A left coset gH is an *equivalence class*, where

$$g \sim g' \iff gH = g'H \iff g = g'h \text{ for some } h \in H.$$

Our proposed binary operation commits the cardinal sin of working with an equivalence class: choosing a representative g of the class gH and not worrying about whether our definition was independent of that choice.

It turns out the following kind of subgroup is exactly what we need.

Definition 2.21. A subgroup $H \leq G$ is *normal* if for every $g \in G$ and $h \in H$ we have that $ghg^{-1} \in H$. If H is a normal subgroup, we indicate this with $H \trianglelefteq G$.

It is also common to just say "$H \leq G$ is a normal subgroup", you don't have to us the symbol $\trianglelefteq$ every time, necessarily.

Remark 2.22. An alternative phrasing is that H is normal if and only if $gHg^{-1} = H$ for all $g \in G$.

Example 2.23. The improper subgroups $\{e\} \leq G$ and $G \leq G$ are, of course, normal.

Example 2.24. Any subgroup of an abelian group G is normal.

You should not discount this abelian example as trivial. All the great things that are about to happen when a subgroup is normal will happen for any subgroup of an abelian group. This is one of the main reasons abelian groups are so nice.

Example 2.25. Let's think about D_{2n}, for $n \geq 3$. The subgroup $K = \{e, s\}$ is not normal; for example, $rsr^{-1} = r^2 s \notin \{e, s\}$. The subgroup $H = \{e, r, \ldots, r^{n-1}\}$ is normal; to see this we do all conjugations: $r^\ell r^k r^{-\ell} = r^k \in H$ for all k, ℓ and $sr^k s^{-1} = s^2 r^{-k} = r^{-k} \in H$ for all k.

The following is a helpful way to restate normality.

Lemma 2.26 (Normal subgroup recognition criterion)**.** *A subgroup $H \leq G$ is normal if and only if $gH = Hg$ for all $g \in G$.*

The lemma has a handy corollary.

Corollary 2.27. *If $H \leq G$ has index two, then H is normal.*

Here is why normal subgroups are so fantastic.

Theorem 2.28. *If $H \leq G$ is a subgroup, then the formula*

$$(g_1 H) \cdot (g_2 H) := (g_1 \cdot g_2) H$$

gives a well-defined binary operation on the set of left cosets G/H if and only if H is a normal subgroup. If indeed H is a normal subgroup then the data $(G/H, \cdot, H)$ is a group.

We give these groups whose elements are cosets a name.

Definition 2.29. If $H \trianglelefteq G$ is a normal subgroup, then the group G/H is called the *quotient group* of G by H.

Exercise 2.1. For $n \in \mathbb{N}$, recall that the set

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

with the operation $a +_n b =$"the remainder of $a + b$ on division by n" is a group. Check that

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}; \qquad k \mapsto k + n\mathbb{Z}$$

is a bijection and a homomorphism. Thus it is an isomorphism, giving an alternative perspective on the group $\mathbb{Z}_n$.

Example 2.30. It was observed in Example 2.25 that the subgroup of $H \leq D_{2n}$ generated by r is normal. By Lagrange's Theorem, we have $|G/H| = |G|/|H| = 2$. So the quotient group must necessarily be isomorphic to C_2. In summary

$$D_{2n}/H = \{H, sH\} \cong C_2.$$

An alternative was to deduce H is normal is to use Lagrange's Theorem to compute H is index 2 and use Corollary 2.27.)

Example 2.31. By inspecting the conjugates of r^2, similarly to Example 2.25, we see that $H = \{e, r^2\} \leq D_8$ is a normal subgroup. Lagrange's Theorem tells us the index is $|G/H| = |D_8|/|H| = 8/2 = 4$. We have classified groups of order 4 as either C_4 or $C_2 \times C_2$, distinguished by whether each nontrivial element is order 2 or not. We have

$$G/H = \{H, rH, sH, rsH\}.$$

We check: $rH \cdot rH = r^2H = H$, $sH \cdot sH = s^2H = H$ and $rsH \cdot rsH = (rsrs)H = (rr^{-1}ss)H = H$. As all elements have order 2, we have $D_8/H \cong C_2 \times C_2$.

Example 2.32. Consider $H = \{\mathbf{1}, -\mathbf{1}\} \leq Q_8$. By inspecting the conjugates, we see this is a normal subgroup, so that

$$Q_8/H = \{H, \mathbf{i}H, \mathbf{j}H, \mathbf{k}H\}$$

is a group of order 4. Checking the orders of the elements, we see again that $Q_8/H \cong C_2 \times C_2$.

The Isomorphism Theorem(s)

An important perspective on normal subgroups is as kernels of homomorphisms.

Proposition 2.33. *If $\varphi\colon G \to H$ is a homomorphism, then $\ker(\varphi) \leq G$ is a normal subgroup.*

In fact EVERY normal subgroup is the kernel of some homomorphism, which is easy to show.

Definition 2.34. Let $N \leq G$ be normal, the *quotient map* (a.k.a. *projection map* is the function

$$q\colon G \to G/N; \qquad g \mapsto gN.$$

Proposition 2.35. *Let $N \leq G$ be normal. Then the quotient map is a surjective group homomorphism with kernel N.*

Remark 2.36. A sequence of group homomorphisms

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is called a *short exact sequence* if f is injective, g is surjective, and $\mathrm{im}(f) = \ker(g)$.
A nice way to summarise the previous proposition is to say that

$$H \xrightarrow{i} G \xrightarrow{q} G/N$$

is a short exact sequence, where i denotes the inclusion map.

Theorem 2.37 (The First Isomorphism Theorem)**.** *Let $\varphi\colon G \to H$ be a homomorphism. Then the function*

$$\overline{\varphi}\colon G/\ker(\varphi) \to \mathrm{im}(\varphi); \qquad g\ker(\varphi) \mapsto \varphi(g)$$

is a well-defined group isomorphism.

The rank-nullity theorem from linear algebra follows from the First Isomorphism Theorem. A linear map $T\colon V \to W$ is an additive group homomorphism. Choosing a basis of $\ker(T)$ and extending it to a basis of V, the extension determines a subspace $U \subseteq V$ such that $V = \ker(T) \oplus U$, and such that $U \cong G/\ker(T)$. Then

$$\begin{aligned}\dim V &= \dim\ker(T) + \dim U \\ &= \dim\ker(T) + \dim G/\ker(T) \\ &= \dim\ker(T) + \dim\mathrm{im}(T).\end{aligned}$$

Example 2.38. Consider the function $\varphi\colon \mathbb{Z} \to Z_n$ given by $\varphi(x) =$"the remainder of x on division by n". This map is surjective, so $\mathrm{im}(\varphi) = \mathbb{Z}_n$. The kernel of this map is $n\mathbb{Z}$, the set of integers that are a multiple of n. By the First Isomorphism Theorem, we thus have that

$$\overline{\varphi}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n; \qquad x \mapsto \varphi(x)$$

is an isomorphism. This is the inverse of the isomorphism given in Example 2.1.

Example 2.39. The function

$$\varphi\colon (\mathbb{R}, +, 0) \to (\mathbb{C}\setminus\{0\}, \times, 1); \qquad \varphi(t) = e^{2\pi i t}$$

is a group homomorphism. The image is $S^1 \subseteq \mathbb{C}\setminus\{0\}$ and the kernel consists of the integers $\mathbb{Z} \subseteq \mathbb{R}$. Thus, by the First Isomorphism Theorem, there is a group isomorphism $\mathbb{R}/\mathbb{Z} \cong S^1$.

This is an algebraic statement, but can be upgraded to a topological statement. The intuition is that taking the quotient by $\mathbb{Z}$ is an instruction to wrap the real line around the circle integer many times.

Remark 2.40. As you might imagine there is a Second, Third and even Fourth Isomorphism Theorem. It is the opinion of the author that you should be aware of the existence of the other ones but not worry too much about them until you need them for something.

To give you a flavour, here's number Three. It says that if $H, K \trianglelefteq G$, $H \leq K$ then $K/H \trianglelefteq G/H$ and that the quotient groups "cancel like fractions":

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

Hopefully this gives you the vibe. The other isomorphism theorems are increasingly specific, and useful in a pinch, but can be glossed over on a first pass.

Simple groups

Any technique for breaking a big group into smaller groups is helpful for the task of classifying groups.

If a group G has a normal subgroup H, we can now attempt to understand G by understanding the groups H, G/H, and how they fit together.

Some groups have no proper normal subgroups.

Definition 2.41. A group G is called *simple* if G has no normal subgroups except $\{e\}$ and G.

Simple groups are particularly hard to analyse and classify because they do not "decompose" in any way. They can be thought of as the building blocks of group theory, similar to primes as the building blocks of the integers. They are the fundamental symmetries.

Theorem 2.42. *An abelian group is simple if and only if it is isomorphic to the cyclic group C_p, for some prime p.*

Remark 2.43. All finite simple groups are classified - this is known as The Enormous Theorem. The proof consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published mostly between 1955 and 2004. Here are the types of finite simple group:

- Cyclic groups C_p of prime order (we've seen these)
- Alternating groups A_n for $n \geq 5$ (we'll see these soon)
- Simple groups of Lie type. There are 16 infinite families – we will not see these in the course.
- The sporadic groups. There are just 26 of these. We will not see them in the course.

The largest sporadic simple group is called the **MONSTER GROUP**. It has order

$$808,017,424,794,512,875,886,459,$$
$$904,961,710,757,005,754,368,000,000,000.$$

Figure 2.3: Bernd Fischer abstractly predicted the existence of the MONSTER GROUP in 1973.

Figure 2.4: Robert Griess explicitly constructed the MONSTER GROUP in 1980.

3 *Finite groups of small order*

We almost know enough to classify all groups of order at most 8.

The quaternion group

We introduce a new group of small order, not so far considered. Let's start with an example.

Example 3.1. Consider the following four 2×2 complex matrices, which each square to be the identity matrix,

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Exercise 3.1. Verify the following formulas:

- $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$
- $\mathbf{ij} = \mathbf{k}, \qquad \mathbf{jk} = \mathbf{i}, \qquad \mathbf{ki} = \mathbf{j}.$
- $\mathbf{ji} = -\mathbf{k}, \qquad \mathbf{kj} = -\mathbf{i}, \qquad \mathbf{ik} = -\mathbf{j}.$

These formulas verify that matrix multiplication gives a well-defined binary operation on the set $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j} \pm \mathbf{k}\}$ (i.e. the set is closed under matrix multiplication).

The next step is to use the matrix multiplication as the rules for a binary operation, but we can forget about the fact that the rules came from matrices, if we like.

Definition 3.2. The *quaternion group* is the group defined by the data

$$Q_8 = (\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j} \pm \mathbf{k}\}, \cdot, \mathbf{1})$$

and using the rules that $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}$.

Exercise 3.2. Use the multiplication formulas to verify this is indeed enough to define a group. In particular, find all inverses.

Remark 3.3. The discovery of quaternions was a stunning achievement. It is similar in importance to the discovery of complex numbers. Quaternions are a foundational idea that turn up all through physics, geometry and algebra. They also explain the existence of the cross product in dimension 3 (not obvious, but worth delving into).

Figure 3.1: William Rowan Hamilton (1805-1865) discovered the quaternions while deep in thought on a walk in Dublin. He carved them into the stone of a nearby bridge. There is a plaque on the bridge commemorating the momentous event.

We make a distinction between the quaternion group (which is a group) and the "the quaternions" which is the 4-dimensional real vector space with basis $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$. Unlike most vector spaces, the vectors in this vector space can be multiplied together to form new vectors, making the quaternions into an *associative algebra*. This remark will mean more to you by the end of the course.

Direct products

The quaternions are special because they are not related to any other group of order ≤ 8. Most groups are just combinations of lower order groups, similarly to how most integers are just combinations of prime numbers.

Here is a way to make new groups from old.

Note that $|G \times H| = |G||H|$. This is just a set-theoretic statement about Cartesian products.

Definition 3.4. Given groups $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$. The Cartesian product $G \times H$ has binary operation

$$(g, h) \cdot (g', h') = (g \cdot g', h \cdot h')$$

and identity (e_G, e_H). This defines the product group $G \times H$.

Exercise 3.3. Prove that $H \times G$ is isomorphic to $G \times H$.

Example 3.5. The projection map $G \times H \to G$ given by $(g, h) \mapsto g$ is a surjective group homomorphism with kernel $\{e\} \times H$. Thus $\{e\} \times H \leq G \times H$ is a normal subgroup and $G \times H/(\{e\} \times H) \cong G$ by The First Isomorphism Theorem.

Here is a straightforward consequence you might recall from an elementary Number Theory course.

Theorem 3.6 (Chinese Remainder Theorem). *Suppose $n, m \in \mathbb{N}$ have no common factors. Then*

$$\varphi\colon C_{nm} \to C_n \times C_m; \qquad \varphi(x) := (x^m, x^n)$$

is an isomorphism.


孫子筭經卷上
唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋
度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Figure 3.2: Almost nothing is known about the Chinese mathematician Sun Zi (≈ 400) to whom the "Chinese Remainder Theorem" is attributed.

Here is a theorem for quickly deciding if a group breaks into a product.

Proposition 3.7 (Direct product recognition theorem). *Let $H_1, H_2 \leq G$ be subgroups. Then the map*

$$H_1 \times H_2 \to G; \qquad (h_1, h_2) \mapsto h_1 \cdot h_2$$

is an isomorphism if the following are true.

(i) $H_1 \cap H_2 = \{e\}$.

(ii) If $h_1 \in H_1$ and $h_2 \in H_2$ then $h_1 \cdot h_2 = h_2 \cdot h_1$.

(iii) For every $g \in G$, there exist $h_i \in H_1$ and $h_2 \in H_2$ such that $g = h_1 \cdot h_2$.

Classifying groups of small order

We will need a couple more tools for the classification of all finite groups with at most 8 elements.

Proposition 3.8. *If every element of G has order 1 or 2 then*

$$G \cong C_2 \times \cdots \times C_2.$$

We will not prove the following right now, but will permit ourselves to use the result as part of our classification.

It is a little naughty to use a theorem without having proved it. But I am impatient to classify groups of order at most 8, and the nicest proof of Cauchy's Theorem needs material from the next section. Please forgive me!

Theorem 3.9 (Cauchy's Theorem)**.** *Suppose p is a prime that divides the order of a finite group G. Then G has a subgroup of order p.*

OK, let's classify! Suppose G is a finite group or order at most 8.

- Order 1: $G = \{e\}$.
- Order $p = 2, 3, 5, 7$: $G \cong C_p$.

  Recall Corollary 2.16: finite groups of prime order p are cyclic (and therefore isomorphic to C_p).
- Order 4: Each element of G has order 1, 2, or 4, by Lagrange's Theorem.
  - If G has an element of order 4 then $G \cong C_4$.
  - If there is no element of order 4 then all elements are of order 1 or 2. So $G \cong C_2 \times C_2$ by Proposition 3.8.

    We have just shown that the Kleinviergruppe is isomorphic to $C_2 \times C_2$.
- Order 6: Each element of G has order 1, 2, 3 or 6, by Lagrange's Theorem.
  - If there is an element of order 6 then $G \cong C_6$.
  - If there is no element of order 6, proceed as follows. By Cauchy's Theorem, G has a subgroup $\{e, s\} = H_1$ of order 2 and a subgroup $\{e, r, r^2\} = H_2$ of order 3. It must be that $H_1 \cap H_2 = \{e\}$ as otherwise some element would have order both 2 and 3, which cannot happen. If r and s were to commute then $(rs)^2 = r^2s^2 = s^2 \neq e$ and $(rs)^3 = r^3s^3 = r \neq e$, showing that rs does not have order 2 or 3, meaning rs has order 6. As we assumed no element had order 6, it must be that r and s do not commute. Thus the elements e, r, r^2, s, rs and sr are all distinct elements of the group, meaning $G = \{e, r, r^2, s, rs, sr\}$. Consider this from the perspective of left cosets of H_1:

    $$G = H_1 \cup rH_1 \cup r^2H_1 = \{e, s\} \cup \{r, rs\} \cup \{r^2, r^2s\}.$$

    As sr must be in one of these left cosets, we can, by inspection, eliminate all possibilities except $sr = r^2s$. Thus, indeed, $G \cong D_6$

    This shows D_6 is the only non-abelian group of order 6.
- Order 8: Each element of G has order 1, 2, 4, or 8 by Lagrange's Theorem.
  - If G has an element of order 8 then $G \cong C_8$.
  - If all elements of G are order 1 or 2, then $G \cong C_2 \times C_2 \times C_2$.

– Suppose there is no element of order 8, and there exists an element x of order 4, which generates a subgroup $H = \{e, x, x^2, x^3\}$. The index of this subgroup must be $|G : H| = 2$, so it has exactly two left cosets H and yH, say, for some $y \in G$. Thus we have

$$G = H \cup yH = \{e, x, x^2, x^3, y, yx, yx^2, yx^3\}.$$

If $y^2 \in yH$, we would have $y \in H$, a contradiction, so $y^2 \in H$. If $y^2 = x$ or $y^2 = x^3$ then $y^4 = x^2 \neq e$ or $y^4 = x^6 = x^2 \neq e$, so we deduce y would have order 8, which is a contradiction.

Thus the possibilities are $y^2 = e$ or $y^2 = x^2$.

Claim. We claim G is isomorphic to one of $C_4 \times C_2$, D_8 or Q_8.

Recall we only get $C_{nm} \cong C_n \times C_m$ when n and m are coprime, so $C_8 \ncong C_4 \times C_2$.

* Suppose $y^2 = e$ and $xy = yx$. Then the reader may check the conditions of the Direct Product Recognition Theorem are satisfied for the subgroups $\{e, y\} \cong C_2$ and $\{e, x, x^2, x^3\} \cong C_4$. Thus $G \cong C_2 \times C_4$.
* Suppose $y^2 = e$ and $xy \neq yx$. Consider the four left cosets of $K = \{e, y\} \leq G$. Note no two of e, x, x^2, and x^3 can be in the same coset as each other, and thus can be used as representative for the four cosets. So the cosets are

$$\begin{aligned} G &= K \cup xK \cup x^2K \cup x^3K \\ &= \{e, y\} \cup \{x, xy\} \cup \{x^2, x^2y\} \cup \{x^3, x^3y\} \end{aligned}$$

As $yx \neq xy$, we must have $yx \in x^2K$ or $yx \in x^3K$. If $yx \in x^2K$ then $yx = x^2y$. This implies $yxy = x^2$. But the left-hand side is order 4 and the right-hand side is order 2, a contradiction. So $yx \in x^3K$ and thus $yx = x^3y = x^{-1}y$. This implies $xy = yx^{-1}$, so we now have all the generators and relations for the dihedral group D_8

$$G = \langle x, y \mid x^4 = e, y^2 = e, xy = yx^{-1} \rangle \cong D_8.$$

* Suppose $y^2 = x^2$ and $xy = yx$. Then the reader may check the conditions of the Direct Product Recognition Theorem are satisfied for the subgroups $\{e, yx^{-1}\} \cong C_2$ and $\{e, x, x^2, x^3\} \cong C_4$. Thus $G \cong C_2 \times C_4$ again.
* Suppose $y^2 = x^2$ and $xy \neq yx$. We have either $xy \in H$ or $xy \in yH$. But if $xy \in H$, then $y \in H$, which is not the case. So $xy \in yH$. This implies $y^{-1}xy \in H$. This is an element of order 4, so must be either x or x^3. It cannot be the $y^{-1}xy = x$ as this implies $xy = yx$. Hence $y^{-1}xy = x^3 = x^{-1}$, so $xy = x^{-1}y$. The reader may now wish to check the following bijection of sets is a group homomorphism, and thus an

isomorphism.

$$G \to Q_8;\qquad \begin{array}{rclrcl} e & \mapsto & \mathbf{1}, & y & \mapsto & \mathbf{j}, \\ x & \mapsto & \mathbf{i}, & yx & \mapsto & -\mathbf{k}, \\ x^2 & \mapsto & -\mathbf{1}, & yx^2 & \mapsto & -\mathbf{j}, \\ x^3 & \mapsto & -\mathbf{i}, & yx^3 & \mapsto & \mathbf{k}. \end{array}$$

Yay!

4 Group actions

Actions of groups on sets

Definition 4.1. An *action* of a group $(G, \cdot, e)$ on a set X is a function $*\colon G \times X \to X$ satisfying, for all $a, b \in G$, $x \in X$,

(i) $e * x = x$, IDENTITY

(ii) $(a \cdot b) * x = a * (b * x)$. ASSOCIATIVITY

Specifically, this is called a *left action* because the group elements are applied on the left of the set elements. This is completely arbitrary and we could instead apply elements on the right to get a *right action*. We will explore this in more detail later.

Example 4.2. Any group G acts on any set X by the *trivial action* $a * x = x$ for all $a \in G$ and $x \in X$.

Example 4.3. Any group G acts on the set $X = G$ by the *left-regular action* $a * x = a \cdot x$ for all $a \in G$ and $x \in G$.

Example 4.4. Given any set X, the symmetric group $\mathrm{Sym}(X)$ acts on X by $f * x = f(x)$.

Example 4.5. Let X be one of the platonic solids. Then the group of isometries $\mathrm{Isom}(X)$ acts on the set X via $f * x = f(x)$.
This formula also works to make the group $\mathrm{Isom}(X)$ act on the set $V \subseteq X$ of vertices of the solid. Similarly, on the set $E \subseteq X$ of faces of the solid. Similarly, on the set $F \subseteq X$ of edges of the solid.

In contrast, elements of the full symmetry group $\mathrm{Sym}(X)$ of a platonic solid are not necessarily isometries, so most will not preserve geometric features like edges and faces. Hence $\mathrm{Sym}(X)$ *does not* act on the subsets $V, E, F \subseteq X$ using the formula $f * x = f(x)$.

Example 4.6. The dihedral group D_{2n} acts on the set of vertices of the regular n-gon via $f * x = f(x)$.

Example 4.7. The general linear group $(\mathrm{GL}_2(\mathbb{R}), \times, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$ acts on $\mathbb{R}^2$ in the usual way, via matrix multiplication. Let $(u, v) \in \mathbb{R}^2$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} u \\ v \end{pmatrix} := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} au + bv \\ cu + dv \end{pmatrix} \in \mathbb{R}^2.$$

Definition 4.8. Let G act on X.

(i) The *orbit* of $x \in X$ is

$$Gx := \{y \in X \mid a * x = y \text{ for some } a \in G\} \subseteq X.$$

The orbit of x consists of all the points in the set you can move x to, using the group action.

(ii) The *stabiliser* of $x \in X$ is

$$G_x := \{a \in G \mid a * x = x\} \subseteq G.$$

The stabiliser of x is the collection of group elements that fix x in place when they act on the set.

Some actions have the property that there is a way to send any element of X to any other element of X using the action, we give this a special name.

Definition 4.9. An action of G on X is *transitive* it, for all $x, y \in X$, there exists $a \in G$ such that $a * x = y$.
An equivalent way to say an action is transitive is that each element of the set has orbit the entire set: $Gx = X$ for all $x \in X$.

Here are some elementary facts about orbits and stabilisers.

Proposition 4.10. *Let G act on X. For all $x \in X$, the stabiliser is a subgroup $G_x \leq G$.*

Theorem 4.11. *Let G act on X. Then the following is an equivalence relation on X*

$$\text{“}x \text{ is related to } y \iff y \in Gx \text{ ”}.$$

In other words, $x \sim y \iff y = a * x$ for some $a \in G$.

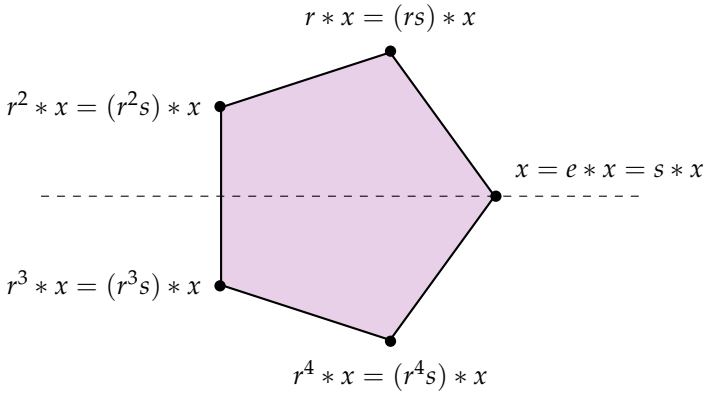
Here are some immediate consequences

- By definition, the orbits Gx are the equivalence classes of this equivalence relation.
- $Gx = Gy \iff x \in Gy \iff y \in Gx$.
- The set of orbits partitions the set X.
- To check an action is transitive, you do not have to show $Gx = X$ for all $x \in X$, it suffices to show $Gx = X$ for some $x \in X$.

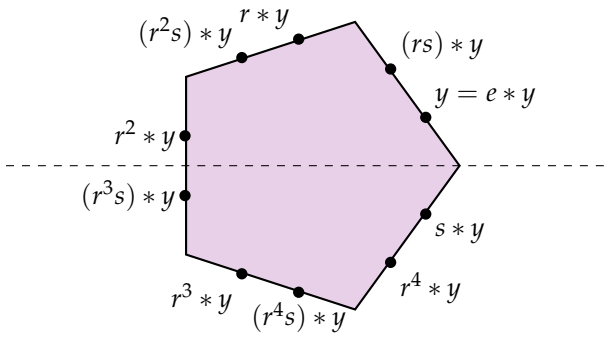
Examples of group actions

Example 4.12. The dihedral group $G = D_{2n}$ acts on the regular n-gon $X \subseteq \mathbb{R}^2$. Let's illustrate with $n = 5$:

$$D_{10} = \{e, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\} = \langle r, s \mid r^5 = e, s^2 = e, rs = sr^{-1} \rangle$$

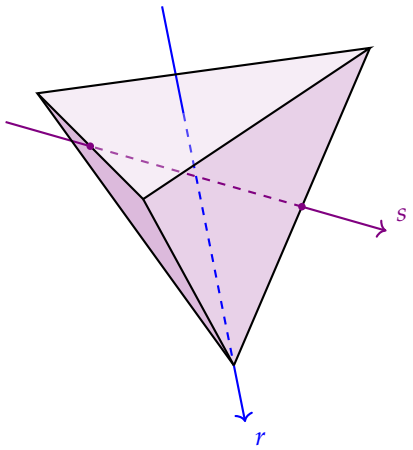


- Picking any vertex $x \in X$, we can see the orbit $Gx \subseteq X$ is the set of all vertices of X. The stabiliser is the subgroup generated by the reflection s in the dashed line $G_x = \{e, s\} \leq G$. Note that $|Gx| = n$, $|G_x| = 2$, and so $|Gx||G_x| = |G| = 2n$.
- Now pick a point $y \in X$ on one of the edges, but not on the midpoint of an edge.



We see that the orbit $Gy \subset X$ now consists of $2n$ points, and that the only element of G that stabilises y is e, so that $G_y = \{e\} \leq G$. Note, however, that we still have $|Gy||G_y| = |G| = 2n$.

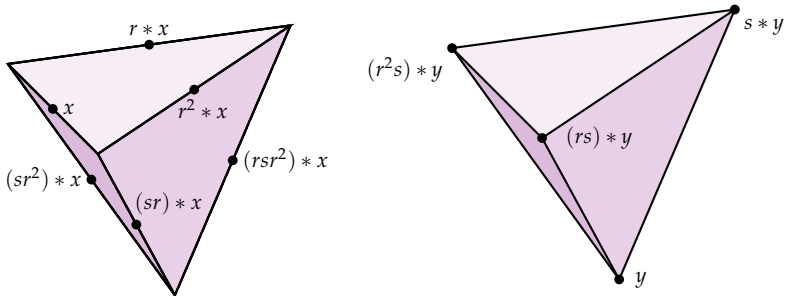
Example 4.13. The group G of rotational symmetries of the tetrahedron acts on the tetrahedron. There are two types of rotation axis: the type through a vertex and opposite face centre (four of these), and the type through an edge midpoint and opposite edge midpoint (three of these). Let's depict just one of each type.



In the diagram above, we denote the right-handed turns around the depicted axes as s and r. Note r is order 3 and s is order 2.

- Let x be a point in the middle of one of the edges. The orbit is the set of midpoints of all six edges, as shown in the diagram,

so $|Gx| = 6$. A rotation can only fix x if x is on the axis of rotation, thus s is the only non-trivial stabiliser of x. In other words, $G_x = \{e, s\} \leq G$ and $|Gx||G_x| = 6 \cdot 2 = 12$.



- Now let y be one of the vertices. There are group elements sending y to each of the other vertices (see picture), and by symmetry y cannot be sent to a non-vertex element by the group action. Hence the orbit of y is the set of all 4 vertices $|Gy| = 4$. The stabiliser of y is the subgroup of G generated by the rotation r, and thus $G_y = \{e, r, r^2\}$. Once again, $|Gy||G_y| = 12$.

Remark 4.14. Let G act on X. The obvious conjecture from the examples above is that, for any given $x \in X$, the product $|Gx||G_x|$ is a way of computing the order of the group G. This is indeed true, and is the central theorem for group actions, called the *Orbit-Stabiliser Theorem*. We will prove this in due time, after developing some more technology.

Left versus right actions

What we described in Definition 4.1, is called more specifically a *left action*, because the group elements are applied on the left of the set elements $a * x$. There is nothing special about the left, and the definition works equally well on the right.

Definition 4.15. A *right action* of a group $(G, \cdot, e)$ on a set X is a function $\bullet\colon X \times G \to X$ satisfying, for all $a, b \in G$, $x \in X$,

(i) $x \bullet e = x$, IDENTITY

(ii) $x \bullet (a \cdot b) = (x \bullet a) \bullet b$. ASSOCIATIVITY

The theory works exactly the same for right actions. We have orbits partitioning the set and stabilisers which are subgroups of G.

Notation 4.16. For a right action we will write xG for the orbit of a point $x \in X$. We will continue to write G_x for the stabiliser of x.

The left/right distinction doesn't change the theory. Indeed, a left action determines a right action an vice-versa, as the next exercise shows.

Exercise 4.1. Given a left action of G on X

$$*\colon G \times X \to X; \qquad (a, x) \mapsto a * x,$$

verify that the following is a right action of G on X

$$\bullet\colon X \times G \to X; \qquad (x, a) \mapsto x \bullet a := a^{-1} * x.$$

So in some sense, left versus right is just a notation choice. Do you prefer hitting x with the symbol a on the left or on the right? We generally default to left, but for no particular reason.

There are situations when two group actions are naturally present on the same set. It can then make notational sense to have one action coming in on the left and one coming in from the right, either to distinguish the actions, or because naturally one look like a "left thing" and one looks like a "right thing". This is the reason to make this careful left/right distinction, despite the fact that the previous exercise shows the concepts are essentially interchangeable.

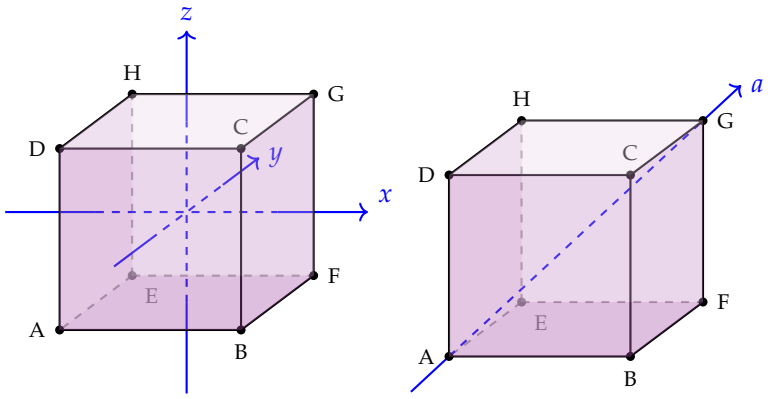
The Orbit-Stabiliser Theorem

Theorem 4.17 (The Orbit-Stabiliser Theorem)**.** *Let G be a finite group acting on a set X. Then for any $x \in X$, the size of the orbit is equal to the index of the stabiliser $|Gx| = |G : G_x|$. Equivalently $|G| = |G_x||Gx|$.*

Examining the proof of the Orbit-Stabiliser theorem, one can see that the version for infinite groups is that the cardinality of Gx is equal to the cardinality of G/G_x.

Example 4.18. In Example 4.13, the action of the group G of rotational symmetries of the tetrahedron, we saw example of elements x in the tetrahedron such that $|Gx||G_x| = 12$. The Orbit-Stabiliser Theorem now implies $|G| = 12$.

Example 4.19. Let's compute the number of rotational symmetries of a cube. Let G be the group of rotational symmetries.



There are 3 axes of rotation perpendicular to the faces and each of these rotations has order 4. There are 4 axes of rotation going diagonally through the cube between opposite vertices (only one is pictured above), and each of these rotations has order 3.
Let x be the vertex labelled A. The action is transitive (we leave it to the reader to imagine how A can be sent to each of B, C, D, E, F, H, G using rotations). Hence $|Gx| = 8$. The only rotations that fix A are the ones with axis of rotation through A. Call a $2\pi/3$ right-handed rotation around this axis a. Then G_x is the subgroup generated by a, namely $\{e, a, a^2\} \leq G$. Thus $|G| = |Gx||G_x| = 8 \cdot 3 = 24$, by the Orbit-Stabiliser Theorem.

Exercise 4.2. Repeat the strategy employed above to compute that the octahedron has 24 rotational symmetries, the dodecahedron has 60, and the icosahedron has 60.

Exercise 4.3. Repeat the strategy employed above again, to compute that order of the full isometry group (now allowing reflections, too) for all 5 platonic solids.

Cauchy's Theorem

We can now produce the promised proof of Cauchy's Theorem, which we restate for the reader's convenience.

Theorem 4.20 (Cauchy's Theorem)**.** *Suppose p is a prime that divides the order of a finite group G. Then G has a subgroup of order p.*

Proof. Consider the action of the cyclic group $C_p = \langle \xi \mid \xi^p = e \rangle$ on $G^p = G \times \cdots \times G$ given by "cycling" the co-ordinates

$$\xi * (x_1, x_2, \ldots, x_{p-1}, x_p) = (x_2, x_3, \ldots, x_p, x_1).$$

In fact, we want to consider this action on a particular subset $X \subseteq G^p$, defined as follows

$$X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdot \ldots \cdot x_p = e\}.$$

Note the following:

- We have $|X| = |G|^{p-1}$. To see this, consider that the first $p-1$ elements in $(x_1, \ldots, x_p)$ can be chosen freely/independently, and the pth element is forced to be $(x_1 \cdot \ldots \cdot x_{p-1})^{-1}$.
- The cycling action on G^p sends elements of X to elements of X, because cycling the co-ordinates does not change the fact that their product is e. So C_p acts of X by cycling.

Figure 4.1: Augustin-Louis Cauchy (1789-1857) pioneered the study of analysis, both real and complex, and the theory of permutation groups.

As the size of an orbit divides the order of the group, it must be that orbits are size 1 or size p. An element of X in a size 1 orbit must have all entries the same or else cycling the entries would change the element. Thus size 1 orbits look like $\{(x,\dots,x)\}$ such that $x^p = e$. As p is prime, having $x^p = e$ implies either $x = e$ or x is order p. The proof will be complete if we can show there is at least one orbit $\{(x,\dots,x)\}$ of size 1, where $x \neq e$, as then the subgroup generated by x will be the order p subgroup we are seeking.

If $x^n = e$ for n, not prime, we cannot conclude $x = e$ or x is order n. For example $(-1)^4 = 1$, but -1 is order 2.

We know that X is partitioned into orbits and $|X| = |G|^{p-1}$. So consider

$$\begin{aligned} |G|^{p-1} &= \underbrace{(\text{number of size 1 orbits})}_{n} \cdot 1 + \underbrace{(\text{number of size } p \text{ orbits})}_{m} \cdot p \\ &= n + mp. \end{aligned}$$

We can rearrange the equation above to get $n = |G|^{p-1} - mp$. We can use our hypothesis that p divides $|G|$ to then see that p must divide n. So $n = kp$ for some $k \in \mathbb{N}$. We know $k \neq 0$, because there is at least one size 1 orbit, namely that of $(e,\dots,e)$. So $k \geq 1$. We can conclude there are at least $p-1$ orbits of the type we are interested in: size 1 orbits $\{(x,\dots,x)\}$ where $x \neq e$. This completes the proof. □

Note we have actually proved something stronger than the statement of Cauchy's Theorem, namely there are at least $p-1$ subgroups of G of order p.

Groups acting on themselves – the regular actions

We think of the group's binary operation as the group *acting on itself*.

Definition 4.21. The left action of G on the set $X = G$

$$*\colon G \times G \to G; \qquad a * b := a \cdot b$$

is called the *left regular action* of G on itself.
Given any subgroup $H \leq G$ we obtain a left action of H on the set $X = G$

$$*\colon H \times G \to G; \qquad a * b := a \cdot b,$$

which is called the *left regular action* of H on G.

Okay! Now let's do that again, but coming in from the right.

Definition 4.22. The right action of G on the set $X = G$

$$\bullet\colon G \times G \to G; \qquad b \bullet a := b \bullet a$$

is called the *right regular action* of G on itself.
Given any subgroup $H \leq G$ we obtain a right action of H on the set $X = G$

$$\bullet\colon G \times H \to G; \qquad b \bullet a := b \bullet a,$$

which is called the *right regular action* of H on G.

Observe that if G is abelian then

$$a * b = a \cdot b = b \cdot a = b \bullet a$$

so there is no distinction between the left and right regular actions.

What are the stabilisers and orbits?

Well, if $a \cdot b = a$ or $b \cdot a = a$ then $b = e$. So the only "do nothing" left/right multiplication is by the identity. So the stabiliser of any $a \in G$ under the left/right regular action is $\{e\}$. Not very interesting.

The orbits, however are very interesting.

Exercise 4.4. Let $H \leq G$ be a subgroup. Verify the following.

(i) A left coset gH of H in G is exactly the orbit of $g \in H$ under the right regular action of H on G.

(ii) A right coset Hg of H in G is exactly the orbit of $g \in H$ under the left regular action of H on G.

As orbits of an action partition the set, this gives an elegant proof of a fact we already knew, that the sets of cosets G/H and $H\backslash G$ are each partitions of G.

Cayley's Theorem

The following is a very important perspective shift on the concept of a group action.

Theorem 4.23. *There is a one-to-one correspondence between actions of a group G on a set X and homomorphisms $\rho\colon G \to \mathrm{Sym}(X)$ from G to the symmetry group of X.*

The fact that a group action assigns each group element a symmetry of X should be intuitive. What requires checking is that this assignment is a well-defined group homomorphism $\rho\colon G \to \mathrm{Sym}(X)$.

Definition 4.24. The homomorphism

$$\rho\colon G \to \mathrm{Sym}(X)$$

associated to a group action is called the *permutation representation*.

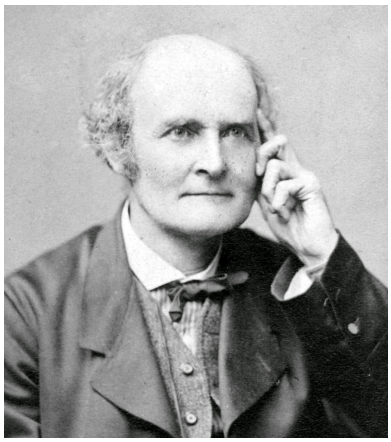


Figure 4.2: Arthur Cayley (1821 - 1895). Heavily involved in developing the algebra of matrices and non-Euclidean geometry.

The following is kind of a proof-of-concept for the idea that the abstract thing we defined called a "group", really is always representing the symmetry of something. In practice, I have never found this theorem super helpful for anything, it's more confirmation that the entire topic of Group Theory is on the right track as a study of symmetries.

Theorem 4.25 (Cayley's Theorem)**.** *For any group G there is a set X such that $G = \mathrm{Sym}(X)$.*

We can now introduce another concept in group actions.

Definition 4.26. Let G act on a set X, and write $\rho\colon G \to \mathrm{Sym}(X)$ for the the permutation representation.

(i) The *kernel* of the action is $\ker(\rho) \leq G$. In other words, g is in the kernel of the action if, for all $x \in X$, we have $g * x = x$.

The kernel of an action consists of the group elements g that fix every element of X in place. The group elements that are not "doing anything".

(ii) The action is *faithful* if the kernel is $\{e\}$. In other words, for all non-trivial $g \in G$, there exists $x \in X$ such that $g * x \neq x$.

The intuition for faithful actions is that every non-trivial element of the group is actually "doing something" to X.

Remark 4.27. A more convenient way to format a proof that an action is faithful is to prove the statement: "If $g * x = x$ for all $x \in X$ then $g = e$."

Example 4.28. The trivial action of any group G on any set X has kernel G, by definition. This is the least faithful action one can define.

Example 4.29. The left-regular action can only be non-faithful if G is the trivial group. To see this, consider that $g * g = g^2$. So if $g^2 = g$ for all $g \in G$ then $g = e$ for all $g \in G$.

Example 4.30. The cyclic group $C_4 = \{1, i, -1, -i\}$ acts on the set $X = \{1, i, -1, -i\}$ in the following way (that is not the regular action). For $g \in C_4$, the action is $g * x := g^2 x$. For $g = -1$, we have $g^2 = 1$, so this means $g = -1$ is in the kernel and the action is not faithful. For both $g = i$ and $g = -i$, we have $g^2 = -1$, which multiplies non-trivially. Hence $g = i$ and $g = -i$ are not in the kernel.

Groups acting on themselves – the conjugation action

There is another important action that every group has on itself.

Definition 4.31. We say elements $a, b \in G$ are *conjugate* to one-another if there exists $g \in G$ such that $b = g \cdot a \cdot g^{-1}$.

This language gets used in various other ways: "a and b are conjugates", "b is the conjugation of a by g", to name a couple.

You should briefly convince yourself bare-hands that "being conjugate" is an equivalence relation, before reading the next definition, which leads to a slicker proof of that fact.

Definition 4.32. The *conjugation action* of a group G on the set G is

$$g * a := g \cdot a \cdot g^{-1}$$

Exercise 4.5. Prove the conjugation action indeed defines an action.

The orbits, stabilisers, and kernel of the conjugation action play a central role in group theory.

Definition 4.33. Let G be a group and consider the conjugation action.

(i) An orbit of the action is called a *conjugacy class*. The conjugacy class of $a \in G$ is written

$$[a] = \{b \in G \mid b = g \cdot a \cdot g^{-1} \text{ for some } g \in G\}.$$

As orbits partition the set being acted on, we see every group is partitioned into its conjugacy classes.

(ii) The stabiliser of an element $a \in G$ is called the *centraliser* of a, and is written

$$C_G(a) = \{g \in G \mid a = g \cdot a \cdot g^{-1}\} = \{g \in G \mid a \cdot g = g \cdot a\}.$$

In other words, the centraliser of a is the subgroup of G consisting of all elements that commute with a.

(iii) The kernel of the conjugacy action is called the *centre* of G and is written

In other words, the centre of a group G is the subgroup of all elements that commute with everything in G.

$$\begin{aligned} Z(G) &= \{g \in G \mid a = g \cdot a \cdot g^{-1} \text{ for all } a \in G\} \\ &= \{g \in G \mid a \cdot g = g \cdot a \text{ for all } a \in G\}. \end{aligned}$$

Example 4.34. The only conjugacy class that is ever a subgroup is the conjugacy class of e, because this is the only conjugacy class containing e. As $g \cdot e \cdot g^{-1} = e$ for all $g \in G$, the conjugacy class of e is always the trivial subgroup $\{e\} \leq G$.

Example 4.35. Everything commutes with everything in an abelian group G, so $G = Z(G)$ for abelian groups.

Example 4.36. Consider the dihedral group $D_6 = \{e, r, r^2, s, rs, r^2s\}$ of isometries of an equilateral triangle.

- The partition of D_6 by conjugacy classes looks like

  $$D_6 = \{e\} \cup \{r, r^2\} \cup \{s\} \cup \{rs, r^2s\}.$$

  This can be proved by exhaustion; in other words, just check all possible conjugates of everything! You will need the rules: $r^3 = e$, $s^2 = e$ and $srs = r^{-1} = r^2$. As an example:

  $$\begin{aligned} [r] &= \{ere^{-1}, rrr^{-1}, r^2r(r^2)^{-1}, srs^{-1}, (rs)r(rs)^{-1}, (r^2s)r(r^2s)^{-1}\} \\ &= \{r, r, r, r^2, r^2, r^2\} \\ &= \{r, r^2\}. \end{aligned}$$

- We can also work out a few stabilisers:

  $$C_{D_6}(e) = G, \quad C_{D_6}(r) = \{e, r, r^2\}, \quad C_{D_6}(s) = \{e, s, r^2s\}$$

  This was also done by exhaustion.

- The centre of this group is $Z(D_{2n}) = \{e\}$. To prove this, we give counterexamples to each other element being in the centre
  - $sr = r^2s \neq rs$, so neither s nor r are in the centre.
  - $(rs)r = r(sr) = r(r^2s) = s \neq r(rs)$ so rs is not in the centre.
  - $(r^2s)r = r^2(sr) = r^2(r^2s) = rs \neq s = r(r^2s)$ so r^2s is not in the centre.

It also possible to conjugate an entire subgroup all at once, as follows.

Definition 4.37. Let $H \leq G$ and $g \in G$. Then the *conjugate of H by g* is

$$gHg^{-1} := \{b \in G \mid b = g \cdot h \cdot g^{-1} \text{ for some } h \in H\}.$$

Lemma 4.38. *The conjugate of a subgroup $H \leq G$ by an element $g \in G$ is again a subgroup $gHg^{-1} \leq G$. The order of H is the same as the order of gHg^{-1}.*

Example 4.39. As D_6 is order 6, any proper subgroup must have order 2 or 3 by Lagrange's Theorem. As these number are prime, any subgroup is cyclic. Thus, by inspecting the orders of the elements, we have that a complete list of subgroups of D_6 is

$$\{e\}, \quad E = \{e, r, r^2\}, \quad F = \{e, s\}, \quad H = \{e, rs\}, \quad J = \{e, r^2 s\}, \quad D_6.$$

Conjugation of a subgroup is again a subgroup, and of the same order. We can do some ad hoc computations.

- The subgroup $\{e, r, r^2\}$ can only be conjugated to itself because the order of a subgroup is preserved under conjugation and this is the only subgroup of order 3.
- We have $sHs^{-1} = s\{e, rs\}s^{-1} = \{ses^{-1}, srss^{-1}\} = \{e, r^2 s\} = J$.
- We have $rHr^{-1} = r\{e, rs\}r^{-1} = \{rer^{-1}, rrsr^{-1}\} = \{e, r^2 sr^2\} = \{e, r^2 rs\} = \{e, s\} = F$.

So any of the order 2 subgroups F, H, J can be conjugated to any of the others. For example

$$\begin{aligned} & r^{-1}Fr = H = s^{-1}Js \\ \implies & F = rs^{-1}Jsr^{-1} = (rs)J(rs)^{-1}. \end{aligned}$$

The conjugacy class $[a]$ of $a \in G$ is the set of elements conjugate to a and is equal to the orbit of a. The centraliser is the stabiliser of the action. Thus the following is a direct application of the Orbit-Stabiliser Theorem to the conjugation action.

Proposition 4.40. *For $a \in G$ a finite group, the number of conjugates of a is the index of its centraliser*

$$|G : C_G(a)| = \#\text{ elements conjugate to } a.$$

Any group action partitions the set being acted on into orbits. For the conjugation action on a finite group, a quick analysis of these orbits results in a powerful way of thinking about the order of a group and how the group decomposes.

Theorem 4.41 (The Class Equation)**.** *Let G be a finite group and let $g_1, \ldots, g_r$ be representatives of the distinct conjugacy classes of G that are not contained in the centre $Z(G)$. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

If $a \in Z(G)$, its only conjugate is itself, so the conjugacy class is a singleton $[a] = \{a\}$. The setup of the theorem is just trying to separate out the size 1 conjugacy classes from the conjugacy classes of larger size, represented by $g_1, \ldots, g_r$.

Remark 4.42. Here are some basic observations.

- The order $|Z(G)|$ divides $|G|$, by Lagrange's Theorem. The indices of subgroups divide $|G|$, again by Lagrange's Theorem. Thus the RHS of the class equation is a partition of the number $|G|$ by numbers dividing $|G|$.
- For all $i = 1, \ldots, r$, we have

$$1 < |G : C_G(g_i)| < |G|$$

  (this is an exercise...). In other words, $|G : C_G(g_i)|$ are not just any divisors, but must be *proper* divisors of $|G|$.
- G is abelian if and only if $r = 0$ in the class equation.

Here is an pleasing application.

Lemma 4.43. *If $|G| = p^a$ for p prime and $a > 0$. Then $Z(G) \neq \{e\}$.*

Proof. Consider the LHS of the class equation is divisible by p, which implies the RHS is also. But then $|G : C_G(g_i)|$ is divisible by p for all i. Hence $|Z(G)|$ is divisible by p. So $Z(G) \neq \{e\}$. □

The previous lemma has a really nice consequence, which is good enough to be stated as a theorem.

Theorem 4.44. *If $|G| = p^2$ for some prime p then*

$$G \cong C_{p^2} \qquad \text{or} \qquad G \cong C_p \times C_p.$$

We now know every group of order 9 is isomorphic to either C_9 or $C_3 \times C_3$, so our classification of groups of small order just advanced one notch!

5 *Symmetric and alternating groups*

Permutations, cycles and transpositions

We now begin a study of the symmetric group on n letters, the group of permutations of the numbers $1, \ldots, n$.

$$\begin{aligned} S_n &:= \mathrm{Sym}(\{1, \ldots, n\}) \\ &= \{\sigma \colon \{1, \ldots, n\} \to \{1, \ldots, n\} \mid \sigma \text{ is a bijection}\}. \end{aligned}$$

Here are the elementary tools for describing the symmetric group.

Definition 5.1. An ordered list of distinct elements $a_1, \ldots, a_k \in \{1, \ldots, n\}$ determines type of permutation called a *k-cycle*, written as

$$(a_1 a_2 \ldots a_k) \in S_n,$$

and defined as the permutation that maps

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$$

and fixes all other elements of $\{1, \ldots, n\}$.
A 2-cycle (ab) is called a *transposition* as it switches a and b and fixes all other elements.
If the subsets $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_\ell\}$ of $\{1, \ldots, n\}$ are disjoint sets, we call the corresponding cycles $(a_1 \ldots a_k)$ and $(b_1 \ldots b_\ell)$ *disjoint*.

Remark 5.2. A cycle is just a specific notation for a certain bijective function

$$\sigma \colon \{1, \ldots, n\} \to \{1, \ldots, n\}.$$

As such, cycles can be composed, like functions. The rules/notation for composition are the same as for functions; we compose right-to-left and plug in domain elements $i \in \{1, \ldots, n\}$ to the right of the composition.

Example 5.3. For example, in S_4, we have

$$(12)(234) \colon \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}.$$

Computing:

$$\begin{aligned}((12)(234))(1) &= (12)((234)(1)) = (12)(1) = 2,\\ ((12)(234))(2) &= (12)((234)(2)) = (12)(3) = 3,\\ ((12)(234))(3) &= (12)((234)(3)) = (12)(4) = 4,\\ ((12)(234))(4) &= (12)((234)(4)) = (12)(2) = 1.\end{aligned}$$

So we could alternatively have written the composition of those cycles as one single cycle $(12)(234) = (1234)$.

Let's do another one. Consider the composition

$$(1234)(321)\colon \{1,2,3,4\} \to \{1,2,3,4\}.$$

Computing:

$$\begin{aligned}((1234)(321))(1) &= (1234)((321)(1)) = (1234)(3) = 4,\\ ((1234)(321))(1) &= (1234)((321)(2)) = (1234)(1) = 2,\\ ((1234)(321))(1) &= (1234)((321)(3)) = (1234)(2) = 3,\\ ((1234)(321))(1) &= (1234)((321)(4)) = (1234)(4) = 1.\end{aligned}$$

So we could alternatively have written the composition of those cycles as one single cycle $(1234)(321) = (14)$.

Let's do another one. Consider the composition

$$(321)(1234)\colon \{1,2,3,4\} \to \{1,2,3,4\}.$$

Computing:

$$\begin{aligned}((321)(1234))(1) &= (321)((1234)(1)) = (321)(2) = 1,\\ ((321)(1234))(1) &= (321)((1234)(2)) = (321)(3) = 2,\\ ((321)(1234))(1) &= (321)((1234)(3)) = (321)(4) = 4,\\ ((321)(1234))(1) &= (321)((1234)(4)) = (321)(1) = 3.\end{aligned}$$

So we could alternatively have written the composition of those cycles as one single cycle $(321)(1234) = (34)$.

Remark 5.4. The examples above show that generally S_n is not abelian.

Lemma 5.5. *Let $n \in \mathbb{N}$.*

(i) CYCLES CAN BE CYCLED
For any cycle $(a_1 \dots a_k) \in S_n$, we have

$$(a_1 a_2 \dots a_{k-1} a_k) = (a_2 a_3 \dots a_k a_1).$$

(ii) DISJOINT CYCLES COMMUTE
For any disjoint cycles $(a_1 \dots a_k), (b_1 \dots b_\ell) \in S_n$, we have

$$(a_1 \dots a_k)(b_1 \dots b_\ell) = (b_1 \dots b_\ell)(a_1 \dots a_k).$$

Corollary 5.6. *If $\sigma_1, \dots, \sigma_m \in S_n$ are pairwise disjoint cycles, then*

$$(\sigma_1\sigma_2\dots\sigma_m)^k = (\sigma_1)^k(\sigma_2)^k\dots(\sigma_m)^k.$$

Theorem 5.7 (Disjoint cycle decomposition)**.** *Every $\sigma \in S_n$ is a composition of disjoint cycles. Moreover, when σ is written as a composition of disjoint cycles, this expression is unique, up to*

(i) reordering the disjoint cycles in the composition and

(ii) cycling a given cycle composition.

We cannot expect actual uniqueness of the disjoint cycle expression.
(i) is saying we have to allow for e.g. $(123)(456) = (456)(123)$
(ii) is saying we have to allow for e.g. $(123)(456) = (231)(456)$.
The theorem is saying that other than these ambiguities, the expression is unique.

Notation 5.8. A *partition* of $n \in \mathbb{Z}^{>0}$ is a non-decreasing sequence $a_1, \dots, a_k \in \mathbb{Z}^{>0}$ such that

$$a_1 + a_2 + \dots + a_k = n.$$

For example,

$$1+1+1+2+3 = 8,$$

so $1, 1, 1, 2, 3$ is a partition of 8.

The *partition function* $p(n)$ counts the number of partitions of n. For example $n = 4$ can be partitioned as

$1+1+1+1$,
$1+1+2$,
$1+3$,
$2+2$,
4.

So $p(4) = 5$. There is no known formula for $p(n)$, but, as you can imagine, it is an extremely well-studied function. The first few values are $p(n) = 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, \dots$.

Example 5.9. Suppose we have written $\sigma \in S_9$ as the composition of disjoint cycles

$$\sigma = (12)(675)(93).$$

We don't usually write the 1-cycles in, but let's do it in this example:

$$\sigma = (12)(675)(93)(4)(8).$$

There are two 1-cycles, two 2-cycles and one 3-cycle. This determines a partition

$$1+1+2+2+3 = 9.$$

Theorem 5.7 justifies that this way of assigning a partition to a permutation is a well-defined assignment, justifying the following.

Definition 5.10. We call the partition of n associated to a disjoint cycle decomposition of $\sigma \in S_n$ its *cycle type*.

Example 5.11.

- $(12) \in S_4$ has cycle type $1, 1, 2$.
- $(12)(34) \in S_4$ has cycle type $2, 2$.
- $(12) \in S_7$ has cycle type $1, 1, 1, 1, 1, 2$.
- $(12)(34) \in S_7$ has cycle type $1, 1, 1, 2, 2$.
- $(123)(456)(78) \in S_9$ has cycle type $1, 2, 3, 3$.

Note that $(12) \in S_4$ and $(12) \in S_7$ have different cycle types!

Also, remember you have to add in the 1-cycles that we usually suppress from our notation.

The numbers in the cycle type add up to the n in the S_n!

The cycle type can be used to determine the order of a permutation, as we now investigate.

Example 5.12. Suppose that $\sigma \in S_9$ can be written as

$$\sigma = (12)(345)(6789).$$

Let's find the order of σ, the lowest $k \in \mathbb{N}$ such that $\sigma^k = \mathrm{Id}$.

$$\begin{aligned}
\sigma^2 &= ((12)(345)(6789))^2 = (12)^2(345)^2(6789)^2 = \mathrm{Id} \circ (354)((68)(79)),\\
\sigma^3 &= ((12)(345)(6789))^3 = (12)^3(345)^3(6789)^3 = (12) \circ \mathrm{Id} \circ (6987),\\
\sigma^4 &= ((12)(345)(6789))^4 = (12)^4(345)^4(6789)^4 = \mathrm{Id} \circ (345) \circ \mathrm{Id},\\
&\vdots
\end{aligned}$$

As the disjoint cycles are not interating with each other, to find the order of σ, we will need the least power k so that

$$(12)^k = \mathrm{Id}, \quad (345)^k = \mathrm{Id}, \quad \text{and} \quad (6789)^k = \mathrm{Id}\,.$$

Hence the order is the least common multiple of the cycle lengths. In this case, that number is $\mathrm{lcm}(2,3,4) = 12$.

Lemma 5.13. *The order of $\sigma \in S_n$ is equal to the lowest common multiple of the lengths of the disjoint cycles in a disjoint cycle decomposition for σ.*

The sign of a permutation

It is pretty straightforward to decompose a k-cycle into $k-1$ (non-disjoint) transpositions. For instance, you can check this works:

$$(123456) = (12)(23)(34)(45)(56).$$

This can be done completely generally.

Proposition 5.14. *Every permutation is a composition of transpositions.*

This decomposition is highly non-unique. For example

$$\begin{aligned}
(123456) &= (12)(23)(34)(45)(56)\\
&= (61)(12)(23)(34)(45)\\
&= (61)(12)(23)(34)(45)(23)(23)
\end{aligned}$$

This example shows the 2-cycles in the composition are not unique, and the number of 2-cycles in the composition is not unique. However, it turns out that at least the number of 2-cycles is well-defined modulo 2.

Theorem 5.15. *Suppose $\sigma \in S_n$ can be written as a product of k transpositions and a product of ℓ transpositions, then either k and ℓ are both odd or are both even.*

This allows the following definition.

Definition 5.16. Given $\sigma \in S_n$, let k be the number of transpositions in some decomposition of σ into transpositions. The *sign* of σ is

$$\varepsilon(\sigma) := \begin{cases} +1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd} \end{cases}$$

If $\varepsilon(\sigma) = 1$, we call σ an *even* permutation, and if $\varepsilon(\sigma) = -1$, we call σ an *odd* permutation.

Proposition 5.17. *The sign function $\varepsilon\colon S_n \to \{1, -1\} = C_2$ is a group homomorphism.*

Proposition 5.18. *A k-cycle has sign $(-1)^{k-1}$.*

Example 5.19. The previous two propositions combine to give an effective method for computing the sign of an element $\sigma \in S_n$. First, express σ as a composition of m disjoint cycles $\sigma = \sigma_1 \dots \sigma_m$, where σ_i has length k_i. Then

$$\varepsilon(\sigma) = \varepsilon(\sigma_1) \dots \varepsilon(\sigma_m) = (-1)^{k_1} \dots (-1)^{k_m} = (-1)^{k_1 + \dots + k_m}.$$

I'm sure you can spot some other easy tricks, like "the sign is odd if and only if it has an odd number of odd cycles in the disjoint cycle decomposition".

For example $(123)(4567)(89)$ has sign $(-1)^{3+4+2} = -1$.

We now introduce a new and important type of group.

Definition 5.20. The nth *alternating group* A_n is the subgroup of S_n consisting of all even permutations.

Clearly $A_n \leq S_n$ is indeed a subgroup because it is the kernel of the sign homomorphism. It is also clear that the odd permutations do not form a subgroup of S_n because the identity permutation is not odd.

Observe that $A_n \trianglelefteq S_n$ is normal because it is the kernel of the sign homomorphism. As the sign homomorphism is surjective, we have that

$$S_n / A_n \xrightarrow{\cong} C_2; \qquad \sigma A_n \mapsto \varepsilon(\sigma)$$

is an isomorphism, by The First Isomorphism Theorem. In particular, this shows the alternating group is an index 2 subgroup

$$|S_n : A_n| = |S_n / A_n| = |C_2| = 2.$$

Consequently, we have that

$$|A_n| = \frac{n!}{2}.$$

Conjugation in S_n and the simplicity of A_5

The purpose of this section is to prove that the group A_5 is simple. First, we will prove a refreshingly straightforward result for recognising conjugacy classes of permutations. Let's start with a single cycle.

Proposition 5.21 (CONJUGATING A SINGLE CYCLE). *Given $\sigma \in S_n$ and $(a_1 \dots a_k) \in S_n$, we have*

$$\sigma \circ (a_1 \dots a_k) \circ \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k)).$$

Test the formula out on a couple of examples to get the idea:

$$(13)(1234)(31) = (3214).$$

Corollary 5.22. *Two cycles are conjugate if and only if they have the same length.*

Example 5.23. I want to conjugate (1234) to (2794) in S_9. I should just compare the entries I see in two cycles and define a permutation τ sending the entries one to the other:

$$\tau(1) = 2, \quad \tau(2) = 7 \quad \tau(3) = 9 \quad \tau(4) = 4, \quad \text{otherwise } \tau(i) = i.$$

Then

$$\tau \circ (1234) \circ \tau^{-1} = (2794) \in S_9.$$

This is easily adapted to a complete characterisation of conjugacy in symmetric groups in terms of cycles-type.

Corollary 5.24 (CONJUGACY CRITERION FOR PERMUTATIONS).

(i) Two permutations in S_n are conjugate if and only if they have the same cycle type.

(ii) The number of conjugacy classes in S_n is equal to the number of partitions of n.

Example 5.25. I can conjugate any two cycles in S_9 with the same cycle-type to one another. The procedure is the same as for a single cycle: I should just compare the entries I see and define a permutation τ sending the entries in corresponding disjoint cycles to one-another.
For example, to conjugate $(97)(1234)(568)$ to $(12)(3456)(789)$, I could use

$$\begin{array}{lllllllll} \tau(1) & = & 3, & \tau(2) & = & 4, & \tau(3) & = & 5, \\ \tau(4) & = & 6, & \tau(5) & = & 7, & \tau(6) & = & 8, \\ \tau(7) & = & 9, & \tau(8) & = & 2, & \tau(9) & = & 1. \end{array}$$

Then

$$\tau \circ (97)(1234)(568) \circ \tau^{-1} = (12)(3456)(789).$$

We now embark on a quest to prove that the group A_5 is simple, i.e. has no nontrivial normal subgroups. This can be attacked by thinking about conjugacy classes for the following reason.

Proposition 5.26. *If $H \trianglelefteq G$ is a normal subgroup and $[a]$ is a conjugacy class, then either $[a] \subseteq H$ or $[a] \cap H = \emptyset$.*

Corollary 5.27. *If $H \trianglelefteq G$ is a normal subgroup, then there is a disjoint union $H = \bigcup_{a \in H} [a]$.*

Example 5.28. The possible cycle types, and therefore conjugacy classes, in S_5 are given by the partitions

$$\begin{aligned} &1,1,1,1,1,\\ &1,1,1,2,\\ &1,1,3,\\ &1,4,\\ &5,\\ &1,2,2,\\ &2,3 \end{aligned}$$

Thus S_5, which has order $5! = 120$, has exactly 7 conjugacy classes.

Hence, the possible cycle types in A_5 are given by the partitions

$$\begin{aligned} &1,1,1,1,1,\\ &1,1,3,\\ &5\\ &1,2,2 \end{aligned}$$

because these are the ones generating even cycles. Let's choose representatives

$$\mathrm{Id}, \qquad (123), \qquad (12345), \qquad (12)(34).$$

WARNING! Just because elements σ_1, σ_2 with the same cycle type are conjugate in S_n, does NOT make them conjugate in A_n.

The issue is the element τ you used to conjugate $\tau\sigma\tau^{-1} = \sigma_2$, might not be an element of A_n.

We now investigate the conjugacy classes in A_5 for cycles of the type above.

Lemma 5.29. *All twenty* 3*-cycles in* A_5 *are conjugate to one-another.*

Lemma 5.30. *The twenty-four* 5*-cycles in* A_5 *lie in two distinct conjugacy classes (which are each then of size twelve).*

Lemma 5.31. *All fifteen elements with cycle type* $2,2$ *are conjugate to one-another in* A_5*.*

In summary, there are exactly **five** conjugacy classes in A_5. They have sizes

$$1, \quad 12, \quad 12, \quad 15, \quad 20.$$

Proposition 5.32. A_5 *is simple.*

Proof. Suppose $H \trianglelefteq A_5$ is a normal subgroup. Then H is a (disjoint) union of conjugacy classes, and the union certainly includes the identity conjugacy class $[e] = \{e\}$. Moreover $|H|$ divides $|A_5| = 60$ by Lagrange's Theorem. The reader can now check that the only way to express a divisor of 60 as a sum of 1 and some subcollection of the numbers $12, 12, 15, 20$ is if $|H| = 1$ or if $|H| = 1 + 12 + 12 + 15 + 20 = 60$. As this gives $H = \{e\}$ or $H = A_5$, we conclude A_f has no proper normal subgroup. □

Remark 5.33. The same sort of proof works to show A_6 is simple. The combinatorics get a little hairy if you try and repeat the argument for larger alternating groups.

Remark 5.34. In fact, A_n is simple for all $n \geq 5$. We sketch a common way to prove this.

- Prove that for $n \geq 5$ any two 3-cycles are conjugate.
- Prove that for $n \geq 3$ the group A_n is generated by 3-cycles.
- Prove that for $n \geq 5$ every nontrivial normal subgroup of A_n contains a 3-cycle.

Putting this together, if $H \trianglelefteq A_n$ is normal, it must contain a 3-cycle. But then it must contain the entire conjugacy class of the 3-cycle. But the conjugacy class is the whole group $A_n \subseteq H \subseteq A_n$. Thus the only normal subgroups of A_n are $\{e\}$ and A_n.

6 Fundamental Theorem of Abelian Groups

We do not have time to treat this topic properly, with proofs, but it is such an important idea that I wanted to sketch it out.

Fundamental Theorem of Finitely Generated Abelian Groups

Definition 6.1. A group G is *finitely generated* if there exists a subset $S \subseteq G$ such that every element of G can be written as a word in the elements of S.

Definition 6.2. A finitely generated group G is *free abelian* if it is isomorphic to *the free abelian group of rank r*

$$\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}.$$

It is an exercise to show that the rank of a free abelian group is well-defined. In other words, that if $\mathbb{Z}^r \cong \mathbb{Z}^s$ then $r = s$.

In this case, we call r the *rank* of G.

Theorem 6.3. *Every finitely generated abelian group G is isomorphic to the product of a free abelian group and some number of finite cyclic groups.*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s},$$

for some $r \geq 0$ and $d_1, \ldots, d_s \geq 2$.

Moreover:

(i) The integers d_i can be chosen so that d_{i+1} divides d_i for all $1 \leq i \leq s-1$.

(ii) The list of integers $r, d_1, \ldots, d_s$ satisfying $r \geq 0$, $d_1, \ldots, d_s \geq 2$ and (i) is unique.

Example 6.4. The decomposition is not unique without the divisibility condition on the torsion part. We know from the Chinese Remainder Theorem that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ when m and n are coprime.
For example, consider the group of order 60

$$G = \mathbb{Z}_{60} \cong \mathbb{Z}_4 \times \mathbb{Z}_{15} \cong \mathbb{Z}_{12} \times \mathbb{Z}_5 \cong \mathbb{Z}_{20} \times \mathbb{Z}_3,$$

and the "unique" expression from the theorem is just $G = \mathbb{Z}_{60}$.
On the other hand, consider the order 60 group $G \neq H$ given by

$$H = \mathbb{Z}_2 \times \mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_6 \times \mathbb{Z}_{10}.$$

The "unique" expression from the theorem is $H = \mathbb{Z}_{30} \times \mathbb{Z}_2$.

Combining The Fundamental Theorem of Finitely Generated Abelian Group with the Chinese Remainder Theorem we can break up the d_i as far as they can go, to get.

Corollary 6.5. *Suppose $n \in \mathbb{Z}^{>0}$. Then every finite abelian group of order n is isomorphic to*

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

where each of n_i is a power of one of the distinct primes dividing $p_1, \ldots, p_r$ that divide n (and necessarily $n = n_1 \ldots n_k$).

If you express a finite abelian group as a product of cyclic groups of prime power order, then the prime powers $n_1, \ldots, n_k$ are unique, up to reordering. This follows from the uniqueness component of Theorem 6.3.

So to find all possible finite abelian groups of a given order n, we have to work out all possible ways to separate n into products of prime powers $n = n_1 \ldots n_k$. For example $n = 18$ has

$$18 = 9 \times 2 = 3 \times 3 \times 2.$$

So there are 3 finite abelian groups of order 18.

Example 6.6. Let's find all finite abelian groups of order

$$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5.$$

As $360 = 2^3 \cdot 3^2 \cdot 5$, the possible groups correspond to the different ways of partitioning the exponents of the primes 2 and 3 to form the $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ from Corollary 6.5.

$$2 \cdot 2 \cdot 2 = 2 \cdot 2^2 = 2^3 \quad \text{and} \quad 3 \cdot 3 = 3^2.$$

Giving six possible combinations

$$\begin{aligned}
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\quad (\cong \mathbb{Z}_{30} \times \mathbb{Z}_6 \times \mathbb{Z}_2),\\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 &\quad (\cong \mathbb{Z}_{90} \times \mathbb{Z}_2 \times \mathbb{Z}_2),\\
\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\quad (\cong \mathbb{Z}_{60} \times \mathbb{Z}_6),\\
\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 &\quad (\cong \mathbb{Z}_{180} \times \mathbb{Z}_2),\\
\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\quad (\cong \mathbb{Z}_{120} \times \mathbb{Z}_3),\\
\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 &\quad (\cong \mathbb{Z}_{360}).
\end{aligned}$$

On the RHS we give the "unique" expression predicted by the FTFGAG, where d_{i+1} divides d_i.

Remark 6.7. Expressing the order of a finite abelian group G in terms of powers of distinct primes

$$|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

and writing $p(N)$ for the number of integer partitions of an integer N, we can count that there are

$$p(\alpha_1)p(\alpha_2)\cdots p(\alpha_r)$$

possible groups G could be.

7 *Rings*

Groups were, in some sense, just giving a name to an extremely common algebraic structure found all over mathematics. In particular, they capture the additive structure in number systems like $\mathbb{Z}$ and $\mathbb{Q}$ etc. We now introduce a second binary operation into the mix, to study the kind of algebraic structure that arises when $+$ and $\times$ interact in number systems.

Rings - definitions

Definition 7.1. A *ring* is a quintuple $(R, +, \cdot, 0_R, 1_R)$, consisting of a set R, binary operations $+$ and $\cdot$ on R, and elements $0_R, 1_R \in R$ such that

(i) The triple $(R, +, 0_R)$ is an abelian group. ADDITIVE GROUP

(ii) For all $a, b, c \in R$, we have MULTIPLICATIVE ASSOCIATIVITY

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(iii) For all $a \in G$, we have MULTIPLICATIVE IDENTITY

$$a \cdot 1_R = 1_R \cdot a = a.$$

(iv) For all $a, b, c \in R$, we have DISTRIBUTIVITY

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Some authors do not insist that a ring has a multiplicative identity and call what we are defining a "ring with unity" or "unital ring". We are going to stay away from this can of worms...

WARNING! The triple $(R, \cdot, 1_R)$ is NOT generally a group. Elements may fail to have multiplicative inverses.

It is an amusing exercise to prove the assumption that the group $(R, +, 0_R)$ is abelian is in fact redundant. The trick is to compute $(1 + 1)(a + b)$ in two ways. First, distribute in the order "left parenthesis then right parenthesis". Second, distribute in the order "right parenthesis then left parenthesis". Comparing the two answers, try to deduce $a + b = b + a$.

CONVENTION

We will generally not specify the full quintuple $(R, +, \cdot, 0_R, 1_R)$ unless we need to, for clarity; we will simply write "R".

We will abbreviate multiplication $a \cdot b = ab$ and abbreviate $0 = 0_R$ and $1 = 1_R$, unless we need to be more specific, for clarity.

Here are some intuitively sensible arithmetic properties of rings.

Proposition 7.2. *Let R be a ring.*

(i) For all $a \in R$, we have $0 \cdot a = a \cdot 0 = 0$.

(ii) For all $a, b \in R$, we have $(-a)b = a(-b) = -(ab)$.

(iii) For all $a, b \in R$, we have $(-a)(-b) = ab$.

(iv) For all $a \in R$, we have $-a = (-1)a$.

(v) The identity $1_R \in R$ is unique.

Proof. Here is the proof of (i) to give you the flavour of the care required in these tedious arguments:

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a \\ &= (0 \cdot a) + (0 \cdot a) \end{aligned}$$

Now subtract $0 \cdot a$ from both sides, to get

$$(0 \cdot a) - (0 \cdot a) = (0 \cdot a) + (0 \cdot a) - (0 \cdot a).$$

Hence $0 = 0 \cdot a$.
We leave it to the reader to go through the remaining proofs for themselves. □

Definition 7.3. A ring R is *commutative* is $a \cdot b = b \cdot a$ for all $a, b \in R$.

Non-commutative ring theory is *much* more difficult than commutative ring theory. In this course we will give a few examples of non-commutative rings, so you have seen them, but we will never make a proper study of them.

Definition 7.4. Let $(R, +, \cdot, 0_R, 1_R)$ be a ring and $S \subseteq R$ be a subset. The S is a *subring* of R if $0_R, 1_R \in S$ and the operations $+$ and $\cdot$ make $(S, +, \cdot, 0_R, 1_R)$ into a ring. In this case we write $S \leq R$.

First examples

Example 7.5. The 0-*ring* is the ring $R = \{0\}$, where we set $1 = 0$, $0 + 0 = 0$ and $0 \cdot 0 = 0$.
In fact, suppose R is any ring in which $1_R = 0_R$. Then for all $a \in R$ we have $a = 1_R \cdot a = 0_R \cdot a = 0_R$. So

$$1_R = 0_R \quad \iff \quad R \text{ is the 0-ring.}$$

Example 7.6. The number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all commutative rings with the usual 0 and 1. They are moreover subrings of each other as $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Example 7.7. Let $n \in \mathbb{Z}^{>0}$ and $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. This is an abelian group under the operation $+_n$. Define $a \times_n b$ to be the remainder of ab on division by n. Then $(\mathbb{Z}_n, +_n, \times_n, 0, 1)$ is a commutative ring.

Exercise: verify that the "freshman's dream" $(a+b)^2 = a^2 + b^2$ holds true in the ring $\mathbb{Z}_2$.

Example 7.8. Ordinary addition and multiplication of matrices makes the set $\mathrm{Mat}_n(R)$ of $n \times n$ matrices with entries in $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ is a ring. It is not a commutative ring when $n \geq 2$.

Indeed, for any ring R, the $n \times n$ matrices $\mathrm{Mat}_n(R)$ are a ring, as we discuss later.

Example 7.9. Let X be any set and A be any ring. Then the set of all functions $f\colon X \to A$ is a ring, where addition and multiplication are defined "pointwise"; that is, the functions $f+g$ and $f \cdot g$ are defined at $x \in X$ by the formulas

$$(f+g)(x) := f(x) + g(x), \quad \text{and} \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

The additive identity is the 0-function $f(x) := 0_A$ for all $x \in X$. The multiplicative identity is the function $f(x) := 1_A$ for all $x \in X$.
This ring is commutative if and only if A is commutative.

Zero divisors and domains

WARNING! If a ring has 0-divisors you cannot casually get to $ab = 0$ in some algebra, and conclude $a = 0$ or $b = 0$. That's kind of the point!

Definition 7.10. A *zero divisor* is an element $a \in R$ such that $ab = 0$ or $ba = 0$ for some $b \neq 0$.

A ring with no zero divisors other than 0 is called a *domain*.

A commutative domain is called an *integral domain*.

Example 7.11. The integers, of course, $\mathbb{Z}$ are an integral domain. Moreover, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains.

Example 7.12. For p prime, $\mathbb{Z}_p$ is an integral domain. To see this, suppose $a, b \in \mathbb{Z}_p$ and $a \times_p b = 0$. Then ab is a multiple of p. But then as p is prime, p must divide a or b. Hence $a = 0$ or $b = 0$.

Example 7.13. For n not prime, $\mathbb{Z}_n$ is not a domain. For example, in $\mathbb{Z}_4$ we have that $2 \times_n 2 = 0$. Generally, we have that if $n = rs$ for $r, s \in \mathbb{Z}_n$ and $r, s \neq 1$, then both r and s are zero divisors, as $r \times_n s = 0$.

Example 7.14. The 2×2 integral matrices $\mathrm{Mat}_2(\mathbb{Z})$ are not a domain. For example

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

Units and division rings

WARNING! Be careful about the context, when thinking about units. For example $2 \in \mathbb{Z}$ is not a unit, but $2 \in \mathbb{Q}$ is a unit.

Definition 7.15. A *unit* is an element $a \in R$ such that there exists $b \in R$ with $ab = 1$ or $ba = 1$.

A ring where every non-zero element is a unit is called a *division ring*.

A commutative division ring is called a *field*.

Notation 7.16. The set of units in a ring is denoted

$$R^\times = \{a \in R \mid ab = 1 \text{ or } ba = 1 \text{ for some } b \in R\}.$$

Observe that if $\mathbb{F}$ is a field, then $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.

Exercise 7.1. The set of units of a ring R forms a group using the multiplication from the ring $(R^\times, \cdot, 1_R)$.

Example 7.17. The ring $\mathbb{Z}$ is not a division ring (and thus not a field). The group of units is $\mathbb{Z}^\times = \{-1, 1\} = C_2$.
The rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

Example 7.18. For p prime, $\mathbb{Z}_p$ is a field. To prove this, let $a \in \{2, \ldots, p-1\}$. Then a is coprime to p and so, by Bezout's Theorem, there exist integers x and y such that

$$ax + py = 1.$$

Let $b \in \mathbb{Z}_p$ be the remainder of x upon division by p, so that $x = pq + b$. Then

$$1 = a(pq + b) + py = ab + p(aq + y).$$

This implies $a \times_p b = 1$, so a is a unit.

Example 7.19. When n is composite, $\mathbb{Z}_n$ is not a division ring (and thus not a field). The units in this ring are

$$(\mathbb{Z}_n)^\times = \{a \in \mathbb{Z}_n \mid a \text{ is coprime to } n\}.$$

To see these are units, follow the proof from the previous example to obtain a multiplicative inverse.

Now to see these are all the units, suppose $a \in \mathbb{Z}_n$ where a and n have a prime factor in common, say $n = px$ and $a = py$ for some prime p. Suppose, for a contradiction, that $a \times_n b = 1$ for some $b \in \mathbb{Z}_n$. Then $ab = nq + 1$ for some q. Then $pyb = pxq + 1$. But then $p(yb - xq) = 1$, which is a contradiction as p cannot divide 1.

Comparing Examples 7.13 and 7.19, we get the following.

Proposition 7.20. *The set of non-units in $\mathbb{Z}_n$ is equal to the set of zero divisors.*

Example 7.21. For example, the units in $\mathbb{Z}_8$ are $1, 3, 5, 7$ and the zero divisors are $0, 2, 4, 6$.

Verifying:

$2 \times_8 4 = 0$ and $6 \times_8 4 = 0$.

$3 \times_8 3 = 1$, $5 \times_8 5 = 1$ and $7 \times_8 7 = 1$.

Proposition 7.22 (Fields have no zero divisors)**.** *A zero divisor can never be a unit. In particular, fields have no zero divisors.*

Proposition 7.23 (CANCELLATION PROPERTY)**.** *If $a, b, c \in R$ and a is not a zero-divisor, then*

$$ab = ac \quad \Longrightarrow \quad b = c.$$

Corollary 7.24. *Finite integral domains are fields.*

Rings - more examples

Polynomial rings

Let R be a commutative ring and x be a "indeterminate". A finite "formal sum"

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

is called a *polynomial* in x with *coefficients* $a_i \in R$. All the familiar language applies:

- The integer $n \geq 0$ is the *degree* of the polynomial $\deg(p) = n$.
- The polynomial is *constant* if it is degree 0
- If $a_n \neq 0$, this is called the *leading coefficient*.
- The polynomial is *monic* if the leading coefficient is 1.

If we want to be (perversely) rigorous, the "indeterminate" and "formal sum" are really just book-keeping devices and a polynomial is an $(n+1)$-tuple $(a_n, a_{n+1}, \ldots, a_0) \in R^{n+1}$. The advantage of phrasing this as a polynomial is that the addition and multiplication are MUCH more intuitive if we do so!

Note that this formal perspective emphasises the usual rule that there is equality of polynomials

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} \cdots + a_0 \\ &\qquad = b_n x^n + b_{n-1}x^{n-1} + \ldots b_0 \end{aligned}$$

if and only if $a_i = b_i$ for all $i = 0, 1, \ldots, n$.

Definition 7.25. Let R be a commutative ring and x be an indeterminate. Then we write

$$R[x] = \{p(x) \mid p(x) \text{ is a polynomial in } x \text{ with coefficients in } R\}.$$

Proposition 7.26. *The set of polynomials $R[x]$ is a (commutative) ring using usual multiplication and addition rules for polynomials, together with the additive identity the 0-polynomial and the multiplicative identity the 1-polynomial.*

The 0-*polynomial* is the constant polynomial with coefficient 0. The 1-*polynomial* is the constant polynomial with coefficient 1.

Polynomials are "formal sums". We are NOT thinking of polynomials as functions $p\colon R \to R$ where you are meant to plug in values for the indeterminate x. If we were, then weird things would happen, like $p(x) = x^2 + x \in \mathbb{Z}_2[x]$ would be the 0-function, because $p(0) = 0$ and $p(1) = 1 + 1 = 0$, but it is not the 0-polynomial.

Example 7.27. Whenever we have a subring $S \leq R$ of a commutative ring R, we have subrings $S[x] \leq R[x]$.
In particular, we have a chain of subrings $\mathbb{Z}[x] \leq \mathbb{Q}[x] \leq \mathbb{R}[x] \leq \mathbb{C}[x]$.

Example 7.28. In the polynomial ring $\mathbb{Z}_3[x]$, the coefficients can only have the value 0, 1 or 2, and any addition or multiplication of coefficients must be reduced modulo 3. For example

$$(x^4 + x^3 + x^2 + x + 2) + (2x + 2) = x^4 + x^3 + x^2 + 1$$

and

$$\begin{aligned} &(x^4 + x^3 + x^2 + x + 2)(2x + 2) \\ &= 2x(x^4 + x^3 + x^2 + x + 2) + 2(x^4 + x^3 + x^2 + x + 1) \\ &= (2x^5 + 2x^4 + 2x^3 + 2x^2 + x) + (2x^4 + 2x^3 + 2x^2 + 2x + 2) \\ &= x^5 + x^4 + x^3 + x^2 + 2. \end{aligned}$$

Proposition 7.29. *If R is an integral domain then $R[x]$ is too.*

Proposition 7.30. *If R is an integral domain then:*

(i) *If* $p, q \neq 0$ *then* $\deg(pq) = \deg(p) + \deg(q)$, DEGREE IS ADDITIVE

(ii) $(R[x])^\times = R^\times$. ONLY CONSTANTS CAN BE UNITS

Remark 7.31. It is very easy to introduce more and more polynomial variables:

$$R[x,y] := (R[x])[y], \qquad R[x,y,z] := (R[x,y])[z], \qquad \text{etc.}$$

If R is an integral domain, then so is $R[x_1, x_2, \ldots, x_n]$ for all n.

Matrix rings

Let R be any ring and let $a_{ij} \in R$ for $i, j \in \{1, \ldots, n\}$. Then we write

$$[a_{ij}] = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

and call this an $n \times n$ matrix with entries/coefficients in R. We write

$$\mathrm{Mat}_n(R) := \{[a_{ij}] \mid a_{ij} \in R \text{ for all } i, j \in \{1, \ldots, n\}\}.$$

Proposition 7.32. *The set of matrices* $\mathrm{Mat}_n(R)$ *is a ring using the usual multiplication and addition rules for matrices, together with the additive identity the* 0*-matrix and the multiplicative identity the* $n \times n$ *identity matrix*

$$I_{n\times n} = \begin{pmatrix} 1_R & 0_R & \ldots & 0_R \\ 0_R & 1_R & \ldots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \ldots & 1_R \end{pmatrix}$$

Proposition 7.33. *If* R *is commutative and* $A, B \in \mathrm{Mat}_n(R)$ *then* $AB = I$ *if and only if* $BA = I$.

In particular, when R is commutative, it makes sense to call a matrix *invertible*, rather than distinguishing "left invertible" or "right invertible".

Definition 7.34. The group of units of $\mathrm{Mat}_n(R)$ is called the *general linear group* for R and is written

$$\mathrm{GL}_n(R) := \{A \in \mathrm{Mat}_n(R) \mid AB = I \text{ or } BA = I \text{ for some } B \in \mathrm{Mat}_n(R)\}.$$

In particular, if R is commutative then

$$\mathrm{GL}_n(R) := \{A \in \mathrm{Mat}_n(R) \mid A \text{ is invertible}\}.$$

Example 7.35. Whenever we have a subring $S \leq R$ of a commutative ring R, we have subrings $\mathrm{Mat}_n(S) \leq \mathrm{Mat}_n(R)$.
In particular, we have a chain of subrings

$$\mathrm{Mat}_n(\mathbb{Z}) \leq \mathrm{Mat}_n(\mathbb{Q}) \leq \mathrm{Mat}_n(\mathbb{R}) \leq \mathrm{Mat}_n(\mathbb{C})$$

Example 7.36. The subset of upper triangular matrices in any matrix ring $\mathrm{Mat}_n(R)$ is a subring.

8 Homomorphisms, ideals, quotients

Ring homomorphisms

Definition 8.1. A function $\varphi\colon R \to S$ between rings is called a *ring homomorphism* if, for all $a, b \in R$

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ RESPECTS ADDITION

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ RESPECTS MULTIPLICATION

(iii) $\varphi(1_R) = 1_S$ RESPECTS MULTIPLICATIVE UNIT

Remark 8.2. Condition (i) says that φ is an additive group homomorphism. Hence we get for free that $\varphi(0_R) = 0_S$.

Definition 8.3. Let $\varphi\colon R \to S$ be a ring homomorphism.

(i) The *image* of φ is

$$\operatorname{im}(\varphi) := \{s \in S \mid s = \varphi(r) \text{ for some } r \in R\}$$

(ii) The *kernel* of φ is

$$\ker(\varphi) := \{r \in R \mid \varphi(r) = 0_S\}.$$

WARNING! The kernel is defined as the preimage of $0 \in S$, NOT the preimage of $1 \in S$!

Proposition 8.4. *Let $\varphi\colon R \to S$ be a ring homomorphism.*

(i) The subset $\operatorname{im}(\varphi) \leq S$ is a subring.

(ii) The homomorphism φ is injective if and only if $\ker(\varphi) = \{0_R\}$.

The kernel of a ring homomorphism may not contain 1, so is not necessarily a subring.

Definition 8.5. If a ring homomorphism $\varphi\colon R \to S$ is invertible, it is called a ring *isomorphism*. If such a function exists, we say the rings are R and S are *isomorphic* (as rings) and we write $R \cong S$.

Just as for group homomorphisms, the inverse of an invertible ring homomorphism is automatically a ring homomorphism.

Example 8.6. The function

$$q\colon \mathbb{Z} \to \mathbb{Z}_3; \qquad n \mapsto \text{remainder of } n \text{ on division by 3.}$$

is a surjective ring homomorphism. The kernel is $\ker(q) = 3\mathbb{Z}$, which note is not a subring because $1 \notin 3\mathbb{Z}$.

Example 8.7. For any commutative ring R, the *evaluation map* at 0

$$\mathrm{ev}_0 \colon R[x] \to R; \qquad \mathrm{ev}_0(p) := p(0)$$

is a surjective ring homomorphism with kernel

$$\begin{aligned}\ker(\mathrm{ev}_0) &= \{p(x) \mid p(0) = 0\} \\ &= \{a_n x^n + \cdots + a_1 x + a_0 \mid a_0 = 0, n \geq 0\} \\ &= \{p(x) \in R[x] \mid p(x) = xq(x) \text{ for some } q(x) \in R[x]\}.\end{aligned}$$

Example 8.8. Let R be any ring.
The *trace map*

$$\mathrm{tr} \colon M_2(R) \to R; \qquad \mathrm{tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} := a + d$$

is not a ring homomorphism.
The *determinant map*

$$\det \colon M_2(R) \to R; \qquad \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc.$$

is not a ring homomorphism.

Example 8.9. Let $C(\mathbb{R}, \mathbb{R})$ be the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. The *evaluation map* at 0

$$\mathrm{ev}_0 \colon C(\mathbb{R}, \mathbb{R}) \to \mathbb{R}; \qquad \mathrm{ev}_0(f) := f(0)$$

is a ring homomorphism. The kernel is

$$\ker(\mathrm{ev}_0) = \{f \mid f(0) = 0\}.$$

The image is all of $\mathbb{R}$. To see this, let $a \in \mathbb{R}$. Then the constant function $f(x) = a$ for all $x \in \mathbb{R}$ is continuous and $\mathrm{ev}_0(f) = f(0) = a$.

Example 8.10. Let R be any ring. Suppose $\iota \colon \mathbb{Z} \to R$ is a ring homomorphism. Then $\iota(1) = 1_R$. Hence if $n \geq 0$ we have

$$\iota(n) = \iota(1 + 1 + \cdots + 1) = 1_R + 1_R + \cdots + 1_R$$

and similarly if $n \leq 0$ we have

$$\iota(n) = \iota(-1 - 1 + \cdots - 1) = -1_R - 1_R - \cdots - 1_R$$

So ι there is no choice about how to define ι, it is completely determined by the definition of a ring homomorphism.

In other words *there is a unique ring homomorphism from $\mathbb{Z}$ to any ring*.

Ideals and quotient rings

To give the reader a good feel for ring theory, without overcomplicating things, we focus only on commutative rings from now on.

CONVENTION
From this point on all rings are assumed to be commutative.

We now try to generalise the concept of quotient group to the setting of rings. We need to identity the analogous things for normal subgroups.

Let $I \subseteq R$ be a subset that is a subgroup of the additive abelian group $(R, +, 0_R)$. It then makes sense to talk about the *cosets* of I in R, just thinking of them as additive cosets.

Note that as the additive group structure is abelian, we do not have to worry about left vs. right cosets any more; they are the same.

$$R/I := \{r + I \mid r \in R\}.$$

As R is abelian, I is automatically normal as an additive subgroup, so R/I is a quotient group with well-defined addition

$$(r + I) + (s + I) := (r + s) + I.$$

To give it a full ring structure, we would like the following to make sense as a multiplication

$$(r + I)(s + I) := rs + I.$$

Here is the condition that will guarantee our proposed multiplication of cosets is well-defined, independent of the coset representative chosen.

Definition 8.11. A subset $I \subseteq R$ is an *ideal* of R if it satisfies

(i) $(I, +, 0_R) \leq (R, +, 0_R)$ ADDITIVE SUBGROUP

(ii) $rI \subseteq I$ for all $r \in R$ STRONGLY MULTIPLICATIVELY CLOSED

WARNING! If you are reading a text that does not include the requirement that rings have a multiplicative unit, you might read the sentence "ideals are subrings". In our definition, this is not necessarily true! See Corollary 8.16.

Notation 8.12. If $I \leq R$ is an ideal we use the notation $I \trianglelefteq R$.

Remark 8.13. The steps to check a subset $I \subseteq R$ is an ideal:

- Check $0_R \in I$.
- Closed under addition: $a + b \in I$ for all $a, b \in I$.
- Strongly closed under multiplication: $ra \in I$ for all $r \in R$ and $a \in I$.

Note the "strong closure" is stronger than the type of closure you check when seeing if I is a subring. For that you only have to check it is closed under multiplication with other elements from I. Now you have to check I is closed under multiplication by EVERYTHING from the whole ring.

Definition 8.14. An ideal $I \trianglelefteq R$ is *proper* if $I \neq R$.

Lemma 8.15. *If an ideal $I \trianglelefteq R$ contains a unit of R then $I = R$.*

Corollary 8.16. *Proper ideals cannot contain units and therefore cannot be subrings as $1_R \notin I$.*

Corollary 8.17. *A ring R is a field if and only if the only ideals are 0 and R.*

We already have a large source of ideals, coming from the following.

The easiest way to check a subset $I \subseteq R$ is an ideal is to write down a ring homomorphism to another ring $\varphi\colon R \to S$, so that I is the kernel of φ.

Lemma 8.18. *The kernel of a ring homomorphism $\varphi\colon R \to S$ is an ideal $\ker(\varphi) \trianglelefteq R$.*

Theorem 8.19. *If $I \trianglelefteq R$ is an ideal, then the additive cosets R/I form a ring, with addition*

$$(r + I) + (s + I) := (r + s) + I,$$

multiplication

$$(r + I)(s + I) := rs + I,$$

and identities

$$0_{R/I} := 0_R + I, \qquad 1_{R/I} := 1_R + I.$$

Definition 8.20. If $I \trianglelefteq R$ is an ideal, then the group R/I is called the *quotient ring* of R by I.

Example 8.21. The subset $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal for each n

METHOD 1. We already know it is an additive subgroup, so we need to check it is strongly closed under multiplication. Let $r \in \mathbb{Z}$ and $na \in n\mathbb{Z}$. Then $r(na) = n(ra) \in n\mathbb{Z}$. So $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is an ideal.

METHOD 2. A more efficient way, if you can spot it, is to identify (a.k.a. "invent") a ring morphism for which $n\mathbb{Z}$ is the kernel. There is a natural candidate in $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$, where the function takes the remainder on division by n.

Either way, $n\mathbb{Z}$ is an ideal and hence the set of cosets

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

is a ring.

The First Isomorphism Theorem for groups has a version for rings.

Theorem 8.22 (The First Isomorphism Theorem)**.** *Let $\varphi\colon R \to S$ be a ring homomorphism. Then there is a ring isomorphism*

$$\overline{\varphi}\colon R/\ker(\varphi) \xrightarrow{\cong} \operatorname{im}(\varphi); \qquad \overline{\varphi}(r + I) := \varphi(r).$$

In particular, $R/\ker(\varphi) \cong \operatorname{im}(\varphi)$.

Example 8.23. For each $n \geq 1$, taking the remainder on division by n defines a surjective ring homomorphism

$$\varphi\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n$$

with kernel $\ker(\varphi) = n\mathbb{Z}$. By the First Isomorphism Theorem, we thus have a ring isomorphism

$$\overline{\varphi}\colon \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_n; \qquad \overline{\varphi}(k + n\mathbb{Z}) = \varphi(k).$$

Example 8.24. Applying the First Isomorphism Theorem to Examples 8.7 and 8.9 show that evaluating at 0 determines ring isomorphisms

$$R[x]/\{p(x) \mid p(x) = xq(x) \text{ for some } q(x) \in R[x]\} \cong R$$

and

$$C(\mathbb{R}, \mathbb{R})/\{f \mid f(0) = 0\} \cong \mathbb{R}.$$

Note in the latter that two functions $f, g \in C(\mathbb{R}, \mathbb{R})$ belong to the same coset if and only if $f(0) - g(0) = 0$, or equivalently $f(0) = g(0)$. In other words, functions are grouped according to their value at 0 (explaining why there is a bijective correspondence with $\mathbb{R}$).

Types of ideals

Principal ideals

The simplest ideals to describe are the ideals generated by a single element.

Definition 8.25. An ideal $I \trianglelefteq R$ is called a *principal ideal* if there exists $a \in R$ such that

$$I = aR = \{ar \mid r \in R\}$$

In this case we write $I = (a)$ and call a a *generator* of I.

Example 8.26. Let $u \in R$ be any unit. Then $(u) = R$ because any ideal containing a unit is the entire ring.
This example shows a principal ideal can have more than one generator, and that being principal does not mean the ideal is "small".

Example 8.27. In the integers, the ideals we have seen so far are principal $(n) = n\mathbb{Z} \trianglelefteq \mathbb{Z}$. In fact all ideals in $\mathbb{Z}$ are principal, as we shall prove shortly.

Example 8.28. In Example 8.24, we saw the isomorphism

$$R[x]/\{p(x) \mid p(x) = xq(x) \text{ for some } q(x) \in R[x]\} \cong R.$$

The ideal being quotiented out here is generated by the polynomial x, so is principal. We could therefore write

$$R[x]/(x) \cong R.$$

Example 8.29. Similarly to the previous example, we can generate the principal ideal $(x-a) \trianglelefteq R[x]$. This consists of all polynomials $p(x) = (x-1)q(x)$ for some $q \in R[x]$. In other words, all the polynomials $p(x)$ such that $p(a) = 0$. In other words, the kernel of the ring homomorphism

$$\mathrm{ev}_a \colon R[x] \to R; \qquad \mathrm{ev}_a(p) := p(a).$$

This is surjective, so by the First Isomorphism Theorem we get $R[x]/(x-a) \cong R$.

We can also generate ideals by more than one element.

Definition 8.30. The *ideal generated by* $a_1, \ldots, a_n \in R$ is the subset

$$(a_1, a_2, \ldots, a_n) := \{a_1 r_1 + \cdots + a_n r_n \mid r_1, \ldots, r_n \in R\}.$$

Example 8.31. In $\mathbb{Z}$, the ideal generated by 2 and 3 consists of all linear integer combinations $2a + 3b \in \mathbb{Z}$. But any integer n is such a combination as $3 - 2 = 1$, so $n(3-2) = n$ for any $n \in \mathbb{Z}$. Hence $(2,3) = (1) = \mathbb{Z}$ and the ideal was principal after all.

Example 8.32. Let's show that the ideal $(2, x) \trianglelefteq \mathbb{Z}[x]$ is not principal. This ideal consists of $\{2p(x) + xq(x) \mid p, q \in \mathbb{Z}[x]\}$. This is the set of all integer polynomials whose constant term is even. Suppose, for a contradiction there exists $r(x) \in \mathbb{Z}[x]$ such that $(2, x) = (r(x))$. Then every integer polynomial whose constant term is even is a multiple of $r(x)$. So we must have the constant polynomial 2 is a multiple of $r(x)$, implying $r(x)$ is a constant and moreover $r \in \{\pm 1, \pm 2\}$. If $r \pm 1$ then $(2, x) = (r) = \mathbb{Z}[x]$ because $\pm 1 \in (\mathbb{Z}[x])^\times$. But that is not true because not all integer polynomials have even constant term. But if $r = \pm 2$ then there is also a contradiction, because $2 + x \in (2, x)$ and $2 + x$ is not a multiple of ± 2.

We can also generate on a set of infinitely many elements, but we have to be a little more careful because infinite sums are not generally well-defined in rings.

Definition 8.33. Let $A \subseteq R$ be a subset. The *ideal generated by* A is

$$(A) = \left\{ \sum_{a \in A} a r_a \;\middle|\; r_a \in R \text{ and only finitely many } r_a \text{ are non-zero} \right\}.$$

Maximal ideals

Definition 8.34. An ideal $I \trianglelefteq R$ is called *maximal* if it is proper, but not contained in any other proper ideal.

Proposition 8.35. *Every proper ideal is contained in a maximal ideal.*

Proposition 8.36. *An ideal $I \trianglelefteq R$ is maximal if and only if R/I is a field.*

Example 8.37. The ring $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is a field if and only n is a prime. So the ideal $n\mathbb{Z} \subseteq \mathbb{Z}$ is maximal if and only if n is prime.

Example 8.38. We claim $(2, x) \trianglelefteq \mathbb{Z}[x]$ is a maximal ideal. To do this, we show $\mathbb{Z}[x]/(2, x)$ is a field.

The ideal $(2, x) \trianglelefteq \mathbb{Z}[x]$ consists of all polynomials where the constant coefficient is even. Therefore $(2, x) = \ker(\varphi)$ where $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_2$ is the function that returns "0" if the constant coefficient is even, and "1" if odd (check this is a ring homomorphism). As this function is surjective, the First Isomorphism Theorem gives $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. As this is a field, we deduce the proper ideal $(2, x)$ is maximal.

Example 8.39. As $(x) \subseteq (2, x) \trianglelefteq \mathbb{Z}[x]$ and $(2, x)$ is maximal, we can see from the definition that $(x) \trianglelefteq \mathbb{Z}[x]$ is not maximal. We could also have deduced this because $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is not a field.

Example 8.40. We saw that $C(\mathbb{R}, \mathbb{R})/\{f \mid f(0) = 0\} \cong \mathbb{R}$. As $\mathbb{R}$ is a field, we deduce $\{f \mid f(0) = 0\} \trianglelefteq C(\mathbb{R}, \mathbb{R})$ is a maximal ideal.

Prime ideals

Definition 8.41. An ideal $I \trianglelefteq R$ is called *prime* if it is proper, and if whenever $ab \in I$ we must have $a \in I$ or $b \in I$.

This mirrors the definition in the integers: $p \in \mathbb{Z}^{>1}$ is *prime* if whenever $ab = p$, we must have $a = p$ or $b = p$.

Proposition 8.42. *An ideal $I \trianglelefteq R$ is prime if and only if R/I is an integral domain.*

As fields are integral domains, the following is immediate.

Corollary 8.43. *Maximal ideals are always prime ideals.*

It is not true that prime ideals are always maximal, but this does hold in "nice enough" rings. See the section on Principal Ideal Domains, later.

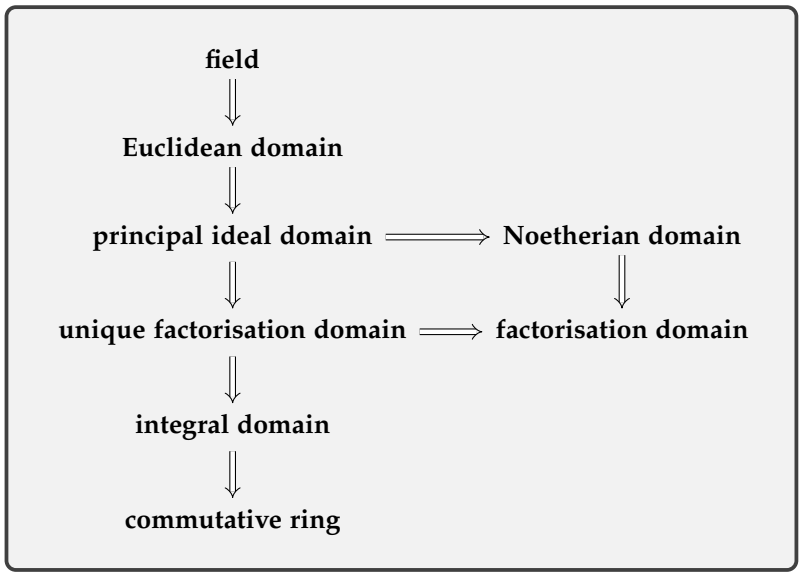
Example 8.44. The ring $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ has zero divisors if and only if n is composite. So $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is a prime ideal if and only if n is prime. So in this ring the prime and maximal ideals are the same.

Example 8.45. We have $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, which is an integral domain, so $(x) \trianglelefteq \mathbb{Z}[x]$ is a prime ideal. But is is not a maximal ideal, so in this ring prime and maximal ideals are different.

9 *Factorisation in integral domains*

Rings are organised by their algebraic complexity, using a combination of how well factorisation/division work in the ring, together with how complicated the ideals in the ring are. In fact, these organisational principals are closely related to one-another.

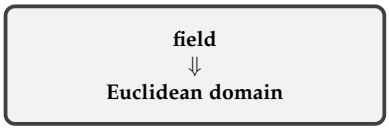
Here is an overview of rings from this perspective:



Fields are the friendliest commutative rings in terms of algebraic complexity and commutative rings that are not integral domains have the potential to be particularly unpleasant.

We have already seen some commutative rings that are not integral domains, for example $\mathbb{Z}_6$, or any $\mathbb{Z}_n$ with n composite, so these guys are not arcane and unusual.

Euclidean domains



The *Euclidean algorithm* is a fundamental tool for studying division.

Example 9.1. The *grade-school division theorem* is what happens when we try to divide $a \in \mathbb{Z}$ by $b \in \mathbb{Z} \setminus \{0\}$. There exists a *quotient* $q \in \mathbb{Z}$ and a *remainder* $r \in \{0, \dots, |b| - 1\}$, such that

$$a = bq + r.$$

This quotient and remainder are unique.

Example 9.2. The *Euclidean algorithm* is the repeated application of the grade-school division theorem, as follows. Let $a = 12378$ and $b = 3054$. Then

$$\begin{aligned} 12378 &= 3054 \cdot 4 + 162 \\ 3054 &= 162 \cdot 18 + 138 \\ 162 &= 138 \cdot 1 + 24 \\ 138 &= 24 \cdot 5 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

The final non-zero remainder is the greatest common divisor of a and b.
The Euclidean algorithm can be reversed to give

$$\begin{aligned} 6 &= 24 - 18 \cdot 1 \\ &= 24 - (138 - 24 \cdot 5) \cdot 1 \\ &= 24 \cdot 6 - 138 \cdot 1 \\ &= (162 - 138 \cdot 1) \cdot 6 - 138 \cdot 1 \\ &= 162 \cdot 6 - 138 \cdot 7 \\ &= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\ &= 162 \cdot 132 - 3054 \cdot 7 \\ &= (12378 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\ &= 12378 \cdot 132 - 3054 \cdot 535 \end{aligned}$$

So

$$12378 \cdot 132 - 3054 \cdot 535 = 6.$$

This is an algorithm for expressing the greatest common divisor of a and b as a linear combination of a and b.

We extract the essential features of the grade-school division theorem and turn it into a definition.

Definition 9.3. An integral domain R is a *Euclidean domain* (ED) if there exists a function $v\colon R \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ such that

(i) $v(ab) \geq v(b)$ for all $a, b \neq 0$, and

(ii) If $a, b \in R$ with $b \neq 0$, then there exist $q, r \in R$ with

$$a = bq + r$$

such that either $r = 0$ or $v(r) < v(b)$.

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

A Euclidean function is sometimes called a "norm", but this clashes with more common uses of that word, so we will not use it.

Unlike in the ring $\mathbb{Z}$, the quotient q and remainder r may not be unique in general.

Example 9.4. The integers are a Euclidean domain. We set $v(n) := |n|$ and apply the grade-school division theorem.

Example 9.5. Fields are Euclidean domains. We set $v(r) := 0$ and then every division has a remainder of 0 because $a = b(b^{-1}a) + 0$ for all a, b with $b \neq 0$.

Example 9.6. For any field $\mathbb{F}$, the polynomials $\mathbb{F}[x]$ are a Euclidean domain. We set $v(p) := \deg(p)$ and the division theorem holds by standard polynomial long-division, which does indeed produce remainders with strictly lower degree.

Example 9.7. The integral domain $\mathbb{Z}[x]$ is not a Euclidean domain, because it contains non-principal ideals, for example $(2, x) \trianglelefteq \mathbb{Z}[x]$.

Construction 9.8 (The Euclidean Algorithm). If R is a Euclidean domain, with Euclidean function $v\colon R \setminus \{0\} \to \mathbb{Z}^{\geq 0}$, we can perform the Euclidean algorithm.

Let $a, b \in R$, $b \neq 0$.

(i) Apply the division axiom to produce $q_1, r_1 \in R$ with

$$a = bq_1 + r_1$$

such that either $r_1 = 0$ or $v(r_1) < v(b)$. If $r_1 = 0$, stop.

(ii) Apply the division axiom to produce $q_2, r_2 \in R$ with

$$b = r_1 q_2 + r_2$$

such that either $r_2 = 0$ or $v(r_2) < v(r_1)$. If $r_2 = 0$, stop.

(iii) Apply the division axiom to produce $q_3, r_3 \in R$ with

$$r_1 = r_2 q_3 + r_3$$

such that either $r_3 = 0$ or $v(r_3) < v(r_2)$. If $r_3 = 0$, stop.

(iv) Keep repeating step (iii), increasing all indices by 1 each time.

The sequence of remainders produced has

$$v(r_1) > v(r_2) > \ldots \in \mathbb{Z}^{\geq 0}.$$

Well-Ordering Axiom

A set $S \subseteq \mathbb{Z}$ that is bounded below has a smallest element.

A strictly decreasing sequence of non-negative integers must eventually be 0, by the Well-Ordering Axiom of the integers. So the algorithm must terminate.

In the ring $\mathbb{Z}$, the last non-zero remainder of the Euclidean algorithm turns out to be the greatest common divisor of a and b. After some preparations, we will prove the similar statement for Euclidean domains.

Proposition 9.9. *Every ideal in a Euclidean domain R is principal. More specifically, if $I \trianglelefteq R$ is non-zero then $I = (d)$, where $d \in I$ is any element with $v(d)$ minimal.*

It makes to say $v(d)$ minimal, because the set
$$S = \{v(a) \mid a \in I\}$$
is bounded below by 0, so must have a minimum, by the Well-Ordering Axiom.

Definition 9.10. Let $a, b \in R$ and $b \neq 0$.

We say *a is a multiple of b*, equivalently *b is a divisor of a*, and write $b|a$, if $a = bx$ for some $x \in R$.

A *greatest common divisor* (gcd) of a and b is any $d \in R$ such that

(i) $d|a$ and $d|b$ COMMON DIVISOR

(ii) If there exists $d' \in R$ such that $d'|a$ and $d'|b$ then $d'|d$ GREATEST

WARNING! In some rings, greatest common divisors do not necessarily exist. In most rings, even when they do exist, they are not unique.

Theorem 9.11. *Let R be a ring.*

(i) If $a, b, d \in R$ such that $(a, b) = (d)$, then d is a gcd of a and b.

(ii) If R is a Euclidean domain then the last non-zero remainder of the Euclidean algorithm for $a, b \in R$ with $b \neq 0$ is a gcd for a and b.

Remark 9.12. Proposition 9.9, combined with Theorem 9.11 (i), shows that we can find a gcd of a and b in a Euclidean domain by identifying $d \in I$ with $v(d)$ minimal. In most actual examples, this suggestion is ridiculously impractical. The beauty of the Euclidean algorithm is that it is a practical method for identifying such d.

Principal ideal domains

We saw in Proposition 9.9 that every ideal in a Euclidean domain is principal. This suggests the definition of a new, potentially weaker, kind of integral domain.

Euclidean domain
⇓
principal ideal domain

Definition 9.13. An integral domain is called a *principal ideal domain* (PID) if every ideal is principal.

Example 9.14. As all Euclidean domains are principal, we already have a bunch of examples: any field $\mathbb{F}$, the integers $\mathbb{Z}$, the polynomial ring of a field $\mathbb{F}[x]$.

Example 9.15. We have a non-example in $\mathbb{Z}[x]$ coming from our old favourite non-principal ideal $(2, x) \trianglelefteq \mathbb{Z}[x]$.

These are not really new examples, and we would like an example showing that there exist PIDs that are not EDs. In this course, we will not delve too deeply into "quadratic integer rings", but this is a good source of such examples, so we describe the construction now.

Construction 9.16. Let $\alpha \in \mathbb{C}$ and define the evaluation map

$$\mathrm{ev}_\alpha : \mathbb{Z}[x] \to \mathbb{C}; \qquad \mathrm{ev}_\alpha(p) := p(\alpha)$$

This is a ring homomorphism.
The image of a ring homomorphism is a subring, and in this case we denote the image by

$$\mathbb{Z}[\alpha] = \{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \mid a_k \in \mathbb{Z}, n \geq 0\} \subseteq \mathbb{C}$$

If we choose α so that $\alpha^2 = n + m\alpha$ for some integers $n, m \in \mathbb{Z}$ then all higher powers of α can be reduced down and we get

$$\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

Example 9.17. Here are a couple of (unjustified) examples, to give you an idea.

- The *Gaussian integers* $\mathbb{Z}[\sqrt{-1}]$ are a Euclidean domain, using the Euclidean function $v(n + m\sqrt{-1}) := n^2 + m^2$.
- The ring $\mathbb{Z}[(1 + \sqrt{-19})/2$ is a PID but not a Euclidean domain.
- The ring $\mathbb{Z}[\sqrt{-5}]$ is not even a PID because it contains the non-principal ideal $(2, 1 + \sqrt{-5})$. This is justified below, in Example 9.27.

A maximal ideal is always prime. The converse holds in PIDs.

Proposition 9.18. *In a PID, an ideal is maximal if and only if it is prime.*

Corollary 9.19. *If a polynomial ring $R[x]$ is a PID, then R must be a field.*

Remark 9.20. We have that $\mathbb{F}[x, y] = (\mathbb{F}[x])[y]$. As $\mathbb{F}[x]$ is not a field, the corollary tells us that $\mathbb{F}[x, y]$ is not a PID. So adding one polynomial indeterminate to the field $\mathbb{F}$ "drops" you down from field to PID, adding a second drops you down somewhere else...

Unique factorisation domains and Noetherian domains

principal ideal domain
⇓
unique factorisation domain

We have already defined units and divisors, but let's recall them now, noting the connection to the ideals they generate.

Definition 9.21. Let R be an integral domain.

(i) An element $u \in R$ is a unit if $uv = 1$ for some $v \in R$.
Equivalently, if $(u) = R$.

(ii) We say *a divides b*, and write $a|b$, if $b = ac$ for some $c \in R$.
Equivalently, if $(b) \subseteq (a)$.

(iii) We say a and b are *associates* if $a = ub$ for some unit $u \in R$.
Equivalently, if $(a) = (b)$.
Equivalently, if $a|b$ and $b|a$.

Here is the definition of "the elements that cannot be (meaningfully) broken up".

Definition 9.22. An element $r \in R$ is called *irreducible* if it is, non-zero, not a unit, and if whenever $r = ab$ then a or b is a unit.

You might have expected the definition of "prime" to elements to be the one above. In ring theory, prime elements have a different definition, which turns out to be a little stronger in general.

Definition 9.23. An non-zero element $p \in R$ is *prime* if whenever $p|ab$ then $p|a$ or $p|b$.

Proposition 9.24. *A non-zero element $p \in R$ is prime if and only if (p) is a prime ideal.*

Proposition 9.25. *If R is an integral domain then all primes are irreducible.*

The converse is not generally true, but to find a counterexample we need a fairly nasty ring, due to the following.

As $\mathbb{Z}$ is a PID, this result explains why the usual definition of prime in $\mathbb{Z}$ looks like our definition of irreducible.

Proposition 9.26. *Let R be a PID. Then a non-zero element is prime if and only if it is irreducible.*

So to find an irreducible element that is not prime, we at least need to be in an integral domain that is not a PID.

Example 9.27. Consider the ring

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}.$$

- The square of the standard norm in the complex numbers induces a function

  $$N \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}^{\geq 0}; \qquad a + b\sqrt{-5} \mapsto a^2 + 5b^2$$

  with the property that $N(uv) = N(u)N(v)$.

- $\underline{N(a) = 1}$: If $uv = 1$ then $N(u)N(v) = N(uv) = 1$, so the norm of a unit must be 1. To find units, we must solve the equation $x^2 + 5y^2 = 1$. But the only integer solutions to this are when $y = 0$ and $x \pm 1$.

- $\underline{N(a) \neq 2}$: There is no integer solution to $x^2 + 5y^2 = 2$. So there is no element of $\mathbb{Z}[\sqrt{-5}]$ with $N(a) = 2$.

- We claim $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime.

  Proof of claim. Suppose 2 is reducible. Then $2 = ab$ with neither $a, b \in \mathbb{Z}[\sqrt{-5}]$ and neither one a unit. But then $4 = N(2) =$

$N(ab) = N(a)N(b)$. This implies $N(a), N(b) \in \{\pm 1, \pm 2\}$. As a, b are not units, this is a contradiction. So 2 is irreducible.

To see 2 is not a prime in $\mathbb{Z}[\sqrt{-5}]$, observe that $(1+\sqrt{-5})(1-\sqrt{-5}) = 1+5 = 6$. This product is divisible by 2, but neither $1+\sqrt{-5}$, nor $1-\sqrt{-5}$ is divisible by 2. To carefully show this, note that $N(1 \pm \sqrt{-5}) = 1^1 + 5 \cdot 1^2 = 6$, and this is not divisible by $N(2) = 4$ in $\mathbb{Z}$. □

As we have exhibited an irreducible element $2 \in \mathbb{Z}[\sqrt{-5}]$ that is not prime, we have proved $\mathbb{Z}[\sqrt{-5}]$ is not a PID. An alternative argument, would be to observe that $(2, 1+\sqrt{-5})$ is not a principal ideal, because if it were equal to (r) for some $r \in \mathbb{Z}[\sqrt{-5}]$, then $2 = ra$ for some $a \in \mathbb{Z}[\sqrt{-5}]$. As 2 is irreducible, this implies r or a is a unit. But r cannot be a unit because the ideal is not the entire ring. So a is a unit. But this implies $(2, 1+\sqrt{-5}) = (r) = (2)$. This is a contradiction as then $1+\sqrt{-5} \in (2)$, which cannot be true as this element is not a multiple of 2.

A famous theorem in the ring $\mathbb{Z}$, is that every integer $n \geq 2$ has a unique prime factorisation. Let's turn this property into a definition.

Definition 9.28. Let R be an integral domain. We say R is a *unique factorisation domain* (UFD) if every $r \in R$, which is not a unit and is not zero, has the following properties.

(i) FACTORS INTO IRREDUCIBLES

$r = p_1 \dots p_n$ where $p_i \in R$ irreducible (not necessarily distinct)

(ii) UNIQUE UP TO ASSOCIATES

If also $r = q_1 \dots q_m$, where $q_i \in R$ are irreducible, then $n = m$ and, up to reordering, p_i and q_i are associates.

Proposition 9.29. *If R is a UFD then a non-zero element is prime if and only if it is irreducible.*

Definition 9.30. An integral domain R is *Noetherian* if every *ascending chain* of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

stabilises, in the sense that there exists n such that $I_n = I_{n+1} = \dots$.

Lemma 9.31. *Every PID is a Noetherian domain.*

Lemma 9.32. *Every Noetherian domain R is a* factorisation domain, *meaning every non-zero, non-unit $r \in R$ factors into irreducibles.*

Theorem 9.33. *Every PID is a UFD.*

Figure 9.1: Emmy Noether (1882 - 1935). One of the most significant algebraists in history, she laid many of the foundations of commutative ring theory. Her reach went far beyond algebra and Noether's Theorem is cited as a fundamental result in Physics, relating symmetry to physical conservation principals.

principal ideal domain
⇓
Noetherian domain
⇓
factorisation domain