# Algebra 145 Lecture Notes

Robert Kropholler

October 15, 2018

1. Syllabus, Sets and functions, Equivalence relations
2. Modular arithmetic
3. Binary Operations and Group Axioms
4. Cayley Tables and Cyclic Groups
5. Dihedral Groups
6. Cayley tables for Dihedral groups, Symmetric groups and permutations
7. Cycle notation, cycle type and transpositions
8. Even and odd permutati ons, the alternating group
9. Subgroups generated by a set
10. Orders of elements, Lagrange's theorem and consequences
11. Homomorphisms, isomorphisms, kernels and images
12. Normal subgroups and quotients
13. Isomorphism theorems
14. Review
15. Midterm
16. Finitely generated abelian groups
17. Group Actions and Cayley's theorem
18. Sylow theory and building groups from old
19. Simplicity of the alternating group
20. Puzzles
21. Ring theory

22. More ring theory

23. Polynomial Rings

24. Ideals and Homomorphisms

25. Isomorphism theorems and chinese remainder theorem

26. Review/overflow

27. Review/overflow

28. Review/overflow
    FINAL

# Contents

# 1 The Preliminaries

## 1.1 Notations

Mathematics is a language and like any other language comes with a set of rules and shorthand notations. While I will try and keep use of these abbreviations to a minimum we should all understand the following.

## 1.2 Basic logic

If $P$ and $Q$ are two statements, then $P \Rightarrow Q$ means that if $P$ is true, then $Q$ is true. In this case, we say that $P$ implies $Q$.

For instance, if $x$ is odd, then $x \neq 2$ or if Ron is a cat, then Ron is not a dog.

If $P \Rightarrow Q$ and $Q \Rightarrow P$, then we write $P \Leftrightarrow Q$, we say $P$ is true if and only if $Q$ is true. For instance, $x$ is an even prime if and only if $x = 2$.

The symbol $\forall$ should be read as "for all". The symbol $\exists$ should be read as "there exists", $\exists!$ should be read as "there exists a unique".

## 1.3 Set notation

Let $S$ and $T$ be two sets.

If $s$ is an element of $S$, then we write $s \in S$ and similarly $s \notin S$ is used to denote that $s$ is not a member of $S$. For instance $2 \in \mathbb{Z}$ and $\frac{1}{2} \notin \mathbb{Z}$.

If $S$ has finitely many elements, then we say that $S$ is a finite set. We write $|S|$ to denote the cardinality of $S$ i.e. the number of elements in $S$.

The standard way of writing a set is to specify what the elements look like and then what properties they have. We do this with braces $\{,\}$ and $|$ the latter should be read as such that. For instance, $\{x \in \mathbb{Z} \mid 2 \text{ divides } x\}$, this is the set of even integers.

If the set is finite, then we can just write the elements out. For instance, $\{0, 1, 2, 3, 4, 5\}$ is the set containing the first five natural numbers. This is equivalent to writing $\{n \in \mathbb{N} \mid 0 \leqslant n \leqslant 5\}$.

If every object of $S$ is also an object of $T$, then we say that $S$ is a subset of $T$ and write $S \subset T$. If $S \subset T$ and $T \subset S$, then $S = T$.

For the complement of a set $S$ in a set $T$ we write $T \setminus S$. This is the set $\{x \in T \mid x \notin S\}$.

The intersection is denoted $S \cap T$ and is the set $\{x \mid x \in S \text{ and } x \in T\}$.

The union of two sets, denoted $S \cup T$ is the set $\{x \mid x \in S \text{ or } x \in T\}$.

The cartesian product of $S$ and $T$, denoted $S \times T$ is the set of ordered pairs of elements of $S$ and $T$. Formally, $S \times T = \{(a, b) \mid a \in S, b \in T\}$.

A function $f$ is a mapping from a set $S$ to another set $T$. We express this using the following notation.

$$f \colon S \to Tx \qquad\qquad \mapsto f(x)$$

Some examples of this notation:

$$\begin{aligned} f\colon \mathbb{N} &\to \mathbb{N} \\ x &\mapsto x^2 \end{aligned}$$

$$\begin{aligned} f\colon \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \cos(\sin(x)) \end{aligned}$$

**Definition 1.3.1.** Let $S$ and $T$ be sets and $f\colon S \to T$ be a map.

- We say $S$ is the *domain* of $f$ and $T$ is the *codomain* of $f$.
- We say that $f$ is the identity is $S = T$ and $f(x) = x$ for all $x \in S$. We denote the identity by $id_S$.
- We say that $f$ is *injective* if $f(x) = f(y) \Rightarrow x = y$.
- We say that $f$ is *surjective* if given a $t \in T$ there is and $s \in S$ such that $f(s) = t$.
- A map is *bijective* if it is both injective and surjective.
- If $R$ is a set and $g\colon R \to S$ is a map, then we can compose $f$ and $g$, denoted $f \circ g$. This is a map from $R$ to $T$.

## 1.4 Relations

Within language we naturally talk about people or objects being related. We can do this abstractly in the world of sets. A relation on a set is a way of grouping objects of a set that are similar to one another. The following is the formal definition, however thinking naively works perfectly well.

**Definition 1.4.1.** A *relation* $R$ on a set $S$ is a subset of $S \times S$. One usually writes $aRb$ if $(a, b) \in R$ and says $a$ is related to $b$.

For instance, a relation on the set $\mathbb{Z}$ could be $aRb$ if $a$ is even. A relation on $\mathbb{R}$ is given by $aRb$ if $a = b^3$.

There are certain extra properties that one might wish to put on a relation.

**Definition 1.4.2.** Let $S$ be a set and $R$ be a relation on $S$.

- We say $R$ is *reflexive* if $(a, a) \in R$ for every $a \in S$.
- We say $R$ is *symmetric* if $(a, b) \in R \Rightarrow (b, a) \in R$.
- We say $R$ is *transitive* if $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$.

We say that $R$ is an *equivalence relation* if it is reflexive, symmetric and transitive. Equivalence relations will usually be denoted by $\sim$

**Example.** $S = \mathbb{R}$ and $xRy$ if and only if $x^4 = y^4$. This is an equivalence relation.

**Example.** $S = \mathbb{R}$ and $xRy$ if and only if $y \leqslant x^2$. This is transitive.

**Example.** $S = \mathbb{Z}$ and $xRy$ if and only if $y \leqslant x^2$. This is reflexive and transitive.

**Example.** $S = \mathcal{P}(\mathbb{N})$ and $XRY$ if and only if the smallest element of $X$ is equal to the smallest element of $Y$. This is an equivalence relation.

**Example.** $S = \mathbb{Z} \times \mathbb{Z}$ and $(a, b)R(c, d)$ if and only if $a = c$ and $b^2 = d^2$. This is an equivalence relation.

**Example.** $S = \{\text{words in the English language}\}$ and $wRv$ if the are synonymous. This is reflexive and symmetric.

**Example.** $S = \mathbb{Z}$ and $xRy$ if and only if 2 divides $x^2$ and 2 divides $y^2$. This is an symmetric and transitive.

Most relations that you can think of will be equivalence relations although coming up with examples that don't satisfy at least one of these properties is not hard.

**Definition 1.4.3.** Let $\sim$ be an equivalence relation on a set $S$. Then we define the *equivalence class* of $x$ as

$$[x] = \{y \in S \mid x \sim y\}.$$

Since equivalence relations are reflexive, we see that $x \in [x]$, this also tells us that the union of equivalence classes is the set $S$.

Using the symmetric and transitive property, it can be shown that either $[x] = [y]$ or $[x] \cap [y] = \varnothing$.

**Definition 1.4.4.** Let $S$ be a set and $\{X_i\}$ be a collection of subsets of $S$. We say that $\{X_i\}$ is a partition of $S$ if the following hold:

- Each $X_i \neq \varnothing$.
- The union of the $X_i$ is $S$.
- If $i \neq j$, then $X_i \cap X_j = \varnothing$.

We have seen that the equivalence classes of an equivalence relation form a partition. These concepts will appear many times throughout the course so I recommend becoming familiar with them as quickly as possible.

## 1.5 Modular Arithmetic

Fix an $n \in \mathbb{N}$ given any integer $m$ there is a remainder $r$ when divided by $n$. This remainder satisfies the following the inequality $0 \leqslant r < n$. We call $r$ the *remainder modulo* $n$. This gives a natural equivalence relation on $\mathbb{Z}$:

$a \sim b \Leftrightarrow a - b$ is divisible by $n \Leftrightarrow a$ and $b$ have the same remainder modulo $n$.

We denote the equivalence classes of this equivalence relation by $\mathbb{Z}/n\mathbb{Z}$. There are $n$ equivalence classes $[0], [1], \ldots, [n-1]$. We call these equivalence classes *residue classes*.

There is a surjective map $[\cdot]\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $m \mapsto [m]$. This map is clearly not injective, e.g. $m, m+n$ have the same image.

One can describe the residue classes in the following way $[m] = \{l \in \mathbb{Z} \mid l = m + kn \text{ for some } k \in \mathbb{Z}\}$. Using this one can prove the following.

**Proposition 1.5.1.** *Let $n \in \mathbb{N}$ and $a, a', b, b' \in \mathbb{Z}$. If $[a] = [a']$ and $[b] = [b']$, then $[a+b] = [a'+b']$ and $[ab] = [a'b']$.*

This allows us to define addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ by $[a] + [b] = [a+b]$ and $[a] \times [b] = [ab]$.

This definition seems to depend on choice of $a \in [a]$ and $b \in [b]$ although the above proposition tells us that if we pick different representatives, then we obtain the same result.

This addition and multiplication work similarly to that of $\mathbb{Z}$. For instance there is a zero, i.e. $[0]$ with the property that $[a] + [0] = [a] = [0] + [a]$.

There is also an analogue of unity given by $[1]$. This has the property that $[1] \times [a] = [a] = [a] \times [1]$.

Also notice, similarly to $\mathbb{Z}$, that $[0] \times [a] = [0] = [a] \times [0]$.

We call a residue class $[a]$ *non-zero* if $[a] \neq [0]$.

Some properties that differ from $\mathbb{Z}$ are that we can add $[1]$ to itself repeatedly and eventually get back to $[0]$. Also if $n = rs$ where $1 < r, s < n$, then $[r] \times [s] = [0]$. One property of $\mathbb{Z}$ is that if $xy = 0$, then $x = 0$ or $y = 0$.

**Proposition 1.5.2.** *For every $n \in \mathbb{N}$ and $m \in \mathbb{Z}$ the congruence*

$$mx \equiv 1 \mod n$$

*has a solution if and only if $m$ and $n$ are coprime.*

*Proof.* If $m$ and $n$ are coprime, then by the Euclidean algorithm we can find $r, s$ such that $rm + sn = 1$ thus $r$ is the solution to the stated equation.

If there is a solution to the equation, then there is an integer $r$ such that $rm = 1 + sn$. Thus $rm - sn = 1$, the greatest common divisor of $m$ and $n$ divide the left hand side and thus must be equal to 1. Hence $m$ and $n$ are coprime. □

The congruence above can be written as an equation in $\mathbb{Z}/n\mathbb{Z}$ by $[a] \times [x] = [1]$. We say that $[a]$ has a multiplicative inverse if there exists a $b \in \mathbb{Z}$ such that $[a] \times [b] = [1]$. The above proposition shows that $[a]$ has a multiplicative inverse if and only if $a$ and $n$ are coprime.

In $\mathbb{Q}$ multiplication has the property that for all non-zero rational numbers $q$ there is a rational number $r$ such that $qr = 1$. We can examine when this

property holds for $\mathbb{Z}/n\mathbb{Z}$. This is the same as asking that $n$ is coprime to $1, 2, \ldots, m-1$. This occurs only when $n$ is prime.

Later we will phrase such objects as fields.

Not all objects we meet will come from numbers many will be more abstract and exotic but these form a very nice class of examples that will appear often throughout the course.

# 2 Group Theory

We begin by studying groups in some ways these are the simplest of algebraic objects. They have a single binary operation which satisfies some additional properties.

## 2.1 Binary Operations

**Definition 2.1.1.** Let $G$ be a set. A *binary operation* $*$ on $G$ is a map $*\colon G \times G \to G$. We write $a * b$ for the image of $(a, b)$.

A binary operation is a way of defining a multiplication on a set. It takes in 2 elements of the set and outputs a third. You are already familiar with several binary operations, although they may not be familiar in such terminology.

**Examples.**

1. Addition, $+$, on the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
2. Subtraction, $-$, on the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
3. Multiplication, $\times$, on the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
4. Matrix multiplication.
5. Addition of vectors in a vector space.
6. Cross product of vectors in $\mathbb{R}^3$.
7. Multiplication of polynomials.
8. Composition of functions $\mathbb{R} \to \mathbb{R}$.

**Non Example.** Division, $\div$, in $\mathbb{R}$. This is not a binary operation as $1 \div 0$ is not defined.

Many of the binary operations you have met satisfy the property of being associative.

**Definition 2.1.2.** A binary operation is *associative* if

$$a * (b * c) = (a * b) * c.$$

Hence, the expression $a * b * c$ has a well defined meaning.

**Exercise.** Which of the above binary operations are associative?

With associativity we can drop all brackets from expressions, i.e. $a_1 * a_2 * \cdots * a_n$ has a well defined meaning.

Another nice property that one might care about is commutativity.

**Definition 2.1.3.** A binary operation is *commutative* if

$$a * b = b * a.$$

**Exercise.** Which of the above binary operations are commutative?

**Definition 2.1.4.** An element $e \in G$ is an *identity* for the binary operation $*$ if, for any $a \in G$,

$$a * e = a = e * a.$$

**Exercise.** Which of the above binary operations have an identity? What is the identity in these cases?

**Proposition 2.1.5.** *If a binary operation has an identity $e$, then it is unique.*

*Proof.* Let $e_1$ and $e_2$ be identities, then the following equalities hold:

$$\begin{aligned} e_1 * e_2 &= e_2 \qquad \text{as } e_1 \text{ is an identity.} \\ e_1 * e_2 &= e_1 \qquad \text{as } e_2 \text{ is an identity.} \end{aligned}$$

So $e_1 = e_2$. □

**Definition 2.1.6.** If a binary operation $*$ has an identity $e \in G$ and $a \in G$, then $b \in G$ is said to be an *inverse* of $a$ if

$$a * b = e = b * a.$$

**Proposition 2.1.7.** *Let $*$ be an associative binary operation on a set $G$ with an identity $e$ and let $a \in G$. Then an inverse of $a$, if it exists, is unique.*

*Proof.* Let $b, c \in G$ be elements such that $a * b = e = c * a$. Consider the element of $G$ given by $c * a * b$ on since $c * a = e$, $e * b = b$ and $*$ is associative we arrive at $c * a * b = b$. Also, since $a * b = e$, $c * e = c$ and $*$ is associative we arrive at the equality $c * a * b = c$. Thus $b = c * a * b = c$. □

**Notation 2.1.8.** We denote the inverse of $a$, if it exists, $a^{-1}$.

Let $G$ be a set and let $*$ be a binary operation on $G$. If $H$ is a subset we can restrict $*$ to $H$ to obtain a map $*\colon H \times H \to G$. This will not usually be a binary operation on $H$. If the binary operation restricts to a binary operation on $H$, then we say $H$ is *closed under* $*$.

**Examples.** $n\mathbb{Z}$ and $\mathbb{N}$

## 2.2 Group Axioms

**Definition 2.2.1.** A *group* $(G, *)$ consists of a set $G$ and a binary operation $*$ on $G$ satisfying the following axioms.

- The binary operation $*$ is associative.
- There is an identity element $e \in G$.
- For each $a \in G$, there is an inverse, $a^{-1}$, for $a$.

*Remark* 1. When the binary operation $*$ is clear from context we will simply write "$G$ is a group" as a shorthand for "$(G, *)$ is a group"

When verifying that $(G, *)$ is a group we must check the three axioms above as well as the fact that $*$ is a binary operation on the set $G$. This is sometimes to referred to as closure of the operation.

As in basic algebra we regularly suppress $*$ in notation. Thus, $a * b$ is simply written as $ab$.

Let $n$ be an integer. We will use the following shorthand:

$$x^n = \begin{cases} \underbrace{xx\dots x}_{n \text{ times}} & n > 0, \\ e & n = 0, \\ \underbrace{x^{-1}x^{-1}\dots x^{-1}}_{-n \text{ times}} & n < 0. \end{cases}$$

One can quickly check that the following come directly from the axioms of being a group.

**Proposition 2.2.2.** *Let $x, y$ be elements of a group $G$ and let $n, m$ be integers.*

1. $(xy)^{-1} = y^{-1}x^{-1}$.
2. $x^n x^m = x^{n+m}$
3. $(x^n)^m = x^{nm}$
4. *If $xz = xy$, then $z = y$.*
5. *If $zx = yx$, then $z = y$.*

*Proof.* Exercise □

**Definition 2.2.3.** We say that a group $(G, *)$ is *abelian* if $*$ is a commutative binary operation. I.e. $xy = yx$ for all $x, y \in G$.

**Example.** The set $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with addition as a binary operation form abelian groups. In each case $e = 0$ and $x^{-1} = -x$.

**Example.** The sets $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ with multiplication form abelian groups. In each case $e = 1$ and $x^{-1} = \frac{1}{x}$.

**Example.** The set $(0, \infty)$ of positive real numbers under multiplication forms a group. Once again $e = 1$ and $x^{-1} = \frac{1}{x}$.

**Example.** Any vector space with the operation of vector addition forms a group.

**Example.** The set of real invertible $n \times n$ matrices under matrix multiplication form a group. This group is the *general linear group* $GL_n(\mathbb{R})$.

There are many other interesting groups of matrices, here are a few.

**Example.** The set of real $n \times n$ matrices with determinant 1 under matrix multiplication. This is the *special linear group* $SL_n(\mathbb{R})$.

**Example.** The set of $n \times n$ orthogonal matrices under matrix multiplication forms the group $O(n)$. (Recall a matrix $A$ is orthogonal if $A^{-1} = A^T$.)

**Example.** The set of $n \times n$ orthogonal matrices with determinant 1 under matrix multiplication forms the group $SO(n)$.

**Example.** The set $\mathbb{Z}/n\mathbb{Z}$ forms a group under addition.

**Example.** The set of elements coprime to $n$ in $\mathbb{Z}/n\mathbb{Z}$ forms a group under multiplication.

**Example.** We can look at symmetries of objects. For instance the triangle or a rectangle.

**Example.** Given any set $S$ we can look at the set of bijections $S \to S$. This forms a group denoted $Sym(S)$.

Finally we can build new groups from old ones by taking direct products.

**Theorem 2.2.4.** *Let $(G, *_G)$ and $(H, *_H)$ be groups. The the operation $*$ on $G \times H$ given by*

$$(g, h) * (g', h') = (g *_G g', h *_H h')$$

*is a group operation. The group $(G \times H, *)$ is called the* direct product of $G$ and $H$.

*Proof.* The binary operation $*$ is associative since both $*_G$ and $*_H$ are associative.

The identity for $*$ is $(e_G, e_H)$ where $e_G$ is the identity in $G$ and $e_H$ is the identity in $H$.

The inverse of the element $(g, h)$ is the element $(g^{-1}, h^{-1})$.

Thus the operation $*$ satisfies the three axioms of a group and $(G \times H, *)$ forms a group. □

### 2.2.1 Cayley tables

Let $G$ be a group. Each $g \in G$ gives a map from $\alpha_g \colon G \to G$ given $\alpha_g(h) = gh$. We can record this information in a table with $G$ rows and $G$ columns. In this $(g, h)$ place we put $gh$. Since $gh = gh'$ implies that $h = h'$ we see that each row has every element of $G$ exactly once. Similarly each column has each element of $G$ exactly once.

An $n \times n$ grid filled with $n$ symbols such that each symbol occurs once in each column and each row is called a *Latin square*. You have probably come across Latin squares in the form of Su Doku or other number puzzles.

Not all Latin squares correspond to groups but when they do they are referred to as *Cayley tables*.

Lets look at some examples.

We have already seen the group $\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$ and we can write the Cayley table as follows:

| $\cdot$ | [0] | [1] | [2] | [3] | [4] |
|---|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] | [4] |
| [1] | [1] | [2] | [3] | [4] | [0] |
| [2] | [2] | [3] | [4] | [0] | [1] |
| [3] | [3] | [4] | [0] | [1] | [2] |
| [4] | [4] | [0] | [1] | [2] | [3] |

Table 1: A Cayley table for $\mathbb{Z}/5\mathbb{Z}$.

**Non Example.** Given 5 elements $x, y, z, t, e$ we can get the following Latin square which does not correspond to any group.

| $\cdot$ | $e$ | $x$ | $y$ | $z$ | $t$ |
|---|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ | $t$ |
| $x$ | $x$ | $e$ | $t$ | $y$ | $z$ |
| $y$ | $y$ | $t$ | $z$ | $e$ | $x$ |
| $z$ | $z$ | $y$ | $x$ | $t$ | $e$ |
| $t$ | $t$ | $z$ | $e$ | $x$ | $y$ |

How do we know this doesn't correspond to a group. Since $ty = e$, we have that $t = y^{-1}$ in a group this would imply that $yt = e$ however the table tells us that $yt = x$.

We can deduce many things about a group from its Cayley table. Firstly we can see if the group is abelian. If the elements of the group are labelled $x_i$, then the $(i, j)$-th position of the Cayley table is $x_i x_j$. Thus we can see if the group is abelian by checking that the $(i, j)$-th entry and the $(j, i)$-th entry are the same. Alternatively we can see if the Cayley table is symmetric about the leading diagonal.

**Definition 2.2.5.** We say that two Cayley tables are *equivalent* if there is a way to reorder the elements of the group such that the rows and column of one are the same as the rows and columns of the other.

Later we will formalise this to the notion of isomorphism but this will do for now.

**Proposition 2.2.6.** *If two Cayley tables are equivalent, then the groups they represent are the same with the elements reordered.*

*Proof.* content... □

This allows us to assume that the first column and row correspond to the identity element of the group.

Let us look at Cayley tables for a group of with 3 elements, let us label these elements $\{e, x, y\}$.

We can start filling it out to get the following.

| $\cdot$ | $e$ | $x$ | $y$ |
|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ |
| $x$ | $x$ | | |
| $y$ | $y$ | $\square$ | |

Let us now consider the entry labelled by $\square$ in the above table. This cannot be $x$ or $y$ since they already appear in that column or row respectively. So we see that this entry must be $e$ and we get the following,

| $\cdot$ | $e$ | $x$ | $y$ |
|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ |
| $x$ | $x$ | $\circ$ | |
| $y$ | $y$ | $e$ | |

We now know that the $\circ$ in the above table must be $y$ and this allows us to fill in the rest of the table to obtain:

| $\cdot$ | $e$ | $x$ | $y$ |
|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ |
| $x$ | $x$ | $y$ | $e$ |
| $y$ | $y$ | $e$ | $x$ |

This may not be a table which represents a group however if we compare it to the table for $\mathbb{Z}/3\mathbb{Z}$ i.e.

| $\cdot$ | $[0]$ | $[1]$ | $[2]$ |
|---|---|---|---|
| $[0]$ | $[0]$ | $[1]$ | $[2]$ |
| $[1]$ | $[1]$ | $[2]$ | $[1]$ |
| $[2]$ | $[2]$ | $[1]$ | $[0]$ |

We see that the table above does indeed represent a group. In particular there is only one group with 3 elements.

Let us look at groups with 4 elements $\{e, x, y, z\}$. Once again the first row and column are easy and we start with,

| $\cdot$ | $e$ | $x$ | $y$ | z |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | z |
| $x$ | $x$ | | | |
| $y$ | $y$ | | | |
| $z$ | $z$ | | | |

We now have a choice for the $xy$ entry, it can be either $e$ or $z$. Let us begin with the case that it is $e$. We also know that if $xy = e$, then $yx = e$. So we get,

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | ? | $e$ | ? |
| $y$ | $y$ | $e$ | ? | ? |
| $z$ | $z$ | ? | ? | ? |

Since there is an $e$ in each column and row, we see that $z^2 = e$. Also focusing on the third row and column we see that $yz = zy = x$. We now get,

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | ? | $e$ | ? |
| $y$ | $y$ | $e$ | ? | $x$ |
| $z$ | $z$ | ? | $x$ | $e$ |

We can now deduce the rest to obtain

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | $z$ | $e$ | $y$ |
| $y$ | $y$ | $e$ | $z$ | $x$ |
| $z$ | $z$ | $y$ | $x$ | $e$ |

If we now replace $e$ with [0], $x$ with [1], $t$ with [3] and $z$ with [2] we obtain the table for $\mathbb{Z}/4\mathbb{Z}$.

| $\cdot$ | [0] | [1] | [3] | [2] |
|---|---|---|---|---|
| [0] | [0] | [1] | [3] | [2] |
| [1] | [1] | [2] | [0] | [3] |
| [3] | [3] | [0] | [2] | [1] |
| [2] | [2] | [3] | [1] | [0] |

We see that this is certainly the table for a group and is in fact the table for $\mathbb{Z}/4\mathbb{Z}$.

Now we return to the case that $xy = z$. Since $xy = e$ if and only if $yx = e$, we also know that $yx = z$. We obtain the following

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | ? | $z$ | ? |
| $y$ | $y$ | $z$ | ? | ? |
| $z$ | $z$ | ? | ? | ? |

We now once again have two options. Either $x^2 = e$ or $x^2 = y$. Let us begin with the case that $x^2 = y$ filling in the obvious blanks we obtain the following.

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | $y$ | $z$ | $e$ |
| $y$ | $y$ | $z$ | ? | ? |
| $z$ | $z$ | $e$ | ? | ? |

We also see that $zy = x$ and from this we can finish the table.

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | $y$ | $z$ | $e$ |
| $y$ | $y$ | $z$ | $e$ | $x$ |
| $z$ | $z$ | $e$ | $x$ | $y$ |

Once again we can ask if this is a group table and indeed by relabelling $e$ as [0], $x$ as [1], $y$ as [2] and $z$ as [3] we once again obtain the table for $\mathbb{Z}/4\mathbb{Z}$.

| $\cdot$ | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] |
| [1] | [1] | [2] | [3] | [0] |
| [2] | [2] | [3] | [0] | [1] |
| [3] | [3] | [0] | [1] | [2] |

We now have one more case $xy = z$ and $x^2 = e$, we also deduce that $xz = y = zx$ we obtain the following

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | $e$ | $z$ | $y$ |
| $y$ | $y$ | $z$ | ? | ? |
| $z$ | $z$ | $y$ | ? | ? |

We now once again split into two options. If we let $y^2 = z$, then we can replace to once again obtain the table for $\mathbb{Z}/4\mathbb{Z}$ again. If we let $y^2 = e$ we obtain the following:

| $\cdot$ | $e$ | $x$ | $y$ | $z$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $z$ |
| $x$ | $x$ | $e$ | $z$ | $y$ |
| $y$ | $y$ | $z$ | $e$ | $x$ |
| $z$ | $z$ | $y$ | $x$ | $e$ |

This is a fundamentally different group but is the same as the group of symmetries of a rectangle discussed earlier. This group is known as the Klein 4 group. What we have seen is that all groups with 4 elements are abelian.

### 2.2.2 Cyclic groups

**Definition 2.2.7.** A group $G$ is *cyclic* if there is an element $g \in G$ such that $G = \{g^k \mid k \in \mathbb{Z}\}$.

Such a $g$ is called a *generator* for $G$.

Cyclic groups form and important class of groups.

**Example.** The group $\mathbb{Z}$ is a cyclic group with generator 1 or $-1$.

**Definition 2.2.8.** The cardinality $|G|$ of a group $G$ is called the *order* of $G$. We say that a group is *finite* if $|G|$ is finite.

**Definition 2.2.9.** The *cyclic group of order* $n$, $C_n$, is the group with elements

$$e, g, g^2, \ldots, g^{n-1}$$

which satisfy $g^n = e$. Thus the multiplication is defined by

$$g^i * g^j = \begin{cases} g^{i+j} & \text{if } 0 \leqslant i + j < n, \\ g^{i+j-n} & \text{if } n \leqslant i + j \leqslant 2n - 2. \end{cases}$$

**Definition 2.2.10.** Let $g$ be an element of a group $G$. The *order of* $g$ is the minimal $n > 0$ such that $g^n = e$. If no such $n$ exists we say that $g$ is of infinite order.

We denote the order of $g$ by $o(g)$.

**Lemma 2.2.11.** *Let $g$ be an element of a group with finite order. Then $g^k = g^{k-o(g)}$. Also, $g^k = g^{k+o(g)}$.*

*Proof.* Exercise. Key ingredient: $g^{o(g)} = e$. □

**Theorem 2.2.12.** *Let $g$ be an element of a group. Then $g^k = e$ if and only if $o(g)$ divides $k$.*

*Proof.* For one direction, if $o(g)$ divides $k$, then $k = p(o(g))$. Thus, $g^k = (g^{o(g)})^p = e^p = e$.

For the other direction, if $g^k = e$, then using Lemma 2.2.11 we can repeatedly add or subtract $o(g)$ from $k$ to obtain $l$. Thus $l$ has the following properties:

- $g^k = g^l$.
- $l = k + q(o(g))$ for some $q \in \mathbb{Z}$.
- $0 \leqslant l < o(g)$.

Since $o(g)$ was minimal among $n$ such that $n > 0$ and $g^n = e$, we see that $l = 0$. Thus, $0 = k + q(o(g))$ and $k$ is divisible by $o(g)$. □

**Proposition 2.2.13.** *If $g$ is an element of a group $G$, then the order of $g$ is the size of the set $\{g^k \mid k \in \mathbb{Z}\}$.*

*Proof.* Suppose that $g$ has infinite order, we will show the set is infinite. It contains the subset $\{g^k \mid k \in \mathbb{N}\}$. Suppose that two elements of this set are equal i.e. there are positive integers $k, l$ such that $g^k = g^l$. We can assume that $k < l$. So $g^{l-k} = g^l g^{-k} = e$. Thus contradicting $g$ having infinite order. Thus the set $\{g^k \mid k \in \mathbb{Z}\}$ is an infinite set.

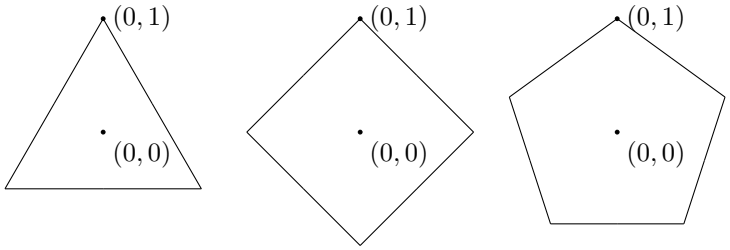
Suppose now that $g$ has finite order. By Lemma 2.2.11 we can replace any power of $g$ with $g^l$ such that $0 \leqslant l < o(g)$. Thus $\{g^k \mid k \in \mathbb{Z}\} = \{g^k \mid 0 \leqslant k < o(g)\}$ so we have that $|\{g^k \mid k \in \mathbb{Z}\}| \leqslant o(g)$. Suppose there were two numbers $0 \leqslant k, l < o(g)$ such that $g^k = g^l$. Then $g^{k-l} = e$ we may assume that $k - l \geqslant 0$. Thus, $0 \leqslant k - l < o(g)$ so by minimality of $o(g)$ we have that $k - l = 0$. Thus, $|\{g^k \mid 0 \leqslant k < o(g)\}| = o(g)$. □

**Corollary 2.2.14.** *If $G$ is finite, then $o(g)$ is finite for all elements $g \in G$.*

*Proof.* The set $\{g^k \mid k \in \mathbb{Z}\}$ is a subset of $G$ which is a finite group. □

### 2.2.3 Dihedral groups

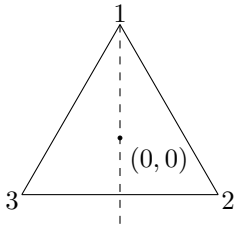
Let $n \geqslant 3$ be an integer. Let $P$ be the regular $n$-gon in the plane with center at $(0, 0)$ and a vertex at $(0, 1)$. The first few are depicted below




**Definition 2.2.15.** The *$n$-th dihedral group* $D_n$ is the group of linear maps $f$ from $\mathbb{R}^2$ to $\mathbb{R}^2$ such that $f(P) = P$. This is the set of symmetries of a regular $n$-gon. This is a group since:

- The identity map is in $D_n$.
- The composition of two such maps is in $D_n$.
- The inverse of such a map is in $D_n$
- Composition of functions is associative.

Let us carefully study some small cases. First consider the case $n = 3$.




Let $r$ be the rotation clockwise by $\frac{2\pi}{3}$ and let $s$ be the reflection in the dashed line through $(0,1)$ and $(0,0)$. We will also label the vertices $1,2,3$. We have the following six symmetries

$$e, r, r^2, s, rs, r^2s.$$

These are all different since they each do different things to the vertices. In fact, they give the following permutations:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

In fact, since these are the only possible permutations of the vertices, these must be all the elements.

In the case $n = 4$, we similarly let $r$ be the rotation clockwise by $\frac{\pi}{2}$ and $s$ as before. We now have the following 8 elements along with the permutation they induce on the vertices

$$e = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \quad r = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \quad r^2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \quad r^3 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},$$
$$s = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}, \quad rs = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \quad r^2s = \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \quad r^3s = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

Once again we can see that these are 8 different elements. However, it is harder to see that these are all the elements as there are $4! = 24$ permutations of the vertices. We do however have the following.

**Proposition 2.2.16.** *There are $2n$ elements of $D_n$.*

*Furthermore, let $r$ be the rotation clockwise through an angle of $\frac{2\pi}{n}$. Let $s$ be the reflection through the $y$-axis. Then $D_n$ consists of the elements $e, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s$.*

*Proof.* Labelling the vertices of the regular $n$-gon with the numbers $1, \ldots, n$ we see that any element of $D_n$ send the vertex labelled 1 to any other vertex. Once one has decided where 1 goes then there are 2 choices for where the map sends 2. Once the images of 1 and 2 are chosen, then the image of 3 is decided since this must be adjacent to 2 but cannot be the image of 1. Similarly the image of all the other vertices are decided. This gives at most $2n$ elements of $D_n$.

To check that there are in fact $2n$ elements, consider the list of elements given by $e, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s$. One can check that these elements send

the vertices labelled 1 and 2 to any choice of 2 adjacent vertices in the polygon $P$. Thus these are all $2n$ possible choices of map. □

**Proposition 2.2.17.** *The following identities hold in $D_n$.*

$$r^n = e$$
$$s^2 = e$$
$$sr = r^{n-1}s = r^{-1}s$$

*Proof.* One can simply check that the maps above are as stated. □

## 2.3 Symmetric groups

**Definition 2.3.1.** Let $S$ be a set. A bijection $f\colon S \to S$ is called a *permutation* of $S$ and the set of all permutations of $S$ is called $Sym(S)$.

If $n$ is a positive integer, then we write $S_n$ for $\mathrm{Sym}(\{1, 2, \ldots, n\})$.

**Theorem 2.3.2.** *Let $S$ be a set.*

1. *Then* $\mathrm{Sym}(S)$ *is a group, where the binary operation is composition of functions.*
2. *The order of $S_n$ is $n!$.*
3. *If $|S| > 2$, then* $\mathrm{Sym}(S)$ *is non-abelian.*

*Proof.* For the first point it is clear that the composition of two bijections is a bijection, thus this is binary operation on $\mathrm{Sym}(S)$. Composition of functions is an associative operation. The map $\mathrm{id}_S$ is the identity for this operation. We proved on Problem sheet 1 Q3, that any bijective map has an inverse. Thus $\mathrm{Sym}(S)$ is a group.

For a bijection $f$ on $\{1, 2, \ldots, n\}$, we have $n$ possibilities for $f(1)$. For $f(2)$ we have $n-1$ choices since we can choose any element which isn't $f(1)$. Repeating this we make $n!$ choices. Thus there are $n!$ elements of $S_n$.

To show that it is not Abelian consider the permutation $\sigma$ which exchanges 1 and 2 and the permutation $\tau$ which exchanges 2 and 3. It is easy to check that $\sigma \circ \tau(1) = 2$ while $\tau \circ \sigma(1) = 3$. Thus, they are different permutations and $S_n$ is non-abelian for $n > 2$. □

We have already written some permutations when we looked at the dihedral groups. One way to write the permutation $\sigma$ is as follows.

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

We will improve on this notation shortly.

**Example.** The group $S_2$ consists of two elements.

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

**Example.** We have already seen the group $S_3$ although we have seen it as a different group, namely, $D_3$. It consists of the 6 permutations,

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

**Example.** Set

$$\alpha = \begin{pmatrix}1&2&3&4&5&6\\1&4&6&5&2&3\end{pmatrix}, \beta = \begin{pmatrix}1&2&3&4&5&6\\5&2&1&4&6&3\end{pmatrix}, \gamma = \begin{pmatrix}1&2&3&4&5&6\\2&1&6&5&4&3\end{pmatrix}$$

in $S_6$. Determine $\alpha\beta\gamma$, $\beta^{-1}$ and the order of $\gamma$.

*Proof.* $\alpha\beta\gamma = \begin{pmatrix}1&2&3&4&5&6\\4&2&6&3&5&1\end{pmatrix}, \beta^{-1} = \begin{pmatrix}1&2&3&4&5&6\\3&2&6&4&1&5\end{pmatrix}$ and $o(\gamma) = 2$. □

We will now try and simplify the notation of permutations allowing arguments to be more succinct. We will first need the idea of a cycle, this is a special type of permutation.

**Definition 2.3.3.** A permutation $\sigma$ is a *cycle* if there are distinct elements $a_1, \ldots, a_k$ such that

$$\sigma(a_i) = a_{i+1} \text{ for } 1 \leqslant i < k \qquad \sigma(a_k) = a_1$$

and

$$\sigma(x) = x \text{ for } x \notin \{a_1, \ldots, a_k\}.$$

The *length* of such a cycle is $k$ and we call $\sigma$ a *$k$-cycle*.

To denote the $k$-cycle we write $(a_1\, a_2\, \ldots\, a_k)$. Note that this notation is not unique, we could also write $(a_2\, a_3\, \ldots\, a_k\, a_1)$, in fact, there are $k$ ways to write this cycle.

Two cycles $(a_1\, \ldots\, a_k)$ and $(b_1\, \ldots\, b_l)$ are disjoint if $a_i \neq b_j$ for all $i, j$.

**Proposition 2.3.4.** *Disjoint cycles commute.*

*Proof.* Let $\alpha$ be the cycle $(a_1\, a_2\, \ldots\, a_k)$ and $\beta$ be the cycle $(b_1\, b_2\, \ldots\, b_l)$. Let us now consider $\beta(\alpha(i))$. There are three possibilities.

1. $i \in \{a_1, a_2, \ldots, a_k\}$ suppose $i = a_j$. In this case $\alpha(i) = \alpha(a_j) = a_{j+1}$ or $a_1$ of $j = k$. Now consider $\beta(a_{j+1})$. Since these are disjoint permutations we see that $\beta(a_{j+1}) = a_{j+1}$. The reasoning is similar for $a_1$.

2. $i \in \{b_1, b_2, \ldots, b_l\}$. Suppose the $i = b_m$. Since the permutations are disjoint we see that $\alpha(i) = \alpha(b_m) = b_m$. Now we compute $\beta(b_m) = b_{m+1}$ or $b_1$ depending on whether $m = l$ or not.

3. Finally assume $i \notin \{a_1, \ldots, a_k, b_1, \ldots, b_l\}$. In this case $\alpha(i) = i$ and $\beta(i) = i$. Thus $\beta(\alpha(i)) = i$.

   Now check what happens when we compose the other way. I.e. compute $\alpha(\beta(i))$. Once again there are three cases, computing as above we get the same answer.

□

**Theorem 2.3.5.** *Every element of $S_n$ can be expressed as a product of disjoint cycles. Such an expression is uniquely determined up to the ordering of the cycles and the notational redundancy within each cycle.*

*Proof.* Let $\sigma$ be an element of $S_n$. Choose any $i_1 \in \{1, \ldots, n\}$. We can now construct a sequence of elements of $\{1, \ldots, n\}$ starting with $i_1$ by repeatedly applying $\sigma$:

$$i_1,\ i_2,\ i_3,\ \ldots,$$

so that $i_j = \sigma(i_{j-1})$ for $j \geqslant 2$. This sequence must involve repetitions. Suppose that the $k$th term is the first one which is a repetition. In other words, $i_k$ has already appeared earlier in the sequence but the earlier terms themselves have each appeared for the first time. If $i_k = i_j$ with $j < k$ and $j \neq 1$ then we get a contradiction because two different elements $i_{j-1}, i_{k-1}$ map to $i_k$. Therefore it must be the case that $i_k = i_1$.

In this way we see that $\sigma$ involves the $k-1$-cycle

$$(i_1\ \ldots\ i_{k-1}).$$

If necessary we can repeat this starting with an $i_1' \in \{1, \ldots, n\}$ which does not appear in the first cycle. We now obtain a second cycle and it must be disjoint from the first because $\sigma$ is a permutation. Continuing in this way we obtain a disjoint cycle representation of $\sigma$. □

For brevity, we will remove cycles of length 1.

**Example.** We can now write $\alpha, \beta, \gamma$ from above as

$$\alpha = (2\,4\,5\,2)(3\,6), \beta = (1\,5\,6\,3), \gamma = (1\,2)(3\,6)(4\,5).$$

**Definition 2.3.6.** As a consequence of the above theorem, the lengths of the various cycles of a permutation are well defined. This is known as the *cycle type* of the permutation.

**Proposition 2.3.7.** *Let $\sigma = \rho_1\rho_2 \ldots \rho_k$ be an expression for $\sigma$ as a product of disjoint cycles of length $l_1, \ldots, l_k$. Then the order of $\sigma$ is $lcm(l_1, \ldots, l_k)$.*

*Proof.* Since disjoint cycles commute we see that $\sigma^n = \rho_1^n\rho_2^n \ldots \rho_k^n$. So for this expression to be the trivial element we see that $\rho_i^n$ must be trivial for all $i$. The order of an $l$ cycle is $l$. Thus $\rho_i^n$ is trivial if and only if $l_i$ divides $n$. Thus $\sigma^n$ is trivial if and only if $l_i$ divides $n$ for all $n$. The smallest such positive number is the lowest common multiple of $(l_1, \ldots, l_k)$. □

**Proposition 2.3.8.** *Let $k \leqslant n$. Then there are*

$$\frac{n!}{(n-k)!k}$$

*cycles of length $k$ in $S_n$.*

*Proof.* There are $n$ choices for the first element, then $n-1$ choices for the second element and so on. This gives $\frac{n!}{(n-k)!}$. However since the order only matters up to cyclic permutation we can see that we have over counted by $k$. Thus we obtain that the number of $k$-cycles is

$$\frac{n!}{(n-k)!k}.$$

□

**Example.** How many permutations are there of each cycle type in $S_6$?

*Proof.*

| Cycle type | Number of permutations |
|---|---|
| $(1,1,1,1,1,1)$ | 1 |
| $(2,1,1,1,1)$ | 15 |
| $(2,2,1,1)$ | 45 |
| $(2,2,2)$ | 15 |
| $(3,1,1,1)$ | 40 |
| $(3,2,1)$ | 120 |
| $(3,3)$ | 40 |
| $(4,1,1)$ | 90 |
| $(4,2)$ | 90 |
| $(5,1)$ | 144 |
| $(6)$ | 120 |

□

If you forgot the numbers in the permutation and just remembered the cycle type. This ideas is captured by conjugacy in the symmetric group.

**Definition 2.3.9.** Two permutations $\sigma, \tau$ are *conjugate* if there is a permutation $\rho$ such that $\tau = \rho\sigma\rho^{-1}$. We say that $\rho$ *conjugates* $\sigma$ to $\tau$.

**Lemma 2.3.10.** *Any two $k$-cycles are conjugate. In fact, given the cycle $\tau = (a_1\, a_2\, \ldots\, a_k)$ we can show that $\sigma\tau\sigma^{-1} = (\sigma(a_1)\, \sigma(a_2)\, \ldots\, \sigma(a_k))$.*

*Proof.* Exercise □

**Theorem 2.3.11.** *Two permutations are conjugate if and only if they have the same cycle type.*

*Proof.* Let $\sigma = \sigma_1 \ldots \sigma_k$ where $\sigma_i$ and $\sigma_j$ are disjoint. Assume that $\tau$ is conjugate to $\sigma$, so there is a $\rho$ such that $\rho\sigma\rho^{-1} = \tau$. Then $\rho\sigma\rho^{-1} = \rho\sigma_1 \ldots \sigma_k\rho^{-1} = \rho\sigma_1\rho^{-1}\rho\sigma_2\rho^{-1} \ldots \rho\sigma_k\rho^{-1}$. By the above lemma $\rho\sigma_1\rho^{-1}$ is a cycle with the same length as $\sigma_1$. Also we can see that $\rho\sigma_i\rho^{-1}$ is disjoint from $\rho\sigma_j\rho^{-1}$ so we have written $\tau$ as a product of disjoint cycles with the same lengths as those for $\sigma$. Thus they have the same cycle type.

Let $\sigma$ and $\tau$ be permutations with the same cycle type. First write $\sigma$ as a product of disjoint cycles $\sigma = \sigma_1 \ldots \sigma_k$ and $\tau$ as a product of disjoint cycles $\tau = \tau_1 \ldots \tau_k$, where $\sigma_i$ and $\tau_i$ have the same length. Define $\rho$ as the permutation which sends that $j$-th element of $\sigma_i$ to the $j$-th element of $\tau_i$. The lemma above shows that $\rho\sigma\rho^{-1} = \tau$. □

**Example.** Find a permutation that conjugates $(1\,2)(3\,4)(5\,6\,7\,8)$ to $(5\,8)(2\,7)(1\,6\,4\,3)$.

*Proof.* The permutations $(1\,5)(2\,8\,3)(4\,7)(6)$ is a permutation that has the desired effect. □

**Definition 2.3.12.** A *transposition* is another name for a 2-cycle.

A permutation is said to be *odd* (respectively *even*) if it is a product of an odd (respectively even) number of transpositions.

**Theorem 2.3.13.** *Every permutation can be written as a product of transpositions.*

*Proof.* Since every permutation is a product of disjoint cycles, it is enough to show that each cycle can be written as a product of transpositions. This is certainly the case as $(a_1\,a_2\,\ldots\,a_k) = (a_1\,a_2)(a_2\,a_3)\ldots(a_{k-1}\,a_k)$. □

**Theorem 2.3.14.** *There is no permutation which is both even and odd.*

*Remark* 2. Note that cycles of even length are odd permutations and cycles of odd length are even permutations.

The above is somewhat annoying but parity has similar properties to additions of odd and even numbers.

**Proposition 2.3.15.** *Let $\sigma, \tau \in S_n$. Then*

- *If $\sigma, \tau$ are even, then $\sigma\tau$ is even.*
- *if $\sigma, \tau$ are odd, then $\sigma\tau$ is even.*
- *if $\sigma$ is odd and $\tau$ is even, then $\sigma\tau$ is odd.*
- *if $\sigma$ is even and $\tau$ is odd, then $\sigma\tau$ is odd.*

**Proposition 2.3.16.** *The set of even permutations form a group, called the* alternating group*, denoted $A_n$.*
*For $n \geqslant 2$ the order of $A_n$ is $\frac{n!}{2}$.*
*For $n \geqslant 4$ $A_n$ is non-abelian.*

*Proof.* content... □

## 2.4 Subgroups

**Definition 2.4.1.** Let $G$ be a group. A subset $H \subset G$ is a *subgroup* if the group operation $*$ restricts to $H$ to make $H$ a group. That is $H$ is a subgroup of $G$ if:

1. $e \in H$,
2. if $g, h \in H$, then $gh \in H$,
3. if $g \in H$, then $g^{-1} \in H$.

If $H$ is a subgroup of $G$, then we write $H \leqslant G$.

**Example.** $A_n$ is a subgroup of $S_n$.

**Proposition 2.4.2.** *Let $G$ be a group. Let $H$ be a subset. Then $H$ is a subgroup if and only if $H$ is non-empty and whenever $g, h \in H$, then $gh^{-1} \in H$.*

*Proof.* content... □

**Example.** The subgroups of $S_3$ are

$$\{e\}, \{e, (1\,2)\}, \{e, (2\,3)\}, \{e, (1\,3)\}, \{e, (1\,2\,3), (3\,2\,1)\} = A_3, S_3.$$

**Example.** The subgroups of $D_4$ are

$$\{e\}, \{e, r^2\}, \{e, s\}, \{e, rs\}, \{e, r^2s\}, \{e, r^3s\},$$

$$\{e, r, r^2, r^3\}, \{e, rs, r^2, r^3s\}, \{e, s, r^2, r^2s\}, D_4.$$

**Example.** The subgroups of $C_6$ are

$$\{e\}, \{e, g^3\}, \{e, g^2, g^3\}, C_6.$$

The only subgroups of $C_5$ are $\{e\}$ and $C_5$.

**Proposition 2.4.3.** *Let $G$ be a group and $H, K$ subgroups of $G$. Then $H \cap K$ is a subgroup of $G$.*

**Definition 2.4.4.** The *subgroup generated by a set $S$* , denoted $\langle S \rangle$, is the smallest subgroup containing $S$. I.e. $\langle S \rangle = \bigcap_{S \subset H} H$ where $H$ is a subgroup of $G$.

If $g \in G$, then we write $\langle g \rangle$ rather than the more cumbersome $\langle \{g\} \rangle$.

If $\langle S \rangle = G$, then the set $S$ is called a *generating set* for $G$.

**Example.** Determine $\langle S \rangle$ in each of the following cases:

1. $G = \mathbb{Z}$ and $S = \{16, 56\}$.
2. $G = S_5$ and $S = \{(1\,2)(3\,4), (1\,3)(2\,4)\}$.

**Example.** Show that if $G$ is abelian and $g, h \in G$, then $\langle g, h \rangle = \{g^n h^m \mid n, m \in \mathbb{Z}\}$.

**Proposition 2.4.5.** *Let $G$ be a group and $g \in G$. Then $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.*

*Proof.* content... □

**Definition 2.4.6.** The *order* of an element $g \in G$, denoted $o(g)$, is the smallest integer $n > 0$ such that $g^n = e$. If no such integer exists, then $o(g) = \infty$.

**Proposition 2.4.7.** *If $o(g)$ is finite, then $\langle g \rangle = \{e, g, \ldots, g^{o(g)-1}\}$.*

*Proof.* content... □

We can now redefine what it means to be a cyclic group. $G$ is cyclic if and only if there exists a $g \in G$, such that $G = \langle g \rangle$.

*Remark* 3. Note that in a finite group $G = \langle g \rangle$ if and only if $o(g) = |G|$.

**Theorem 2.4.8.** *Let $G$ be a cyclic group and $H$ a subgroup of $G$. Then $H$ is cyclic.*

*Proof.* content... □

**Proposition 2.4.9.** *Let $m, n$ be non-zero integers. By Theorem 2.4.8 we have that*

$$\langle m, n \rangle = \langle h \rangle \qquad \langle m \rangle \cap \langle n \rangle = \langle l \rangle$$

*for some $h, l \in \mathbb{Z}$. Then $h$ and $l$ have the following properties:*

1. *$h \mid n$ and $h \mid m$,*
2. *if $x \mid n$ and $x \mid m$, then $x \mid h$*
3. *there exists $u, v \in \mathbb{Z}$ such that $un + vm = h$.*
4. *$m \mid l$ and $n \mid l$,*
5. *if $m \mid x$ and $n \mid x$, then $l \mid x$.*

**Definition 2.4.10.** We define $h$ to be the *highest common multiple* and $l$ to be the *lowest common multiple*.

## 2.5 Lagrange's theorem

Recall that the order of an element $g$ is the minimal $n > 0$ such that $g^n = e$. If no such $n$ exists, then we say $g$ is of infinite order.

**Proposition 2.5.1.** *If $g \in G$ and $o(g) < \infty$, then $g^n = e$ if and only if $o(g) \mid n$.*

*Proof.* content... □

**Definition 2.5.2.** Let $H$ be a subgroup of a group $G$.

Then the *left cosets* of $H$ in $G$ are the sets

$$gH = \{gh \mid h \in H\}.$$

The *right cosets* of $H$ in $G$ are the sets

$$Hg = \{hg \mid h \in H\}.$$

**Notation 2.5.3.** We write $G/H$ for the set of left cosets of $H$. The cardinality of $G/H$ is the *index* of $H$ in $G$.

Note that different elements $g_1, g_2$ can represent the same left coset. I.e. $g_1 H = g_2 H$ yet $g_1 \neq g_2$.

In general, $gH \neq Hg$, there are certain special cases where this will be true.

**Example.** Let $G = S_3$ and $H = \{e, (1\,2)\}$. Then

$$\begin{aligned} eH = (1\,2)H = \{e, (1\,2)\}, \qquad & He = H(1\,2) = \{e, (1\,2)\}, \\ (1\,3)H = (1\,3\,2)H = (1\,3), (1\,3\,2), \qquad & H(1\,3) = H(1\,2\,3) = (1\,3), (1\,2\,3), \\ (2\,3)H = (1\,2\,3)H = (2\,3), (1\,2\,3), \qquad & H(2\,3) = H(1\,3\,2) = (2\,3), (1\,3\,2). \end{aligned}$$

**Lemma 2.5.4.** *Let $H \leqslant G$ and $g, k \in G$. Then $gH = kH$ if and only if $g^{-1}k \in H$. Similarly $Hg = Hk$ if and only if $kg^{-1} \in H$.*

*Proof.* content... □

*Remark* 4. This allows us to put an equivalence relation on $G$ by making $g \sim h$ if and only if $g^{-1}h \in H$. The equivalence classes of this relation are the left cosets of $H$.

From the examples that have been given so far you may have noticed that in the case where $G$ is finite and $H \leqslant G$, we have that $|H| \mid |G|$. This is not a coincidence! The following theorem is known as Lagrange's theorem.

**Theorem 2.5.5.** *Let $G$ be a finite group and $H \leqslant G$. Then the order of $H$ divides the order of $G$.*

*Proof.* content... □

The converse of Lagrange's theorem is false in general. However, we will see some partial converses to Lagrange's theorem.

**Example.** Find all the subgroups of $C_{31}, D_5$ and $C_5 \times C_5$.

*Proof.* content... □

**Proposition 2.5.6.** *Let $G$ be a finite group. Then $o(g)$ divides $|G|$ for all $g \in G$.*

*Proof.* content... □

The converse of this is obviously false. Otherwise this would imply that every finite group is cyclic.

**Corollary 2.5.7.** *Let $G$ be a group such that $|G| = p$ where $p$ is prime. Then $G$ is cyclic.*

*Proof.* content... □

The following two theorems are very useful in cryptography. The first is known as Fermat's little theorem and was proved by Fermat in 1640.

**Theorem 2.5.8.** *Let $p$ be a prime number and $a \in \mathbb{Z}$ be an integer such that $p$ does not divide $a$. Then*

$$a^{p-1} = 1 \mod p.$$

*Proof.* content... □

The second is an extension of this proved by Euler. It requires Euler's phi function which counts the number of integers coprime to $n$.

**Definition 2.5.9.** Euler's $\phi$-function is defined to be the number of integers $0 < i < n$ such that $i$ and $n$ are coprime.

The following allows one to calculate $\phi(n)$ we will not prove it here.

**Theorem 2.5.10.** *Euler's $\phi$-function satisfies the following three properties.*

- *For prime numbers $p$, $\phi(p) = p - 1$,*
- *For prime numbers $p$, $\phi(p^k) = p^k - p^{k-1}$,*
- *If $n, m$ are coprime integers, then $\phi(mn) = \phi(m)\phi(n)$.*

We are now ready for Euler's theorem from 1736.

**Theorem 2.5.11.** *Let $a, n$ be integers such that $a$ and $n$ are coprime. Then*

$$a^{\phi(n)} = 1 \mod n.$$

*Proof.* content... □

**Corollary 2.5.12.** *If $p$ is a prime, then $(p-1)! = -1 \mod p$.*

*Proof.* content... □

**Corollary 2.5.13.** *Let $G$ be a group of even order. Then there is an element of order 2.*

*Proof.* content... □

**Theorem 2.5.14.** *Let $p \geqslant 3$ be a prime number. Then any group of order $2p$ is either $D_p$ or $C_{2p}$.*

*Proof.* content... □

## 2.6 Homomorphisms and isomorphisms

In linear algebra we have a natural notion of map between vector spaces, namely that of a linear map. In group theory we have the following,

**Definition 2.6.1.** Let $(G, *_G)$ and $(H, *_H)$ be groups. A map $\phi\colon G \to H$ is called a *homomorphism* if $\phi(x *_G y) = \phi(x) *_H \phi(y)$ for all $x, y \in G$.

A bijective homomorphism is called an *isomorphism*. If there is an isomorphism $\phi\colon G \to H$, then we write $G \cong H$.

Much like vector spaces isomorphism gives an equivalence relation on the class of groups.

**Proposition 2.6.2.** *Let $G$ be a cyclic group. If $G$ is finite, then there is an $n$ such that $G \cong C_n$. If $G$ is infinite, then $G \cong \mathbb{Z}$.*

*Proof.* content... □

**Theorem 2.6.3.** *Let $m, n$ be coprime integers. Then $C_m \times C_n$ is isomorphic to $C_{mn}$.*

With other theorems we have seen we can now classify all groups of order up to 7.

**Theorem 2.6.4.** *Up to isomorphism, the groups of order $\leqslant 7$ are:*

- *Order 1: $\{e\}$.*
- *Order 2: $C_2$.*
- *Order 3: $C_3$.*
- *Order 4: $C_4$ or $C_2 \times C_2$.*
- *Order 5: $C_5$.*
- *Order 6: $C_6$ or $D_3$.*
- *Order 7: $C_7$.*

This situation becomes much more complicated for larger orders. There are already 5 groups of order 8.

**Definition 2.6.5.** An *automorphism* is an isomorphism from $G$ to $G$.
A *endomorphism* is a homomorphism from $G$ to $G$.
An injective homomorphism is called a *monomorphism*.
A surjective homomorphism is called a *epimorphism*.

**Proposition 2.6.6.** *Let $\phi\colon G \to H$ be a homomorphism. Then the following hold:*

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

*Proof.* content... □

**Proposition 2.6.7.** *Let $G$ and $H$ be group and $\phi\colon G \to H$ be a homomorpshism. Then $o(\phi(g))$ divides $o(g)$ for all $g \in G$. Moreover if $\phi$ is an isomorphim, then $o(\phi(g)) = o(g)$.*

*Proof.* content... □

**Example.** The map $\mathbb{Z} \to C_n$ given by $k$ goes to $g^k$ is a homomorphism.

**Example.** If $H$ is a subgroup of $G$, then the inclusion map $i\colon H \to G$ given by $i(h) = h$ is a homomorphism.

**Example.** For any groups $G$ and $H$. The map $\phi\colon G \to H$ given by $\phi(g) = e_H$ is a homomorphism.

**Example.** Let $G$ and $H$ be groups. Then the maps

$$\pi_1\colon G \times H \to G \qquad \pi_1((g,h)) = g$$

and

$$\pi_2\colon G \times H \to H \qquad \pi_2((g,h)) = h$$

are homomorphisms.

**Example.** The map $\det\colon S_n \to \{1,-1\}$ given by

$$\det(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

is a homomorphism.

**Example.** The map $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}$ is a homomorphism.

**Example.** The maps $\operatorname{trace}\colon M_n(\mathbb{R}) \to \mathbb{R}$ is a homomorphism.

**Example.** The map $\log\colon (0,\infty) \to \mathbb{R}$ is a homomorphism. Moreover it has an inverse $\exp\colon \mathbb{R} \to (0,\infty)$ so it is in fact an isomorphism.

**Example.** The map $\phi\colon \mathbb{R} \to \mathbb{C} \setminus \{0\}$ given by $\phi(x) = e^{ix}$ is a homomorphism.

**Example.** The map $\phi\colon \mathbb{C} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ given by $\phi(z) = |z|$ is a homomorphism.

**Definition 2.6.8.** Let $G$ be a group and $a \in G$. We can associate to $a$ the map $\theta_a\colon G \to G$ given by $\theta_a(g) = a^{-1}ga$. This is known as *conjugating* by $a$.

Given $g, h \in G$ we say that $g$ and $h$ are *conjugate* if there is an $a \in G$ such that $h = \theta_a(g)$.

**Proposition 2.6.9.** *Conjugation by $a$ is an isomorphism for every $a \in G$.*

*Proof.* content... □

**Corollary 2.6.10.** *If $g$ and $h$ are conjugate, then $o(g) = o(h)$.*

*If $g$ and $h$ are conjugate, then $g^{-1}$ and $h^{-1}$ are conjugate.*

**Proposition 2.6.11.** *All homomorphism $\mathbb{Z} \to \mathbb{Z}$ are of the form $x \mapsto nx$ for some $n \in \mathbb{Z}$.*

*Proof.* content... □

**Proposition 2.6.12.** *Let $G$ be a group. Then any homomorphism $\mathbb{Z} \to G$ is of the form $n \mapsto g^n$ for some $g \in G$.*

*Proof.* content... □

Similarly to linear maps we have a notion of kernel and image. In linear algebra these are subspaces in group theory, unsurprisingly, these are subgroups.

**Definition 2.6.13.** Let $\phi\colon G \to H$ be homomorphism between two groups.

The *kernel* of $\phi$, written $\ker(\phi)$ is

$$\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}.$$

The *image* of $\phi$, written $\mathrm{Im}(\phi)$ is

$$\mathrm{Im}(\phi) = \{h \in H \mid \exists g \in G \text{ s.t. } \phi(g) = h\}.$$

**Proposition 2.6.14.** *Let $\phi\colon G \to H$ be a homomorphism. Then $\ker(\phi) \leqslant G$ and $\mathrm{Im}(\phi) \leqslant H$.*

*Proof.* content... □

**Example.** The map $\phi\colon \mathbb{Z} \to C_n$ given by $k \mapsto g^k$ has kernel $n\mathbb{Z}$ and image $C_n$.

**Example.** The map $\det\colon S_n \to \{1, -1\}$ has kernel $A_n$ and image $\{1, -1\}$.

**Example.** The maps $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}$ has kernel $SL_n(\mathbb{R})$ and image $\mathbb{R}$.

We end our discussion here with a first step to proving the first isomorphism theorem.

**Proposition 2.6.15.** *A homomorphism is constant on cosets of $\ker(\phi)$ and takes different values on different cosets.*

*Proof.* content... □

**Corollary 2.6.16.** *A homomorphism is injective if and only if $\ker(\phi) = \{e_G\}$.*

## 2.7 Normal subgroups and quotients

In this section we will talk about quotient groups. These form some of the key ideas in group theory. They have the downside of begin very abstract, so don't worry if this isn't familiar first time round.

Recall, that if $G$ is a group and $H \leqslant G$, then $G/H$ is the set of left cosets of $H$ in $G$.

**Definition 2.7.1.** Let $H$ be a subgroup of $G$. Then $H$ is a *normal* subgroup, denoted $H \lhd G$, if for all $g \in G$ we have

$$Hg = gH.$$

One can say that $H$ is normal if left cosets and right cosets agree.

WARNING: This does not mean that $hg = gh$ for all $g \in G$ and $h \in H$.

There are always 2 normal subgroups of any group $G$. These are $G$ and $\{e\}$. If there are no other normal subgroups, then $G$ is called *simple.*

**Proposition 2.7.2.** *If $H$ is a subgroup of $G$ and $|G/H| = 2$, then $H$ is a normal subgroup.*

*Proof.* content... □

**Definition 2.7.3.** Let $G$ be a group. Then the *centre* of $G$, denoted $Z(G)$, is the set

$$Z(G) = \{g \in G \mid hg = gh \text{ for all } h \in G\}.$$

**Proposition 2.7.4.** *Let $G$ be a group. Then $Z(G) \lhd G$.*

*Proof.* content... □

**Proposition 2.7.5.** *Let $\phi\colon G \to H$ be a homomorphism. Then* $\ker(phi) \lhd G$.

*Proof.* content... □

One could try and define a binary operation on the set $G/H$ by defining $g_1H * g_2H = g_1g_2H$. However one must check that it does not matter which choice of $g_1$ and $g_2$ are used. This is the key reason for defining normal subgroups.

**Proposition 2.7.6.** *Let $H \leqslant G$. Then the binary operation $g_1H * g_2H = g_1g_2H$ is well defined if and only if $H$ is normal.*

*If $H$ is a normal subgroup of $G$. Then $(G/H, *)$ is a group.*

*Proof.* content... □

**Definition 2.7.7.** If $H \lhd G$, then $(G/H, *)$ is the *quotient group.*

**Proposition 2.7.8.** *Let $G$ be a group and $H \leqslant G$. Then $H\lhd$ if and only if it is the kernel of some homomorphism.*

*Proof.* content... □

**Example.** Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. $H$ is a normal subgroup of $G$. We can see that the quotient $G/H = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$. This can naturally be identified with the integers modulo $n$, or the cyclic group of order $n$.

**Example.** Let $G = S_n$ and $H = A_n$. Then $G/H = \{A_n, (1\,2)A_n\} \cong C_2$.

**Example.** Let $G = \mathbb{C}^*$ and $H = \{z \in \mathbb{C} \mid |z| = 1\}$. Then $G/H \cong (0, \infty)$. Essentially we have forgotten the argument of the complex number and just remembered the modulus.

**Example.** Let $G = AGL_n(\mathbb{R})$, denote the group of affine linear transformations. I.e. functions $\mathbb{R}^n \to \mathbb{R}^n$ which are of the form $x \mapsto Ax + b$ where $A \in GL_n(\mathbb{R})$ and $b \in \mathbb{R}^n$. Let $T$ be the subgroup consisting of translations, that is the subgroup where $A = \mathrm{id}$.

$T$ is a normal subgroup of $G$. And $G/T \cong GL_n(\mathbb{R})$.

## 2.8 Isomorphism theorems

Understanding quotient groups can be hard, especially understanding them in the abstract. To make this study easier, we have the first isomorphism theorem. This allows us to identify a quotient with a certain image in another group.

**Theorem 2.8.1.** *Let $G$ and $H$ be groups and $\phi\colon G \to H$ be a homomorphism. Then $G/\ker(\phi) \cong \mathrm{Im}(\phi)$.*

*Proof.* content... □

**Corollary 2.8.2.** *Let $\phi\colon G \to H$ be a homomorphism. Assume $G$ is finite. Then $|G| = |\mathrm{Im}(\phi)| \times |\ker(\phi)|$.*

**Example.** For $\det\colon S_n \to \{-1, 1\}$, the above reads that $S_n/A_n \cong C_2$.

**Example.** For $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}^*$. The isomorphism theorem reads

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*.$$

**Example.** For the projection onto the first coordinate $G_1 \times G_2 \to G_1$. The isomorphism theorem reads that $(G_1 \times G_2)/(\{e\} \times G_2) \cong G_1$.

**Example.** For $\phi\colon \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = nx$, the isomorphism theorem reads that $\mathbb{Z} \cong \mathbb{Z}/\{0\} \cong n\mathbb{Z}$.

**Example.** For $\phi\colon \mathbb{Z} \to C_n$ given by $\phi(k) = g^k$, the isomorphism theorem tells us that $\mathbb{Z}/n\mathbb{Z} \cong C_n$.

We also have two more isomorphism theorems which are generally less used but can still be very useful.

The second isomorphism theorem reads:

**Theorem 2.8.3.** *Let $G$ be a group, let $H$ be a subgroup and let $N$ be a normal subgroup. Let $HN = \{hn \mid h \in H, n \in N\}$. Then the following hold:*

- $HN \leqslant G$
- $N \lhd HN$
- $H \cap N \lhd H$
- $H/H \cap N \cong HN/N$

*Proof.* content... □

The third isomorphism theorem has many uses. To remember it one can just think that groups work like fractions.

**Theorem 2.8.4.** *Let $G$ be a group and $H, K \lhd G$ and $K \subset H$. Then*

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

*Proof.* content... □

## 2.9 Finitely generated Abelian groups

We will now start looking to classify certain groups. Earlier we saw that we are able to classify all groups of order $< 8$. The classfication theorem for finite groups is a deep problem. We begin with an easier problem, namely classifying the finitely generated abelian groups. The arguments that follow are essentially arguments about vector spaces.

Assume that $G$ is a finitely generated abelian group with generating set $\{g_1, \ldots, g_n\}$. Then there is a homomorphism $\phi\colon \mathbb{Z}^n \to G$ given by $(i_1, \ldots, i_n) \mapsto g_1^{i_1} \ldots g_n^{i_n}$. This homomorphism is surjective.

Let $K$ be the kernel of this homomorphism. By the first isomorphism theorem $G$ is isomorphic to $\mathbb{Z}^n/K$ thus if we can understand the subgroups of $\mathbb{Z}^n$ we can understand the finitely generated abelian groups.

**Definition 2.9.1.** We say that $S$ is a *basis* for $\mathbb{Z}^n$ if $S$ generates $\mathbb{Z}^n$ and $|S| = n$.

You may notice that this definition is similar to that of the basis of a vector space.

There is a natural basis for $\mathbb{Z}^n$ (it's the same as the natural basis for $\mathbb{R}^n$) given by $T = \{e_i \mid e_i \text{ has a 1 in the } i\text{-th position and zeroes elsewhere}\}$. Given another basis $S$ for $\mathbb{Z}^n$ there is an isomorphism $\phi_S\colon \mathbb{Z}^n \to \mathbb{Z}^n$ given by taking the $i$-th element of $S$ to $e_i$. This allows us to change the subgroups we are interested in.

**Example.** Consider the basis $S = \{(1,1),(0,1)\}$ for $\mathbb{Z}^2$. Let $K$ be the subgroup $\{(2i, 2i) \mid i \in \mathbb{Z}\}$. Under the above isomorphism the image of $K$ is $\{(2i, 0) \mid i \in \mathbb{Z}\} = 2\mathbb{Z} \times \{0\}$.

We will show that given any subgroup $K$ of $\mathbb{Z}^n$ there is a basis $S$ such that $\phi_S(K) = d_1\mathbb{Z} \times d_2\mathbb{Z} \times \ldots d_r\mathbb{Z}$ where $r \leqslant n$, $d_i$ divides $d_{i+1}$ and $d_i > 0$. We begin with

**Proposition 2.9.2.** *Any subgroup of $\mathbb{Z}^n$ is finitely generated (by at most $n$ generators).*

*Proof.* content... □

The classification theorem for finitely generated abelian groups. Close look at the classification of finite abelian groups.

## 2.10 Group actions

At this point we have met many examples of groups and hopefully many of them have been interesting to you. Some of these groups can be seen as invertible maps from a space to itself.

**Example.** The diherdral group $D_n$ is the group of symmetries of the regular $n$-gon.

**Example.** The group $GL_n(\mathbb{R})$ is the group of invertible linear transformations from $\mathbb{R}^n \to \mathbb{R}^n$.

**Example.** The symmetric group is the group of maps from a set of size $n$ to itself.

Every can be realised as a group of symmetries of some object. This idea leads us to the group actions.

**Definition 2.10.1.** A *left action* of a group $G$ on a set $S$ is a map

$$\rho\colon G \times S \to S,$$

satisfying the following conditions,

- $\rho(e, s) = s$ for all $s \in S$.
- $\rho(g, \rho(h, s)) = \rho(gh, s)$ for all $g, h \in G$ and $s \in S$.

We have mentioned a few examples above however here are a few more.

**Example.** $\mathbb{Z}$ acts on $\mathbb{R}$ by $\rho(n, r) = n + r$.

**Example.** Let $V$ be a vector space and $v \in V$ be a vector. Then $\mathbb{Z}$ acts on $V$ by $\rho(n, w) = w + nv$.

**Example.** The group $S_n$ acts on a set with $n$ elements by $\rho(\sigma, k) = \sigma(k)$.

**Example.** Any group $G$ acts on itself by left multiplication $\rho(g, h) = gh$.

**Example.** Any group $G$ acts on itself by conjugation $\rho(g, h) = ghg^{-1}$.

**Example.** Any group $G$ acts on $\mathcal{P}(G)$ by left multiplication $\rho(g, X) = \{gx \mid x \in X\}$.

**Example.** Any group $G$ acts on $\mathcal{P}(G)$ by conjugation $\rho(g, X) = \{gxg^{-1} \mid x \in X\}$.

**Example.** Let $G$ be a group and $H$ be a subgroup. Then $G$ acts by left multiplication on $G/H$ via $\rho(g, g'H) = gg'H$.

**Example.** Let $G$ be a group and $X$ be a set upon which $G$ acts. Then there is an action of $G$ on $\mathcal{P}(X)$ via $\rho(g, Y) = \{\rho(g, y) \mid y \in Y\}$.

A profitable way of understanding groups is via their actions.

Given a group $G$ and an action of $G$ on a set $S$. We can associate to each group element $g$ a function

$$\begin{aligned} \rho_g\colon S &\to S \\ s &\mapsto \rho(g, s) \end{aligned}$$

Since $\rho$ is an action of $G$ on $S$ we see that $\rho_g \circ \rho_h = \rho_{gh}$. This allows us to see that $\rho_g$ is a bijection for all $g$ since it has a two-sided inverse, namely $\rho_{g^{-1}}$. Thus, we get a map $G \to Sym(S)$.

**Proposition 2.10.2.** *Let $G$ be a group acting on a set $S$. Then the function*

$$G \to Sym(S)$$
$$g \mapsto \rho_g$$

*is a homomorphism.*

*Proof.* content... □

Another way to specify an action is via a homomorphism $G \to Sym(S)$.

## 2.11 Orbits and stabilisers

Throughout, let $G$ be a group acting on a set $S$.

**Definition 2.11.1.** The *orbit* of $s \in S$ is the set

$$Orb(s) = \{t \in S \mid \exists g \in G \text{ such that } t = \rho(g, s)\}.$$

The *stabiliser* of $s \in S$ is the set

$$Stab(s) = \{g \in G \mid \rho(g, s) = s\}.$$

The *fix point set* of $g \in G$ is the set

$$Fix(g) = \{s \in S \mid \rho(g, s) = s\}.$$

**Example.** When $S_n$ acts on $\{1, \ldots, n\}$ there is one orbit. We also have

$$Stab(i) = Sym(\{1, \ldots, n\} \setminus \{i\}) cong S_{n-1}.$$

**Example.** Let $S_n$ act on the subsets of $\{1, \ldots, n\}$. There are $n+1$ orbits, each corresponding to $|Y|$ for $Y \subset X$. Let $Y$ be a set of size $k$. Then

$$Stab(Y) \cong S_k \times S_{n-k}.$$

**Example.** Let $SL_2(\mathbb{C})$ act on $M_{22}(\mathbb{C})$ via $\rho(A, M) = AMA^{-1}$.

Each orbit has a representative of the form

$$M = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix} \qquad \lambda, \mu \in \mathbb{C}$$

if the matrix is diagonalizeable or it has a representative of the form

$$M = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \qquad \lambda \in \mathbb{C}$$

if the matrix is not diagonalizeable.

**Example.** Let $S$ be the set of colouring of the edges of a pentagon red or blue. There is an action of $D_5$ on $S$. As there are 5 edges $|S| = 2^5 = 32$. There are 8 orbits represented by

$$BBBBB \quad BBBBR \quad BBBRR \quad BBRBR$$

$$BBRRR \quad BRBRR \quad BRRRR \quad RRRRR$$

**Example.** When a group $G$ acts on itself by left multiplication i.e. $\rho(g, h) = gh$. There is one orbit. The stabiliser of any element is $\{e\}$.

**Example.** Let $G$ act on itself by conjugation. Then $Stab(h) = \{g \in G \mid ghg^{-1} = h\}$, this is known as the *centralizer of* $h$ and is denoted $C_G(h)$. The orbit of $h$ is the conjugacy class of $h$ denoted $\mathcal{C}_h$.

We call an action with one orbit *transitive*. We call an action where the stabiliser of any element is $\{e\}$ *free*.

**Proposition 2.11.2.** *The orbits of an action partition the set.*

*Proof.* content... □

**Proposition 2.11.3.** *The stabilisers of an action are subgroups.*

*Proof.* content... □

**Proposition 2.11.4.** *If $s$ and $t$ are in the same orbit, then $Stab(s)$ is conjugate to $Stab(t)$.*

*Proof.* content... □

We are now ready to state one of the key theorems about group actions.

**Theorem 2.11.5.** *The Orbit Stabiliser Theorem*
*Let $G$ be a finite group acting on a set $S$ and let $s \in S$. Then*

$$|Orb(S)||Stab(S)| = |G|.$$

*Proof.* content... □

**Corollary 2.11.6.** *Let $G$ be a group, then $|\mathcal{C}_h| = |G : C_G(h)|$.*

*Proof.* content... □

We can now also immediately see that the size of an orbit divides the size of $G$.

**Example.** Determine the number of conjugates of (123) in $S_5$

**Proposition 2.11.7.** *A group of order $p^r$ has non-trivial centre.*

*Proof.* content... □

**Proposition 2.11.8.** *A group of order $p^2$ is isomorphic to either $C_p \times C_p$ or $C_{p^2}$.*

*Proof.* content... □

**Theorem 2.11.9.** *Cauchy's theorem*
*Let $p$ be a prime number dividing $|G|$. Then there is an element of $G$ of order $p$.*

*Proof.* content... □

### 2.12 Sylow theorems and simple groups

With groups we can try and break them down to pieces that are small in some particular sense.

# 3 Rings

## 3.1 Basic definitions

Rings are much like groups except they have two binary operations. While this may feel like more abstraction you have actually been using rings all your life!

**Definition 3.1.1.** A *ring* $(R, +, \times)$ is a set $R$ together with two binary operation $+$ and $\times$. These operations satisfy the following axioms:

- $(R, +)$ is an abelian group. Since this is an abelian group, we write 0 or $0_R$ for the identity element of this group.
- $\times$ is an associative binary operation, i.e. $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.
- $\times$ is distributive over $+$, i.e. $a \times (b + c) = (a \times b) + a \times c$, for all $a, b, c \in R$.

**Notation 3.1.2.** We will often drop $\times$ in notation, $ab$ for $a \times b$. Much like when we dropped the $*$ in group theory.

*Remark* 5. If the operations $+$ and $\times$ are clear from context we will just write $R$ for $(R, +, \times)$.

**Definition 3.1.3.** We say that a ring is *commutative* if $\times$ is a commutative binary operation, i.e. $ab = ba$.

**Definition 3.1.4.** We say that a ring has an *identity*, if there is an element $1_R \in R$ such that $1_R r = r = r 1_R$ for all $r \in R$. We also require that $1_R \neq 0_R$.

We will study rings that have an identity also we will mostly be interested in commutative rings although some examples will be non-commutative.

The following simple algebra facts are left as an exercise.

**Proposition 3.1.5.** *Let $R$ be a ring with an identity and $a, b, c \in R$.*

- *If $a + b = a + c$, then $b = c$.*
- $-(-a) = a$.
- $a \times 0_R = 0_R = 0_R \times a$.
- $-ab = -a(b) = a(-b)$.
- $(-1_R)a = -a = a(-1_R)$.

**Example.** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings with the usual operations of $+$ and $\times$. In each case $0_R = 0$ and $1_R = 1$.

**Example.** The ring of integers modulo $n$ is a ring with the standard operations of addition and multiplication.

**Example.** Given two rings $(R, +_R, \times_R)$ and $(S, +_S, \times_S)$. Then the *direct sum*, $R \oplus S$ of $R$ and $S$ is the ring with underlying set $R \times S$ and

$$(r, s) + (r', s') = (r +_R r', s +_S s')$$

and

$$(r, s) \times (r', s') = (r \times_R r', s \times_S s').$$

**Example.** $C(\mathbb{R})$, the set of continuous functions from $\mathbb{R} \to \mathbb{R}$ is a ring with pointwise addition and pointwise multiplication. $0_{C(\mathbb{R})}$ is the zero function and $1_{C(\mathbb{R})}$ is the constant function 1.

To prove that this is a ring we need the basic calculus fact that if $f, g$ are continuous functions, then $f + g$ and $fg$ are continuous functions.

**Example.** The set of even integers $2\mathbb{Z}$ is a commutative ring although it does not have an identity.

**Example.** The set of $n \times n$ matrices with real coefficients is a non commutative ring. It has an identity, namely the identity matrix.

**Example.** We can extend the above example to $n \times n$ matrices with coefficients in any ring $R$. This will be denoted $M_n(R)$.

**Example.** The power set $\mathcal{P}(X)$ of a set $X$ with the operations symmetric difference $\triangle$ and intersection $\bigcap$ forms a commutative ring.

Recall $A \triangle B = A \setminus B \cup B \setminus A$.

**Definition 3.1.6.** Let $R$ be a ring. A non-empty subset $S$ of $R$ is a *subring* if for all $r, s, t \in S$ we have that $r - st \in S$.

Equivalently $S$ is a ring with the operations coming from $R$.

**Example.** $\mathbb{Z}$ is a subring of $\mathbb{Q}$ which is a subring of $\mathbb{R}$ which is a subring of $\mathbb{C}$.

**Example.** Matrices with real coefficients form a subring of the matrices with complex coefficients.

There are certain elements in a ring which can be of particular interest. The first is that of a unit.

**Definition 3.1.7.** A *unit* in a ring $R$ is a non-zero element $a$ such that there exists a $b$ such that $ab = 1 = ba$.

Units are the elements of a ring which have a multiplicative inverse.

**Example.** In $\mathbb{Z}$ the units are $1, -1$. In $\mathbb{Q}$ the units are all non-zero elements this is also true in $\mathbb{R}$ and $\mathbb{C}$.

**Example.** For the ring $n \times n$ matrices with real coefficients, the units are the invertible matrices. We met these earlier in the course as $GL_n(\mathbb{R})$.

**Example.** In the ring $C(\mathbb{R})$ of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, the units are the functions which are never 0.

Nicely we have the following.

**Theorem 3.1.8.** *The units in a ring $R$ form a group under multiplication.*

*Proof.* content... □

We have seen some examples where most elements are units i.e. $\mathbb{Q}$ and $\mathbb{R}$. These rings are known as fields.

**Definition 3.1.9.** A commutative ring $R$ is a *field* if every non-zero element is a unit.

**Example.** The rings $\mathbb{Q}$ and $\mathbb{R}$ are fields.

**Example.** The ring $\mathbb{Z}_7$ is a field. In fact, $\mathbb{Z}_n$ is a field if and only if $n$ is prime.

In the other direction we have zero-divisors.

**Definition 3.1.10.** A zero-divisor in a ring $R$ is a non-zero element $a$ such that there is are elements $b, c$ such that $ab = 0 = ca$.

**Example.** The zero divisors in $\mathbb{Z}_6$ are $2, 3, 4$.

**Example.** The zero-divisors in $C(\mathbb{R})$ are the functions which are zero on $(a, b)$ for some $a, b \in \mathbb{R}$.

**Example.** In $\mathcal{P}(X)$ every non-empty set is a zero-divisor.

**Definition 3.1.11.** A ring which contains no zero-divisors is an *integral domain*.

**Example.** The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are integral domains.

**Example.** If $R$ is an integral domain and $S$ is a subring of $R$, then $S$ is an integral domain.

**Example.** Any field is an integral domain.

This is a consequence of the following.

**Proposition 3.1.12.** *An element cannot be both a zero-divisor and a unit. There are rings with elements that are neither a zero-divisor nor a unit.*

*Proof.* content... □

## 3.2 Polynomial Rings

Given a ring $R$ we have a well defined notion of addition and multiplication we can use this to define new rings such as the ring of matrices with coefficients in $R$ or polynomial rings.

**Example.** If $R$ is a ring, then we can consider $R[x]$ the ring of polynomials with coefficients in $R$. If $R$ is commutative, then $R[x]$ is commutative. If $R$ has an identity, then $R[x]$ has an identity, namely the constant polynomial $1_R$. Explicitly given two polynomials $p(x) = \sum_i a_i x^i$ and $q(x) = \sum_i b_i x^i$. Then

$$p(x) + q(x) = \sum_i (a_i + b_i)x^i \qquad p(x)q(x) = \sum_k \sum_{i+j=k} a_j b_i x^k.$$

We can define polynomials rings in several variables by

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x].$$

**Definition 3.2.1.** We say that the *degree* of a polynomial $p(x) = \sum_i a_i x^i \in R[x]$ is $\deg(p) = \max\{i \mid a_i \neq 0\}$.

Note that, in general, we do not have the equality $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$.

**Example.** Let $R = \mathbb{Z}_4[x]$ and $p(x) = q(x) = 2x + 1$. Then

$$p(x)q(x) = 4x^2 + 4x + 1 = 1.$$

But $\deg(p(x)) = \deg(q(x)) = 1$ and $\deg(p(x)q(x)) = 0$.

Also note that factorisation is not unique.

**Example.** The polynomial $x^2 - 1 \in \mathbb{Z}_8[x]$ has the following factorisations

$$x^2 - 1 = (x + 1)(x - 1) = (x - 3)(x - 5).$$

These properties are mysterious at first glance as both are things that naturally work when we consider polynomials with integer or even real coefficients. In fact we can summarise this failure in terms of the original ring $R$.

**Theorem 3.2.2.** *Let $R$ be a ring. $R$ is an integral domain if and only if $R[x]$ is an integral domain.*

*Proof.* content... □

**Theorem 3.2.3.** *If $R$ is an integral domain, then the equality* $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ *holds in* $R[x]$.

*Proof.* content... □

The failure of factorisation is a little more complicated and is beyond the scope of this course cf. unique factorisation domains. Later we will look at the case of fields.

## 3.3 Ideals and homomorphisms

From this point onwards all rings will be assumed to be commutative.

In groups we looked at normal subgroups and quotient groups. We will now look at the analogue of this in rings. The corresponding concept is known as an ideal

**Definition 3.3.1.** A non-empty subset $I$ of a ring $R$ is an ideal if the following are satisfied.

1. If $i, j \in I$, then $i - j \in I$.
2. If $i \in I$ and $r \in R$, then $ri \in I$.

If $I$ is an ideal of $R$, then we write $I \lhd R$.

**Definition 3.3.2.** Let $R$ be a ring and $a \in R$. The *principal ideal* generated by $a$, denoted $(a)$ is the smallest ideal containing $a$. So

$$(a) = \{ra \mid r \in R\}.$$

An ideal $I$ is said to be *principal* if there is an element $a \in R$ such that $I = (a)$.

**Example.** The sets $\{0_R\}$ and $R$ are always ideals of $R$.

**Example.** The $\{f \in C(\mathbb{R}) \mid f(0) = 0\}$ is an ideal in $C(\mathbb{R})$.

**Definition 3.3.3.** The *ideal generated by* $\{a_1, \ldots, a_k\}$ is

$$(a_1, \ldots, a_k) = \{r_1a_1 + r_2a_2 + \cdots + r_ka_k\}$$

is the smallest ideal containing $a_1, \ldots, a_k$.

**Example.** Let $R = \mathbb{Z}[x]$ and $I = (2, x)$. This is an example of an ideal which is non-principal.

**Proposition 3.3.4.** *The ideal in* $\mathbb{Z}$ *are* $n\mathbb{Z}$ *for some integer* $n$.

*Proof.* content... □

**Proposition 3.3.5.** *$R$ is a field if and only if the only ideals are $\{0\}$ and $R$.*

*Proof.* content... □

In groups we could take quotients by normal subgroups to create new groups. In rings we can do the same thing with ideals.

**Definition 3.3.6.** Let $R$ be a ring and $I \lhd R$ be an ideal. The *coset* of $r \in R$ is

$$r + I = \{r + i \mid i \in I\}.$$

We denote the *set of cosets* $\dfrac{R}{I}$.

**Proposition 3.3.7.** *Let $R$ be a ring and $I \lhd R$ be an ideal. $(\dfrac{R}{I}, \oplus, \otimes)$ forms a ring, where*

$$(r + I) \oplus (s + I) = (r + s) + I$$
$$(r + I) \otimes (s + I) = (rs) + I.$$

*Proof.* content... □

Similarly to our study of groups there is a notion of homomorphism between rings.

**Definition 3.3.8.** Let $R$ and $S$ be rings. A map $\psi\colon R \to S$ is a *ring homomorphism* if the following hold,

1. $\psi(a +_R b) = \psi(a) +_S \psi(b)$
2. $\psi(a \times_R b) = \psi(a) \times_S \psi(b)$

**Example.** The map $\psi\colon \mathbb{Z} \to \mathbb{R}$ given by $\psi(n) = n$ is a ring homomorphism.

**Example.** Let $R$ be a commutative ring with an identity and $a \in R$. Then the map $\psi\colon R[x] \to R$ given by $\psi(p) = p(a)$ is a ring homomorphism.

Sometimes we will just say homomorphism when it is clear we are talking about rings.

**Proposition 3.3.9.** *Let $R, S$ be rings and $\psi\colon R \to S$ be a ring homomorphism. Let $r \in R$ and $n$ be an integer. Then*

1. *$\psi(0_R) = 0_R$*
2. *If $R$ has an identity and $S$ is an integral domain, then either $\psi(a) = 0$ for all $a \in R$ or $\psi(1_R) = 1_S$.*
3. *$\psi(nr) = n\psi(r)$*
4. *If $n > 0$, then $\psi(r^n) = \psi(r)^n$.*

*Proof.* content... □

**Definition 3.3.10.** A *ring isomorphism* is a bijective ring homomorphism. We say two rings are *isomorphic* if there is an isomorphism between them. If $R$ and $S$ are isomorphic we write $R \cong S$.

**Example.** Complex conjugation is a ring isomorphism from $\mathbb{C}$ to $\mathbb{C}$.

Once again we have an notion of kernel and image.

**Definition 3.3.11.** Let $R, S$ be rings and $\psi\colon R \to S$ be a ring homomorphism.
The *image* of $\psi$ is the set $\mathrm{Im}(\psi) = \{s \in S \mid s = \psi(r) \text{ for some } r \in R\}$.
The *kernel* of $\psi$ is the set $\ker(\psi) = \{r \in R \mid \psi(r) = 0_S\}$.

**Proposition 3.3.12.** *Let $R, S$ be rings and $\psi\colon R \to S$ be a ring homomorphism. Then $\mathrm{Im}(\psi)$ is subring of $S$ and $\ker(\psi)$ is an ideal of $R$.*

*Proof.* content... □

**Example.** Let $R$ be a ring and $\psi\colon R[x] \to R$ be the homomorphism given by $\psi(p) = p(a)$. Then $\ker(\psi) = (x - a)$ and $\mathrm{Im}(\psi) = R$.

**Example.** The kernel and image of the map $\psi\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $x \mapsto \bar{x}$ are

$$\ker(\psi) = n\mathbb{Z} \text{ and } \mathrm{Im}(\psi) = \mathbb{Z}_n.$$

**Example.** Consider the homomorphism $\psi\colon \mathbb{R}[x] \to \mathbb{C}$ given by $\psi(p) = p(i)$. The kernel $\ker(\psi) = (x^2 + 1)$ and $\mathrm{Im}(\psi) = \mathbb{C}$.

In groups we had isomorphism theorems which allowed us to understand the image of a homomorphism through quotients. We have an almost exact replica of this theorem for rings.

**Theorem 3.3.13.** *Let $R, S$ be rings and let $\psi\colon R \to S$ be a ring homomorphism. Then*

1. $\ker(\psi) \lhd R$,
2. $\mathrm{Im}(\psi)$ *is a subring of* $S$,
3. $\dfrac{R}{\ker(\psi)} \cong \mathrm{Im}(\psi)$.

*Proof.* content... □

**Example.** Let $R$ be a ring and $\psi\colon R[x] \to R$ be the homomorphism given by $\psi(p) = p(a)$. Then the isomorphism theorem tells us that $\dfrac{R[x]}{(x-a)} \cong R$.

**Example.** The isomorphism theorem applied to $\psi\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $\psi(x) = \bar{x}$ says that $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$.

**Example.** The isomorphism theorem applied to the map $\psi\colon \mathbb{R}[x] \to \mathbb{C}$ given by $\psi(p) = p(i)$ tells us that $\dfrac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{C}$.

Given 2 ideals there are several operations we can perform to produce a new ideal.

**Definition 3.3.14.** Let $R$ be a ring and $I$ and $J$ be ideals. Then the following are also ideals.

1. The *sum* of $I$ and $J$ is
$$I + J = \{i + j \mid i \in I, j \in J\}.$$
2. The *intersection* of $I$ and $J$ is
$$\{r \mid r \in I \text{ and } r \in J\}.$$
3. The *product* of $I$ and $J$ is
$$IJ = \{\sum_k i_k j_k \mid i_k \in I, j_k \in J, k \in \mathbb{N}\}.$$

We say that $I$ and $J$ are *coprime* if $I + J = R$.

**Example.** If $m, n$ are integers and $I = (m)$ and $J = (n)$, then

1. the sum $I + J = (hcf(m, n))$.
2. the intersection $I \cap J = (lcm(m, n))$
3. the product $IJ = (mn)$.

Thus we can see that the ideal $(m)$ and $(n)$ are coprime if and only if there highest common factor is 1, i.e. $m$ and $n$ are coprime in the usual sense.

**Proposition 3.3.15.** *Let $I$ and $J$ be ideals. Then $IJ \subset I \cap J$. Moreover if $I$ and $J$ are coprime, then $IJ = I \cap J$.*

*Proof.* content... □

We are now ready to discuss the Chinese remainder theorem.

**Theorem 3.3.16.** *Let $I$ and $J$ be coprime ideals of a ring $R$. Then the map*
$$\psi\colon \frac{R}{I \cap J} \to \frac{R}{I} \oplus \frac{R}{J} \qquad \text{given by} \qquad r + I \cap J \mapsto (r + I, r + J)$$
*is an isomorphism*

*Proof.* content... □

Noting that with the above proposition we get the following corollary.

**Corollary 3.3.17.** *Let $I$ and $J$ be coprime ideals of a ring $R$. Then*

$$\frac{R}{IJ} \cong \frac{R}{I} \oplus \frac{R}{J}.$$

This is particularly useful in the integers.

**Corollary 3.3.18.** *If $m$ and $n$ are coprime, then*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m.$$

Given a list of congruences we can find the congruence in a product.

**Example.** Find $x \mod 165$ given that

$$x \equiv 1 \mod 11$$
$$x \equiv 2 \mod 15$$

## 3.4 Polynomial rings pt. 2

If the ring we start with is a field, then $R[x]$ has some nice features giving some similarity to the ring $\mathbb{Z}$. Namely we have a Euclidean algorithm.

First let us recall the Euclidean algorithm in $\mathbb{Z}$. Given two integers $a, b$ we can find integers $n, r$ such that $0 \leqslant r < b$ and $a = nb + r$.

This is what is known as a division algorithm or Euclidean algorithm. The first consequence is the following.

**Theorem 3.4.1.** *Given integers $a, b$ there are integers $n, m$ such that*

$$na + mb = \gcd(a, b).$$

*Proof.* content... □

One can use this to show that any integer has a unique factorisation as a product of prime numbers.

We can similarly do this in the polynomial ring over a field.

**Proposition 3.4.2.** *Let $R$ be a field. Let $p(x), q(x) \in R[x]$. Then there are polynomials $f, g \in R[x]$ such that $0 \leqslant deg(g) < deg(q)$ and*

$$p = fq + g.$$

*Proof.* content... □

This allows us to factorise a polynomial in a unique way.

**Definition 3.4.3.** Let $R$ be a ring. A polynomial $f(x) \in R[x]$ is *irreducible* if $f(x)$ cannot be written as a product of polynomials of smaller degree.

**Definition 3.4.4.** A polynomial is *monic* if the leading coefficient is 1.

**Theorem 3.4.5.** *Let $R$ be a field. Every polynomial $f(x) \in R[x]$ can be written as a product $ap_1p_2 \dots p_k$ where $a \in R$ and $p_i$ is an irreducible, monic polynomial.*

*Proof.* content... □

The above factorisation is in fact unique although we will not prove that here.

## 3.5 Prime and maximal ideals

**Definition 3.5.1.** Let $R$ be a ring. An ideal $I$ is proper is $I \subsetneq R$.

Note that $I$ is a proper ideal if and only if the quotient $R/I$ is non-trivial.

**Definition 3.5.2.** Let $R$ be a commutative ring. We say that an ideal is prime if it is a proper ideal and given $a, b \in R$ such that $ab \in I$, then $a \in I$ or $b \in I$.

Prime ideals correspond to nice properties of the quotient $R/I$. Namely,

**Theorem 3.5.3.** *Let $I$ be a prime ideal in the ring $R$. Then $R/I$ is an integral domain.*

*Proof.* content... □

**Definition 3.5.4.** A proper ideal $I$ is *maximal* if for all ideals $J$ with $I \subset J$ either $I = J$ or $J = R$.

**Theorem 3.5.5.** *If $I$ is a maximal ideal of $R$, then $R/I$ is a field.*

*Proof.* content... □

# References