3. Groups

3.1 Abstract groups

In Chapter 1, we considered the set $\mathbb{Z}_n = \{0, 1, \ldots, n_0 1\}$ of **remainders modulo** n and saw that it was possible to define the operator $+_n$ on it.

Definition 3.1.1: Abstract group (p69)

A pair $(G, \cdot)$ consisting of

- a set G,
- a *group operation* $\cdot : G \times G \to G$ (*law of composition*)

is called a **group** if the following axioms are satisfied:

1. **Associativity**: For all $a, b, c \in G$,
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$
2. **Identity element**:
$$\exists e \in G : \forall f \in G, e \cdot f = f \cdot e = f$$
3. **Inverse element**:
$$\forall f \in G : \exists g \in G : f \cdot g = e = g \cdot f$$
The element g is called the **inverse** of f and is denoted by f^{-1}.

Abelian group

A group $(G, \cdot)$ is called **abelian** (or **commutative**) if the LOC satisfies **commutativity**:

$$\forall a, b \in G : a \cdot b = b \cdot a.$$

Examples of groups

- $(\mathbb{Z}, +)$
  - infinitely many elements (**infinite order**)
  - abelian
- $(\mathbb{Q} \setminus \{0\}, \cdot)$
- $(\mathbb{Z}_n, +_n)$

Non-examples of groups

- $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ (not every element has an inverse: 0^{-1} does not exist)
- $(\mathbb{N}, +)$ (not every element has an inverse)
- $(\mathbb{Z}_n, \cdot_n)$ (not every element has an inverse, see below)

📖 **Order of a group (p71)**

The **order** of a group $(G, \cdot)$ is the number of elements in G, that is $|G|$.

- If $|G| = n < \infty$ the group is called a **finite group of order** n.

$$\boxed{\operatorname{ord}(G) = n = |G|}$$

- If $|G| = \infty$ the group is of **infinite order**.

$$\operatorname{ord}(G) = \infty$$

$(\mathbb{Z}_n, \cdot_n)$ is not a group

$(\mathbb{Z}_n, \cdot_n)$ comes close to being a group:

1. It is associative (Theorem 1.4.2).
2. The identity element is 1.
3. However, **not every element has an inverse**.
   - $(\mathbb{Z}_6, \cdot_6)$, 2 has no inverse since there is no $x \in \mathbb{Z}_6$ such that

$$2 \cdot x \equiv 1 \pmod 6 \quad \iff \quad 2x = 1 + 6k \text{ for some } k \in \mathbb{Z}.$$

When does an element $a \in \mathbb{Z}_n$ have an inverse in $(\mathbb{Z}_n, \cdot_n)$?

📜 **Invertibility in $(\mathbb{Z}_n, \cdot_n)$ (p71)**

$$\boxed{a \in \mathbb{Z}_n \text{ has an inverse in } (\mathbb{Z}_n, \cdot_n) \iff \gcd(a, n) = 1}$$

Proof

Take $f \in \mathbb{Z}_n$ and assume $\gcd(f, n) = 1$. We want to find g such that

$$f \cdot_n g = 1$$

Using the Extended Euclidean Algorithm, we can find $r, s \in \mathbb{Z}$ such that

$$r \cdot f + s \cdot n = \gcd(f, n) = 1.$$

We can assume $0 \leq s < n$. Otherwise, replace r by $r + kn$ and s by $s - kf$ for some $k \in \mathbb{Z}$:

$$(r + kn) \cdot f + (s - kf) \cdot n = r \cdot f + s \cdot n = \text{the above} = \gcd(f, n) = 1.$$

Using Definition 1.2.1 of congruence modulo an integer, we have that

$$r \cdot f \equiv 1 \pmod n,$$

which means that $r \cdot_n f = 1$. We can thus **choose** $g = r = f^{-1}$.

Conversely, assume that f has an inverse $f^{-1} = g \in \mathbb{Z}_n$. Then

$$\begin{aligned} f \cdot_n g = 1 &\iff (f \cdot g) \bmod n = 1 \\ &\iff f \cdot g = 1 + k \cdot n \text{ for some } k \in \mathbb{Z} \\ &\iff fg - kn = 1 \end{aligned}$$

By **Bézout's identity** (p29), this implies that $\gcd(f, n) = 1$.

Definition: $\mathbb{Z}_n^*$

A slightly modified version of $(\mathbb{Z}_n, \cdot_n)$ is the set $\mathbb{Z}_n^*$:

$$\boxed{\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}}.$$

This group has order (n), where is the **Euler's totient function** (see below).

Definition: Euler's totient function (n)

The **Euler's totient function** (n) is defined as the **number of elements in** $\mathbb{Z}_n^*$, that is:

$$\boxed{= \begin{cases} \mathbb{Z}_{>0} \to \mathbb{Z}_{>0} \\ n \quad |\mathbb{Z}_n^*| \end{cases}}$$

So $\boxed{(n) = |\mathbb{Z}_n^*|} = \operatorname{ord}(\mathbb{Z}_n^*, \cdot_n)$.

$\mathbb{Z}_n^*$ is a group

The pair $(\mathbb{Z}_n^*, \cdot_n)$ is a group of order (n).

This follows directly from the invertibility theorem above and the fact that $\cdot_n$ is associative (Theorem 1.4.2) and has an identity element (1).

Lemma 3.1.7: Uniqueness of identity element (p72)

Let $(G, \cdot)$ be a group. Then it has **exactly one** identity element.

Note that if $(G, \cdot)$ is $(\mathbb{Z}, +)$, it would be very confusing to write ^{3} if what we meant is $+ \ +$.
$\Rightarrow$ write nf or $n \cdot f$ instead of f^n when the group operation is addition

Exercise 3.21

If $(G, \cdot)$ is a group, then

$$\forall f, g \in G : \boxed{(f \cdot g)^{-1} = g^{-1} \cdot f^{-1}}.$$

Definition 3.1.10: Order of an element (p73)

Let $(G, \cdot)$ be a group and $g \in G$.

- If it exists, the **order of the element** g is

$$\boxed{\operatorname{ord}(g) = \text{smallest positive integer } i \text{ such that } g^i = e}$$

- If $\forall i \in \mathbb{N} : g^i \neq e$, we say that g is of **infinite order** and write

$$\operatorname{ord}(g) = \infty$$

Exercise 3.11

Let $(G, \cdot)$ be a group and $f, g \in G$. Then

1. $\boxed{\operatorname{ord}(f^{-1}) = \operatorname{ord}(f)}$
2. $\boxed{\operatorname{ord}(f \cdot g) = \operatorname{ord}(g \cdot f)}$

Lemma: Order of an element

Let $(G, \cdot)$ be a group and $g \in G$. Then **EITHER**

1. $\operatorname{ord}(g) = \infty$:

$$\mathbb{Z} \to G : i \quad g^i \textbf{ is inective}$$

2. $\operatorname{ord}(g) = i < \infty$:

$$\exists k \in \mathbb{Z}_{\geq 0} : g^k = e \text{ and } g^0, g^1, \ldots, g^{k-1} \textbf{ are distinct}$$

Lemma 3.1.12 (p73)

Let $(G, \cdot)$ be a group and $g \in G$ an element. Then

$$\exists i \in \mathbb{Z}_{>0} : \quad \boxed{g^i = e \Rightarrow \operatorname{ord}(g) \mid i}$$

Conversely, if $i \in \mathbb{Z}_{>0}$ is a multiple of $\operatorname{ord}(g)$, then

$$g^i = e \text{ because } g^{k \cdot \operatorname{ord}(g)} = (g^{\operatorname{ord}(g)})^k = e^k = e$$

Order of identity element

Let $(G, \cdot)$ be a group with identity element e. Then

$$\operatorname{ord}(e) = 1$$

Why?
Because $e^1 = e$ and there is no smaller positive integer than 1.

The identity element is the only element of order 1 (p72)

Let $(G, \cdot)$ be a group with identity element e. Then

$$\forall f \in G : \boxed{\operatorname{ord}(f) = 1 \iff f = e}$$

In other words, the **identity element is the <u>only</u> element of order 1.**

Why?
If $f \in G$ is such that $\operatorname{ord}(f) = 1$, then by definition of order of an element, $f^1 = e$. So $f = e$, because by Lemma 3.1.7, the identity element is **unique**.

3.2 Cyclic groups

Counterclockwise rotations of a regular n-gon (p74)

Denote by r the counterclockwise rotation by $2n$ radians (or $360n$ degrees) around the center of a regular n-gon with vertices $0, 1, \dots, n-1$.

Using the composition operator $\circ$, we can define $\boxed{r^0 = e}, r^1 = r, r^2 = r \circ r, \dots, r^{n-1} = \underbrace{r \circ r \circ \cdots \circ r}_{n-1}$.

We can make a group out of the **rotational symmetries of a regular n-gon** using $\circ$ as the group operation:

$$\boxed{C_n := \{e, r, r^2, \dots, r^{n-1}\} = r}.$$

This is a group:

0. The group operation $\circ$ is a function $C_n \times C_n \to C_n$.
1. The group operation $\circ$ (function composition) is associative (Lemma 2.1.2).
2. The identity element is $e \overset{\Delta}{=} r^0$.
3. The inverse of each element is given by $(r^i)^{-1} = r^{-i}$, satisfying $r^i \circ r^{-i} = e$.

Lemma 3.2.1: identities of $(C_n, \circ)$ (p74)

Let $n \in \mathbb{Z}_{>0}$. Then $(C_n, \circ)$ is a group. The following identities hold:

1. $\boxed{r^n = e}$
2. $\forall i \in [0, n-1] : \boxed{(r^i)^{-1} = r^{(-i) \bmod n}}$
3. $\forall i, j \in [0, n-1] : \boxed{r^i \circ r^j = r^{(i+j \bmod n)} = r^{i +_n j}}$

Definition 3.2.2: Cyclic group (p75)

A group $(G, \cdot)$ is called **cyclic** if any element in G can be written as a power of a single element $g \in G$:

$$\exists g \in G : \quad \boxed{G = g = \{g^i \mid i \in \mathbb{Z}\}}.$$

The element g is called a **generator** of G.

The group $(C_n, \circ)$ is an example of a cyclic group.
In fact, $(C_n, \circ)$ is generated by r:

$$\boxed{C_n = r} = \{\underbrace{r \circ \cdots \circ r}_{i \text{ times}} \mid i \in \mathbb{Z}\} = \{r^{i \bmod n} \mid i \in \mathbb{Z}\} = \{r^i \mid i \in \mathbb{Z}\}.$$

Another example is $(\mathbb{Z}_n, +_n)$, which is generated by 1:

$$\boxed{\mathbb{Z}_n = 1} = \{\underbrace{1 +_n \cdots +_n 1}_{i \text{ times}} \mid i \in \mathbb{Z}\} = \{1^i \mid i \in \mathbb{Z}\}.$$

Lemma 3.2.3: Cyclic if order of an element equals order of group (p75)

Let $(G, \cdot)$ be a **finite** group of order n $(\operatorname{ord}(G) = |G| = n)$. Then

$$\boxed{G \text{ is cyclic} \iff \exists g \in G : \operatorname{ord}(g) = |G| = n}.$$

Also,

$$\boxed{g \in G \text{ is a generator of } G \iff \operatorname{ord}(g) = |G| = n}.$$

In this case, $G = \{e, g, g^2, \ldots, g^{n-1}\}$.

Now the climax of Week 3.2:

Theorem 3.2.5: The order of power theorem (p76)

Let $(G, \cdot)$ be a group and $g \in G$ an element of **finite** order $n = \operatorname{ord}(g)$. Then

$$\forall i \in \mathbb{Z}_{\geq 0} : \quad \boxed{\operatorname{ord}(g^i) = \frac{n}{\gcd(n, i)} = \frac{\operatorname{ord}(g)}{\gcd(\operatorname{ord}(g), i)}}$$

For $i = 0$, we have $\operatorname{ord}(g^0) = n \gcd(n, 0) = nn = 1$.

Corollary 3.2.6 (p76)

Let $(G, \cdot)$ be a finite **cyclic** group of order n. Then

- The order of every element in G divides $\operatorname{ord}(G) = n$:

$$\forall g \in G : \quad \boxed{\operatorname{ord}(g) \mid n} \quad \implies \quad \boxed{\operatorname{ord}(g) \mid \operatorname{ord}(G)}$$

- If $d \mid n$, then there are **exactly** $(d) = |\mathbb{Z}_d^*|$ **elements of order** d **in** G.

This corollary implies that **a finite cyclic group of order n has (n) generators**, because it has (n) elements of order n.

Corollary 3.2.7 (p76)

Let n be a positive integer $(n \in \mathbb{Z}_{>0})$. Then

$$n = {}_{d \text{ divides } n} (d)$$

because $\forall g \in G : \operatorname{ord}(g) \mid \operatorname{ord}(G) = n$ and there are (d) elements of order d for each divisor d of n.

Exercise 4.23

A cyclic group is abelian.

Proof: Let $(G, \cdot)$ be a cyclic group. Then $\exists g \in G$ such that $G = \{g^i \mid i \in \mathbb{Z}\}$.
Take $a, b \in G$. Then $\exists i, j \in \mathbb{Z}$ such that $a = g^i$ and $b = g^j$.

$$a \cdot b = g^i \cdot g^j = g^{i+j} = g^{j+i} = g^j \cdot g^i = b \cdot a.$$

3.3 Dihedral groups

Apart from **rotational** symmetries (which form the group C_n), regular n-gons also have **reflectional symmetries**.

We again enumerate the vertices of a regular n-gon as ${}_0, {}_1, \ldots, {}_{n-1}$. We denote - as before - by r the counterclockwise rotation by $2n$ radians around the center of the n-gon. We have already seen that $\boxed{r[{}_k] = {}_{(k+1) \bmod n}}$.

Now consider the **reflection** symmetry s with ***reflection axis* through** ${}_0$:

- s fixes ${}_0$
- $\forall k \in [1, n-1] : s[{}_k] = {}_{(-k) \bmod n}$

So, we have that

$$\boxed{s[{}_i] = {}_{(-i) \bmod n} = {}_{(n-i) \bmod n}} \qquad \forall i \in [0, n-1].$$

We can compose the symmetries r and s using the composition operator $\circ$.

Lemma 3.3.1 (p78)

Let r and s be the *rotational*, respectively *reflectional* symmetries of a regular n-gon as defined above. Then we have:

1. $\boxed{s^{-1} = s} \iff s \circ s = e \iff \boxed{s^2 = e}$
2. $\forall i \in \{0, \ldots, n-1\} : \boxed{s \circ r^i = r^{-i} \circ s} \quad \Rightarrow \quad \boxed{s \circ r = r^{-1} \circ s}$
   Note that we already knew that $\boxed{r^n = e}$ (Lemma 3.2.1).

Note that (2) implies that D_n is **not abelian** for $n \geq 3$.

3.3.1 consequence: D_n is not abelian for $n \geq 3$ (p78)

Let $n \geq 3$ be an integer and let r, s be the rotational, respectively reflectional symmetries of a regular n-gon as defined above. Then

$$\boxed{s \circ r \neq r \circ s} \qquad (n \geq 3)$$

In other words, the group D_n is **not abelian** for $n \geq 3$.

Why for $n \geq 3$? Because for $n = 2$, we have $r = r^{-1}$, so $s \circ r = r \circ s$.

Theorem 3.3.2: The dihedral group (p78)

Let $n \geq 2$ be an integer and define the **dihedral group** D_n as

$$\boxed{D_n := \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2 s, \ldots, r^{n-1} s\}}.$$

Then the pair $(D_n, \circ)$ forms a group of $\boxed{\textbf{order } 2n}$.

The elements $\{e, r, \ldots, r^{n-1}\}$ correspond to the rotational symmetries of the regular n-gon as we have seen. The elements $\{s, rs, \ldots, r^{n-1}s\}$ correspond to its reflection symmetries.

The **dihedral group** D_n is of order $2n$ because it has n *rotational* symmetries (including e) and n *reflectional* symmetries.

3.4 Products of groups & examples of groups of small order

Theorem 3.4.1: Product of groups (p79)

Let $(G_1, \cdot_1)$ and $(G_2, \cdot_2)$ be groups. Define

$$G_1 \times G_2 := \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

and define

$$\cdot : G \times G \to G : ((f_1, f_2), (g_1, g_2)) \ \ (f_1 \cdot_1 g_1, f_2 \cdot_2 g_2).$$

Then $(G, \cdot)$ is a group.

Definition 3.4.3: The quaternion group (p80)

The **quaternion group** is the group $(, \cdot)$ where

$$:= \{1, -1, i, -i, j, -j, k, -k\}$$

and the group operation $\cdot$ is defined by the following multiplication table:

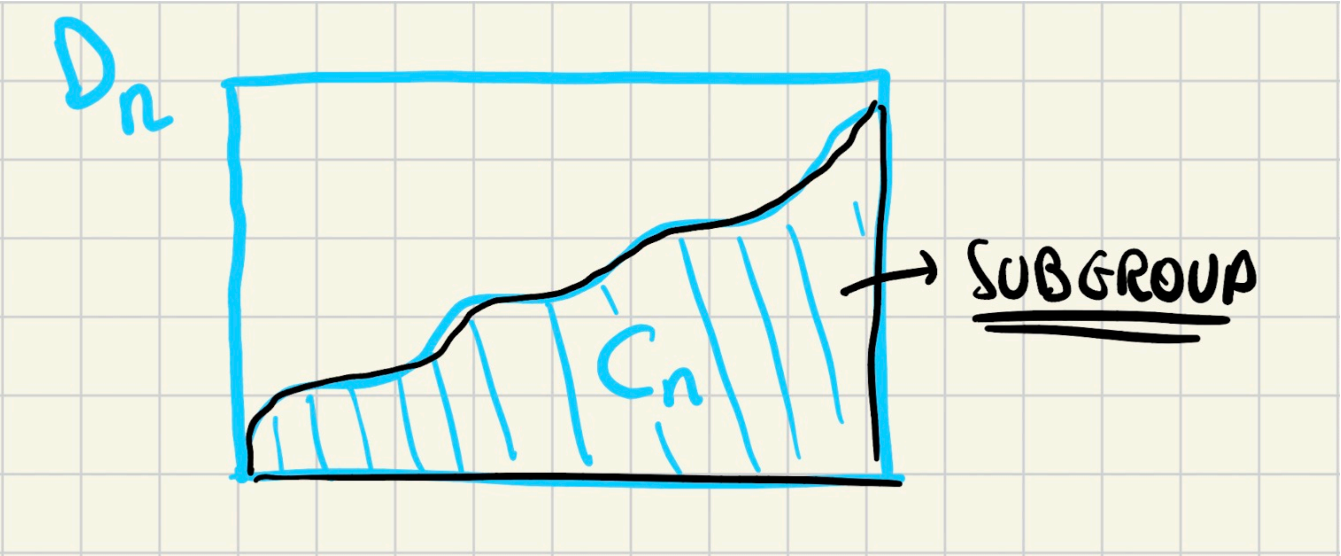
$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

We can derive the multiplication table from the following:

- -1 commutes with any other element: $\quad \forall a \in \ : (-1) \cdot a = a \cdot (-1) = -a$
- $(-1)^2 = 1$
- $i^2 = j^2 = k^2 = ijk = -1$

Example: $ij = k$ because $ij = ij(-1)(-1) = ijkk(-1) = (-1)k(-1) = (-1)^2(k) = k$.

C_n is a subgroup of D_n:


D_n
C_n
SUBGROUP