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
- $(\mathbb{Q} \setminus \{0\}, \cdot)$
- $(\mathbb{Z}_n, +_n)$
  - See

Non-examples of groups

- $(\mathbb{Z}, \cdot)$ (not every element has an inverse)
- $(\mathbb{N}, +)$ (not every element has an inverse)

📖 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.

$$\text{ord}(G) = n$$

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

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

$(\mathbb{Z}_n, \cdot_n)$ 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**.
   - $(\mathbb{Z}, \times)$, 2 has no inverse since there is no $x \in \mathbb{Z}$ such that

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

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)

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

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 $\mathbb{Z}_{*n}$:

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

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:

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

So $(n) = \text{ord}(\mathbb{Z}_{*n}, \cdot_n)$.

$\mathbb{Z}_{*n}$ 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

Definition 3.1.10: Order of an element (p73)

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

- If it exists, smallest positive number i such that $g^i = e$ is called the **order of the element** g and is denoted by $\text{ord}(g)$
- If $\forall i \in \mathbb{N} : g^i \neq e$, we say that g is of **infinite order** and write

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

Lemma: Order of an element

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

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

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

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

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

Lemma 3.1.12: Order of an element divides ... (p73)

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

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

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

$$g^i = e$$

3.2 Cycling groups

Counterclockwise rotations of a regular n-gon (p74)

Denote by r the counterclockwise rotation by $2n$ radians (or $30n$ degrees) around the center of a regular n-gon with vertices $_0, 1, \ldots, _{n-1}$.
Using the composition operator $\circ$, we can define $r^0 = e, r^1 = r, r^2 = r \circ r, \ldots, r^{n-1}$.
We can make a group out of the rotations using $\circ$ as the group operation. Let's define

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

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

The group $(C_n, \circ)$ is an example of a cyclic group:

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 $g \in G$:

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

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

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

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

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 $n = \mathrm{ord}(g)$. Then

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

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