4. Subgroups and cosets

4.1 Subgroups

Definition 4.1.1: A subgroup H (p91)

Let $H \subseteq G$ be a subset of G. Then H is called a **subgroup** of $(G, \cdot)$ if the following properties are satisfied:

1. $\boxed{e \in H}$
2. $\forall f \in G : f \in H \implies \boxed{f^{-1} \in H}$.
3. $\forall f, g \in G : f, g \in H \implies \boxed{f \cdot g \in H}$.

A subgroup $H \subseteq G$ inherits the group operation $\cdot$ from the larger group $(G, \cdot)$

- So the group operation in H is the **restriction** of the group operation of G
- The third property in the definition makes sure that this operation sends two elements of H to another element of H

Lemma 4.1.2: When is a subset a subgroup? (p91)

Let $(G, \cdot)$ be a group and let $H \subseteq G$ be a **non-empty** subset. Then

$$H \text{ is a subgroup of } (G, \cdot) \iff \forall f, g \in H : \boxed{f \cdot g^{-1} \in H}$$

Proof

We proved this in **Exercise 4.17** Note that H being **non-empty** is important, otherwise the identity element e might not be in H.

Example 1

The set of **even integers**,

$$\boxed{2\mathbb{Z}} = \{\dots, -4, -2, 0 = e, 2, 4, \dots\},$$

is a subgroup of the group of integers $(\mathbb{Z}, +)$ according to the above Lemma 4.1.2:

- Choose $k, \ell \in 2\mathbb{Z}$.
- Since k and ℓ are even numbers, $k - \ell$ is an even number as well.
- This implies

$$k - \ell \in 2\mathbb{Z} \quad \overset{\Delta}{\Leftrightarrow} \quad k \cdot \ell^{-1} \in 2\mathbb{Z} \quad \overset{\text{Lemma 4.1.2}}{\iff} \quad 2\mathbb{Z} \text{ is a subgroup of } (\mathbb{Z}, +)$$

Example 2

The cyclic group $C_n = \{e, g, g^2, \dots, g^{n-1}\}$ is a subgroup of the dihedral group $(D_n, \circ)$.
We can show this by using Definition 4.1.1:

1. The identity element e of D_n is also in C_n.
2. If $r^i \in C_n$, then $(r^i)^{-1} = r^{(-i) \bmod n} \in C_n$. (Lemma 3.2.1)
3. If $r^i, r^j \in C_n$, then $r^i \circ r^j = r^{(i+j) \bmod n} \in C_n$. (Lemma 3.2.1)

Definition 4.1.7: The subgroup generated by an element (p92)

Let $(G, \cdot)$ be a group and let $g \in G$ be a group element. The set

$$\boxed{\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}}$$

is a subgroup of G, and is said to be the **subgroup generated by** g.

Note that $\langle g \rangle$ is indeed a subgroup, by Definition 4.1.1:

1. $e = g^0 \in \langle g \rangle$
2. If $f = g^i \in \langle g \rangle$, then $f^{-1} = (g^i)^{-1} = g^{-i} \in \langle g \rangle$
3. If $g^i, g^j \in \langle g \rangle$, then $g^i \cdot g^j = g^{i+j} \in \langle g \rangle$

A subgroup of a cyclic group is cyclic

Any subgroup of a cyclic group is itself cyclic. In particular, the subgroup $\langle g \rangle$ generated by an element g of a group $(G, \cdot)$ is a cyclic subgroup.

Proof

Suupose G is cyclic generated by a: $G = \langle a \rangle$. Let H be a subgroup of G. If $H = \{a\}$, then obviously H is cyclic. Thus, let H be a **proper** subgroup of G.

The elements of H will be some powers of a, since it is a subgroup of $G = \{a^i \mid i \in \mathbb{Z}\}$. Let Furthermore, being a subgroup implies that if $a^s \in H$, $(a^s)^{-1} = a^{-s} \in H$ as well. So if $a^s \in H$, then also $a^{-s} \in H$. Therefore, H contains both elements that are positive, as well as negative powers of a.

Now let m be the **smallest positive integer** such that $a^m \in H$. This m exists, since H contains both negative and positive powers of a, there cannot be only negative powers, and we have at least one positive power (proper subgroup), so we can choose the smallest power m. We will show that $H = \langle a^m \rangle$. Clearly $\langle a^m \rangle \subseteq H$, since $a^m \in H$ and H is a group. We now show the other inclusion.

Let a^t be an arbitrary element of H. If we prove that a^t is a power of a^m then we are done.
By **division with remainder**, we can write

$$t = mq + r \qquad \text{with } 0 \leq r < m$$

$$\begin{aligned} a^m \in H &\implies (a^m)^q = a^{mq} \in H \\ &\implies (a^{mq})^{-1} \in H \\ &\implies a^{(-mq)} \in H \\ &\implies a^t \cdot a^{(-mq)} = a^r \in H \end{aligned}$$

Because m was the smallest positive integer such that $a^m \in H$, and $0 \leq r < m$, it must be that $r = 0$. Therefore, $t = mq$, and thus $a^t = a^{mq} = (a^m)^q$ is a power of a^m. This shows that $H \subseteq \langle a^m \rangle$, and thus $H = \langle a^m \rangle$ is cyclic.

Lemma 4.1.8: Order of the subgroup $\langle g \rangle$ (p92)

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

$$\boxed{|\langle g \rangle| = \mathrm{ord}(g)}$$

So the order of the subgroup $\langle g \rangle$ is the same as the order of the element g.

Theorem

Let $\langle g \rangle$ be the subgroup generated by an element g of a group $(G, \cdot)$ and let $\operatorname{ord}(g) = n < \infty$. Then:

$$\forall i \in \mathbb{Z} : \boxed{\forall g \in \langle g \rangle : g^i = g^{i \bmod n}} \quad \Rightarrow g^n = e$$

Using division with remainder, we can write any integer i:

$$i \quad = \quad n \cdot (i \operatorname{quot} n) + (i \bmod n) \quad = \quad n \cdot q + (i \bmod n)$$

Then it holds that

$$\begin{aligned} g^i &= g^{q \cdot n + (i \bmod n)} \\ &= g^{q \cdot n} \cdot g^{(i \bmod n)} \\ &= (g^n)^q \cdot g^{(i \bmod n)} \\ &= e^q \cdot g^{(i \bmod n)} \\ &= g^{(i \bmod n)} \end{aligned}$$

Note that for the group $(\mathbb{Z}, +)$, we have

$$\boxed{n\mathbb{Z} = \langle n \rangle} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$$

and that this is a **subgroup** of $(\mathbb{Z}, +)$.

In week 1, we saw that the congruence class of $a \in \mathbb{Z}$ modulo n is defined as

$$a + n\mathbb{Z} = \{a + k \cdot n \mid k \in \mathbb{Z}\}$$

This is exactly the same as the **coset** $a + \langle n \rangle$ of the subgroup $\langle n \rangle = n\mathbb{Z}$ of the group $(\mathbb{Z}, +)$.

4.2 Cosets of a group

Definition 4.2.1: Multiplication of subsets (p93)

Let $(G, \cdot)$ be a group and let $M \subseteq G$ and $N \subseteq G$ be two subsets of G. Then we define

$$M \cdot N = \{f \cdot g \mid f \in M, g \in N\}$$

This operation is **associative** because the group operation $\cdot$ in G is associative:

$$\begin{aligned} (M \cdot N) \cdot &= \{k \cdot p \mid k \in M \cdot N, p \in \} \\ &= \{(f \cdot g) \cdot p \mid f \in M, g \in N, p \in \} \\ &= \{f \cdot (g \cdot p) \mid f \in M, g \in N, p \in \} \\ &= M \cdot (N \cdot) \end{aligned}$$

Note that for $(\mathbb{Z}, +)$, this definition corresponds to the usual addition of sets:

$$M + N = \{m + n \mid m \in M, n \in N\}$$

Definition 4.2.3: Left and right cosets (p93)

Let H be a subgroup of a group $(G, \cdot)$ and let $f \in G$ be a group element. Then we define the **left coset of H in G by f** as

$$\boxed{f \cdot H := \{f\} \cdot H = \{f \cdot h \mid h \in H\} \qquad \in G/H}$$

Similarly, we define the **right coset of H in G by f** as

$$H \cdot f := H \cdot \{f\} = \{h \cdot f \mid h \in H\}$$

Subgroups are cosets

A subgroup H of a group $(G, \cdot)$ is itself **both a left and a right coset** of H in G by the identity element $e \in G$:

$$\boxed{H = e \cdot H = H \cdot e}$$

Homework 2: Normal subgroup

SEE DEF. 6.1.10

A subgroup H of a group G is called a **normal subgroup** if the left and right cosets of H in G are the same for every group element $g \in G$, i.e.,

$$\boxed{\forall g \in G : gH = Hg}$$

Or in other words, if all left cosets of H in G are equal to the corresponding right cosets.

In an Abelian group, there is **no difference between left and right cosets** since $f \cdot h = h \cdot f$ for any $f, h \in G$.

Deduction

In an **Abelian** group, **every subgroup is a normal subgroup**.

Notation: The set of all cosets of a subgroup in a group (p94)

The set of **all *left* cosets of H in G** is denoted by

$$G/H = \{f \cdot H \mid f \in G\}$$

Similarly, the set of **all *right* cosets of H in G** is denoted by

$$H \backslash G = \{H \cdot f \mid f \in G\}$$

Exercise 4.19: Intersection is a subgroup

The **intersection** of two subgroups is also **a subgroup**.

Exercise 5.25: Intersection of normal subgroups

The **intersection** of two normal subgroups is also **a normal subgroup**.

4.3 Cosets as equivalence classes

Definition 4.3.1: The relation $\sim_H$ (p95)

Let $(G, \cdot)$ be a group and $H \subseteq G$ a subgroup. For $f, g \in G$, we write

- $\boxed{f \sim_H g \quad \iff \quad f^{-1} \cdot g \in H \quad \iff g \in f \cdot H}$
- $f\ {}_H\!\sim g \quad \iff \quad g \cdot f^{-1} \in H$

Lemma 4.3.2: $\sim_H$ and $_H\sim$ are equivalence relations (p95)

Let $(G,\cdot)$ be a group and $H \subseteq G$ a subgroup. Then the relations $\sim_H$ and $_H\sim$ are **equivalence relations** on G.

Lemma 4.3.3 (p95)

Let $(G,\cdot)$ be a group and $H \subseteq G$ a subgroup. For $f \in G$ we have

$$\boxed{[f]_{\sim_H} = f \cdot H} \quad \text{and} \quad [f]_{_H\sim} = H \cdot f$$

Now that we have identified left and right cosets **of** H **in** G as equivalence classes under $\sim_H$ and $_H\sim$, we can apply Theorem 1.3.3 (Properties of equivalence classes) to these equivalence relations:

Theorem 4.3.4: Properties of cosets (p96)

Let $(G,\cdot)$ be a group and $H \subseteq G$ a subgroup. Then the following holds:

1. $\forall f \in G$, $\boxed{f \in f \cdot H}$ and $f \in H \cdot f$ (reflexivity).
2. We have $G = \bigcup_{f\in G}(f \cdot H) = \bigcup_{f\in G}(H \cdot f)$ (G is covered by all equivalence classes).
3. $\forall f, g \in G$,
   - **either**
     - $\boxed{f \cdot H = g \cdot H}$
     - $\boxed{(f \cdot H) \cap (g \cdot H) = \emptyset}$
   - Similarly, **either**
     - $H \cdot f = H \cdot g$
     - $(H \cdot f) \cap (H \cdot g) = \emptyset$.
4. $\forall f, g \in G:$
   - $\boxed{f \cdot H = g \cdot H \iff f \sim_H g \iff f^{-1} \cdot g \in H \iff g \in f \cdot H}$
   - $H \cdot f = H \cdot g \iff f\ {_H\sim}\ g \iff g \cdot f^{-1} \in H$.

Since $e \cdot H = \{e \cdot h \mid h \in H\} = H$, we see from part 4 of Theorem 4.3.4 that

$$H = f \cdot H \iff e \cdot H = f \cdot H \iff e \sim_H f \iff e^{-1} \cdot f \in H \iff f \in H$$

and similarly

$$H = H \cdot f \iff H \cdot e = H \cdot f \iff H\ {_H\sim}\ f \iff f \cdot e^{-1} \in H \iff f \in H$$

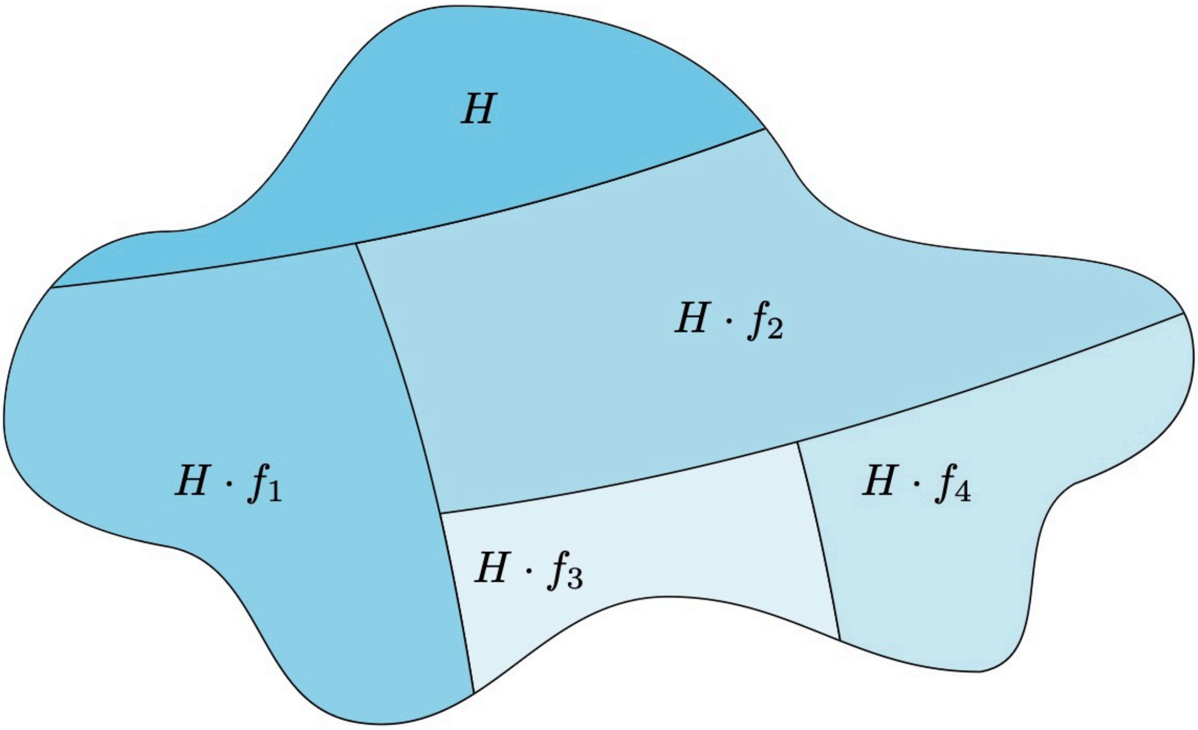
When is a coset equal to the subgroup? (p96)

Let $(G,\cdot)$ be a group and $H \subseteq G$ a subgroup. Then for any $f \in G$, we have

$$\boxed{f \cdot H = H \iff f \in H} \quad \text{and} \quad H \cdot f = H \iff f \in H$$

We call an element from a coset a **representative** of that coset.

Below, it is illustrated that **cosets $H \cdot f$ form a partition of the group G**:



$H \cdot H = H$

For a **subgroup** H of a group $(G, \cdot)$, we have

$$\boxed{H \cdot H = H}$$

Proof

$$\begin{aligned} H \cdot H &= \{h_1 \cdot h_2 \mid h_1, h_2 \in H\} \\ &\subseteq H & \text{by Definition 4.1.1 (3)} \end{aligned}$$

Furthermore, for any $h \in H$, we have $h = h \cdot e \in H \cdot H$. This shows that $H \subseteq H \cdot H$. Combining both inclusions, we get $H \cdot H = H$.

4.4 The order of a subgroup and of an element

LAGRANGE's THEOREM

Theorem 4.4.1: Lagrange's Theorem (p98)

Let $(G, \cdot)$ be a **finite** group and $H \subseteq G$ a subgroup. Then

$$\boxed{|H| \text{ divides } |G|}$$

So **the order of a subgroup divides the order of the group**. More precisely,

$$\boxed{|G| = [G : H] \cdot |H|}$$

This theorem is called *Lagrange's Theorem*

Definition 4.4.2: index of a subgroup in a group (p98)

Let $(G, \cdot)$ be a group and $H \subseteq G$ a subgroup. The number of left (or right) cosets of H in G is denoted by

$$\boxed{[G:H] = |G/H| \overset{\text{Lagrange}}{=} \frac{|G|}{|H|}}$$

and is called the **index of H in G**

The index is at least 1

Let $(G, \cdot)$ be a *finite* group and $H \subseteq G$ a subgroup. Then

$$\boxed{[G:H] \geq 1}$$

Why?

As we already saw, a subgroup H is itself a left coset of H in G by the identity element $e \in G$:

$$H = e \cdot H$$

This shows that there is at least one left coset of H in G, so $|G/H| \geq 1$. By Theorem 4.4.1, we have

$$[G:H] = |G/H| = \frac{|G|}{|H|} \geq 1.$$

Proposition 4.4.4: order of a group element (p98)

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

1. $\boxed{\mathrm{ord}(g) \text{ divides } |G|}$
2. $\forall g \in G : \boxed{g^{|G|} = e}$

Why?

1. This follows from Lemma 4.1.8, which says that

   $$\mathrm{ord}(g) = |\langle g \rangle|$$

   and Theorem 4.4.1, which says that

   $$|\langle g \rangle| \text{ divides } |G|$$

   since $\langle g \rangle$ is a (cyclic) subgroup of G.
2. Because of part 1, we can write

   $$|G| = k \cdot \mathrm{ord}(g)$$

   for some integer k. This gives us

   $$g^{|G|} = g^{k \cdot \mathrm{ord}(g)} = (g^{\mathrm{ord}(g)})^k = e^k = e.$$

Proposition 4.4.4 has a number of interesting consequences for specific groups.

We start with **Euler's theorem**:

▷▷ Corollary 4.4.6: Euler's theorem (p99)

Let $d, n \in \mathbb{Z}$ be two integers and assume that $\gcd(d, n) = 1$. Then

$$d^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ is Euler's totient function defined by $\phi(n) = |(\mathbb{Z}_n)^*|$.

In case n is a prime number p, we have

$$\phi(p) = |\{i \in \{1, \ldots, p-1\} \mid \gcd(i, p) = 1\}| = p - 1$$

This gives us the following special case of Euler's theorem, known as **Fermat's little theorem**:

▷▷ Corollary 4.4.7: Fermat's little theorem (p99)

Let p be a prime number and let $d \in \mathbb{N}$ such that p d. Then

$$d^{p-1} \equiv 1 \pmod{p}$$