Subgroups

Definition: A group $(H, \bullet)$ is a *subgroup* of a group $(G, \circ)$ if $H \subseteq G$ and $\forall a, b \in H : a \bullet b = a \circ b$. We write $(H, \bullet) \leq (G, \circ)$.

The same operational symbol is often used in both groups.

Examples:

$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$

(even integers$, +) \leq (\mathbb{Z}, +)$

$(\{-1, 1\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$

$(\{id, (1, 3, 2)\}, \circ) \leq S_3$

$A_n =$ (even permutations of $S_n, \circ) \leq S_n$ ... the *alternating* group

(permutation matrices$, \cdot) \leq$ (regular matrices$, \cdot)$ ... both from $\mathbb{R}^{n \times n}$

Observation: If $(H, \circ)$ is a subgroup of $(G, \circ)$ then

$e_H = e_G \in H$ and $\forall a \in H : a_G^{-1} = a_H^{-1} \in H$.

Cosets

Definition: Let $(H, \cdot)$ be a subgroup of $(G, \cdot)$. For any $a \in G$
$aH = \{ah : h \in H\}$ is the *left coset* of H in G given by a, and
$Ha = \{ha : h \in H\}$ is the *right coset* of H in G given by a.

Example: Let $(G, \cdot) = (\mathbb{Z}, +)$,
the subgroup $H = \{\text{even integers}\}$ has two cosets.
One coset is H itself (for $a = e = 0$), i.e. the set of even numbers;
the other coset is formed by odd numbers (e.g. for $a = 7$)
... and this coset *is not a subgroup!*

Observation: If the operation is commutative then the left and right cosets given by any $a \in G$ coincide: $aH = Ha$, like in our example.

The cosets given by e always coincide $eH = He = H$,
indeed in non-Abelian groups.

Cosets

Lemma: Let $(H, \cdot)$ be a subgroup of $(G, \cdot)$ then
$\forall a, b \in G$: either $aH = bH$ or $aH \cap bH = \emptyset$.

Proof:
If $aH \cap bH \neq \emptyset$ consider $h_1, h_2 \in H$ s.t. $ah_1 = bh_2 \in aH \cap bH$.
As $a = bh_2 h_1^{-1}$, for any $h \in H$: $ah = bh_2 h_1^{-1} h \in bH$, thus $aH \subseteq bH$.
As $b = ah_1 h_2^{-1}$, for any $h \in H$: $bh = ah_1 h_2^{-1} h \in aH$, thus $bH \subseteq aH$.

Consequences: $H = eH = aH$ for all $a \in H$.
Also $a \notin H$ iff $aH \cap H = \emptyset$ Pf: If $ah_1 = h_2$ iff $a = h_2 h_1^{-1} \in H$.

Lagrange's Theorem: [Camille Jordan, 1861]
If H is a subgroup of a finite group G then $|H|$ divides $|G|$.

Normal subgroup

Problem:
When the group operation transfers onto the cosets like the addition on the sets of even and odd integers?

Formally: For which subgroups H it holds that:
$x \in aH \wedge y \in bH \Longrightarrow xy \in (ab)H$ for all $a, b, x, y \in G$?

Definition: A subgroup H of G is *normal* if $\forall a \in G : aH = Ha$.

Examples: Every subgroup of an Abelian group is normal.

The alternating group A_n is a normal subgroup of S_n:

- If p is even then $pA_n = A_n p = A_n$ ... the positive signs
- If p is odd then $pA_n = A_n p = S_n \setminus A_n$ ... the negative signs

In particular, for $A_3 = (\{id, r_+, r_-\}, \circ)$, the left and right cosets are equal, hence A_3 is normal:

$idA_3 = A_3 id = r_+ A_3 = A_3 r_+ = r_- A_3 = A_3 r_- = \{id, r_+, r_-\} = A_3$
$p_1 A_3 = A_3 p_1 = p_2 A_3 = A_3 p_2 = p_3 A_3 = A_3 p_3 = \{p_1, p_2, p_3\}$

Normal subgroup

Theorem: The group operation transfers onto the cosets of H in G *if and only if* the subgroup H is normal.

Proof: $\Leftarrow$: $x \in aH, y \in bH = Hb \Leftrightarrow \exists h_1, h_2 \in H : x = ah_1, y = h_2 b$
$\Rightarrow xy = ah_1 h_2 b = ah_3 b = abh_4 \in (ab)H$ for suitable $h_3, h_4 \in H$.

$\Rightarrow$: by a contradiction assume that there is $a : aH \neq Ha$
$\Leftrightarrow$ for some $a \in G, h \in H$ we have $aha^{-1} \notin H \Leftrightarrow (aha^{-1})H \cap H = \emptyset$.
Now $\forall x \in aH,\ y \in hH = H, z \in a^{-1}H$ we get that:

- $xyz \in (aha^{-1})H$ ... as the operation transfers $\Rightarrow xyz \notin H$
- $xyz = ah_1 h_2 a^{-1} h_3 = ah_4 a^{-1} h_3 \in (aa^{-1})H = H$
  for suitable $h_1, h_2 = y, h_3, h_4 = h_1 h_2 \in H$, a contradiction.

Factorization by a normal subgroup

Definition: Let $(H, \cdot)$ be a normal subgroup of $(G, \cdot)$ then $(\{aH \colon a \in G\}, \cdot)$, where $aH \cdot bH = (a \cdot b)H$ is the *quotient group* (aka the *factor group*) of G by H.

Example: The quotient group of S_n by A_n has two elements, namely A_n and $S_n \setminus A_n$.

The operation $\circ$ transfers as follows:

$\circ$	A_n	$S_n \setminus A_n$
A_n	A_n	$S_n \setminus A_n$
$S_n \setminus A_n$	$S_n \setminus A_n$	A_n

This quotient group is isomorphic to $(\{1, -1\}, \cdot)$:

$\cdot$	1	-1
1	1	-1
-1	-1	1

Residue classes modulo 6 as a quotient group of $(\mathbb{Z}, +)$

Denote $6\mathbb{Z} = \{6k, k \in \mathbb{Z}\} = \{\dots, -6, 0, 6, 12, \dots\}$

$(6\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$, since $6|a$ & $6|b \Longrightarrow 6|(a+b)$.
In addition, $6\mathbb{Z}$ is a *normal* subgroup, because $+$ is commutative.

Denote the left factor classes of $6\mathbb{Z}$ in $\mathbb{Z}$ as follows:
$T_0 = \{\dots, -6, 0, 6, 12, \dots\}$, $T_1 = \{\dots, -5, 1, 7, 13, \dots\}$,
$T_2 = \{\dots, -4, 2, 8, 14, \dots\}$, $T_3 = \{\dots, -3, 3, 8, 15, \dots\}$,
$T_4 = \{\dots, -2, 4, 10, 16, \dots\}$, $T_5 = \{\dots, -1, 5, 11, 17, \dots\}$.

These six sets with the binary operation $+$, defined as follows, form a *quotient group* of $(\mathbb{Z}, +)$ by the subgroup $(6\mathbb{Z}, +)$.

$+$	T_0	T_1	T_2	T_3	T_4	T_5
T_0	T_0	T_1	T_2	T_3	T_4	T_5
T_1	T_1	T_2	T_3	T_4	T_5	T_0
T_2	T_2	T_3	T_4	T_5	T_0	T_1
T_3	T_3	T_4	T_5	T_0	T_1	T_2
T_4	T_4	T_5	T_0	T_1	T_2	T_3
T_5	T_5	T_0	T_1	T_2	T_3	T_4

The addition transfers, since
$a \in T_i, b \in T_j \Longrightarrow$
$\Longrightarrow a + b \in T_i + T_j$.

Example of a subgroup that is not normal

Let $H = \{id, p_1\}$.

$(H, \circ)$ is a subgroup of S_3, because

$$id \circ id = p_1 \circ p_1 = id \quad \text{and} \quad p_1 \circ id = id \circ p_1 = p_1 .$$

Left cosets are:
$idH = p_1 H = \{id, p_1\}$
$p_2 H = r_- H = \{p_2, r_-\}$
$p_3 H = r_+ H = \{p_3, r_+\}$

On these three clases the operation $\circ$ does not transfer:
$r_- \in p_2 H$, but $r_- \circ r_- = r_+ \notin (p_2 \circ p_2)H = H$

The subgroup H is not normal, also because cosets do not coincide:
$p_2 H = \{p_2, r_-\} \neq \{p_2, r_+\} = Hp_2$.