

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: Additive groups: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$,
(even integers, $+$) \leq $(\mathbb{Z}, +)$.

Multiplicative groups:

$$(\mathbb{Q}^+, \cdot) \leq (\mathbb{R}^+, \cdot)$$

$$\begin{array}{c} \wedge \\ (\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot) \leq (\mathbb{C} \setminus \{0\}, \cdot) \\ \vee \qquad \qquad \qquad \vee \end{array}$$

$$(\{-1, 1\}, \cdot) \leq (\{z \in \mathbb{C} : |z| = 1\}, \cdot)$$

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

Groups of permutations: $(\{id, p_1\}, \circ) \leq S_3$,

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

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

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

Cosets

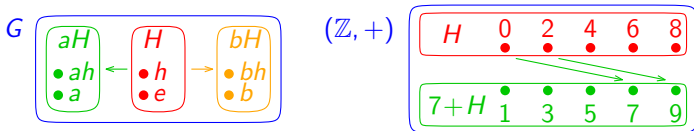
Notation: For simplicity we will mostly omit the group operation symbol \circ in this lesson, i.e. gh means $g \circ h$.

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

Example:

In $G = (\mathbb{Z}, +)$ the subgroup $H = \{\text{even integers}\}$ yields 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 $a = 7$)

This coset $7 + H$ *is not a subgroup!*



Cosets

Notation: For simplicity we will mostly omit the group operation symbol \circ in this lesson, i.e. gh means $g \circ h$.

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

Example:

In $G = (\mathbb{Z}, +)$ the subgroup $H = \{\text{even integers}\}$ yields 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 $a = 7$)

This coset $7 + H$ *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.

The partition into cosets need not to coincide

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

H is a subgroup of S_3 , as

$\text{id id} = p_1 p_1 = \text{id}$ and

$p_1 \text{id} = \text{id } p_1 = p_1$.

Left cosets are:

$\text{id } H = p_1 H = \{\text{id}, p_1\}$

$p_2 H = r_- H = \{p_2, r_-\}$

$p_3 H = r_+ H = \{p_3, r_+\}$

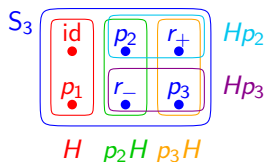
Right cosets are:

$H \text{id} = H p_1 = \{\text{id}, p_1\}$

$H p_2 = H r_+ = \{p_2, r_+\}$

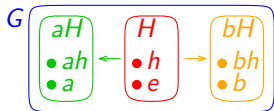
$H p_3 = H r_- = \{p_3, r_-\}$

	id	p_1	p_2	p_3	r_+	r_-
id	id	p_1	p_2	p_3	r_+	r_-
p_1	p_1	id	r_+	r_-	p_2	p_3
p_2	p_2	r_-	id	r_+	p_3	p_1
p_3	p_3	r_+	r_-	id	p_1	p_2
r_+	r_+	p_3	p_1	p_2	r_-	id
r_-	r_-	p_2	p_3	p_1	id	r_+



Coset properties

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

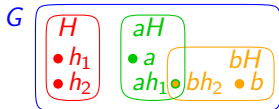


Proof:

If $aH \cap bH \neq \emptyset$ consider $h_1, h_2 \in H$ s.t. $ah_1 = bh_2 \in aH \cap bH$.

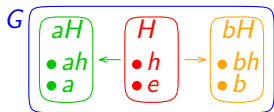
As $a = bh_2h_1^{-1}$, for any $h \in H$: $ah = bh_2h_1^{-1}h \in bH$, thus $aH \subseteq bH$.

As $b = ah_1h_2^{-1}$, for any $h \in H$: $bh = ah_1h_2^{-1}h \in aH$, thus $bH \subseteq aH$.



Coset properties

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



Consequences: $H = eH = aH$ for all $a \in H$.

Also $a \notin H$ iff $aH \cap H = \emptyset$ Pf: $ah_1 = h_2$ iff $a = h_2h_1^{-1} \in H$.

Lagrange's Theorem: [Camille Jordan, 1861]

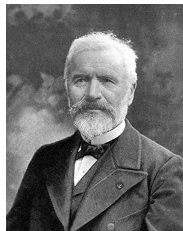
If H is a subgroup of a finite group G then $|H|$ divides $|G|$.

Proof: The map $h \rightarrow ah$ is a bijection $H \rightarrow aH$, thus $|H| = |aH|$.



Giuseppe Lodovico Lagrangia

1736 – 1813



Marie Ennemond Camille Jordan

1838 – 1922

Picts: Wikipedia

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:

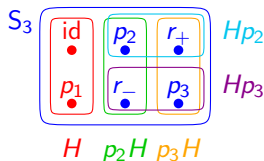
$x \in aH \wedge y \in bH \implies xy \in (ab)H$ for all $a, b, x, y \in G$?

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 subgroup $H = (\{id, p_1\}, \circ) \leq S_3$ is not normal.

Left and right cosets do not coincide.



The operation does not transfer on cosets H , p_2H and p_3H :
 $r_- \in p_2H$, but $r_- r_- = r_+ \notin (p_2 p_2)H = H$

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:

$$x \in aH \wedge y \in bH \implies xy \in (ab)H \text{ for all } a, b, x, y \in G?$$

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 subgroup $H = (\{\text{id}, p_1\}, \circ) \leq S_3$ is not normal.

The alternating group A_n is a normal subgroup of S_n :

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

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

$$\begin{aligned} \text{id}A_3 &= A_3\text{id} = r_+A_3 = A_3r_+ = r_-A_3 = A_3r_- = \{\text{id}, r_+, r_-\} = A_3 \\ p_1A_3 &= A_3p_1 = p_2A_3 = A_3p_2 = p_3A_3 = A_3p_3 = \{p_1, p_2, p_3\} \end{aligned}$$

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 : If the cosets $bH = Hb$ coincide and $x \in aH, y \in bH$ then $\exists h_1, h_2 \in H : x = ah_1, y = h_2b$. From this we get $xy = ah_1h_2b = ah_3b = abh_4 \in (ab)H$ for suitable $h_3, h_4 \in H$.

\Rightarrow : For a contradiction assume that there is an $a : aH \neq Ha$.

- ▶ If $aH \not\subseteq Ha$, then there exists $h \in H$ such that $ah \notin Ha$. Then $aha^{-1} \notin H$ since $aha^{-1} = h' \in H \Rightarrow ah = h'a \in Ha$.

The group operation transfers to the left cosets, so $aha^{-1} = aha^{-1}e \in (aa^{-1})H = eH = H$, a **contradiction**.

- ▶ The case $Ha \not\subseteq aH$ goes similarly by switching the operands. If $Ha \not\subseteq aH$, then there exists $h \in H$ such that $ha \notin aH$. Then $a^{-1}ha \notin H$, since $a^{-1}ha = h' \in H \Rightarrow ha = ah' \in aH$. As the group operation transfers to the left cosets, $a^{-1}ha = a^{-1}hae \in (a^{-1}a)H = eH = H$, a contradiction.

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 : If the cosets $bH = Hb$ coincide and $x \in aH, y \in bH$ then $\exists h_1, h_2 \in H : x = ah_1, y = h_2b$. From this we get $xy = ah_1h_2b = ah_3b = abh_4 \in (ab)H$ for suitable $h_3, h_4 \in H$.

\Rightarrow : For a contradiction assume that there is an $a : aH \neq Ha$.

- ▶ If $aH \not\subseteq Ha$, then there exists $h \in H$ such that $ah \notin Ha$. Then $aha^{-1} \notin H$ since $aha^{-1} = h' \in H \Rightarrow ah = h'a \in Ha$.

The group operation transfers to the left cosets, so $aha^{-1} = aha^{-1}e \in (aa^{-1})H = eH = H$, a **contradiction**.

- ▶ The case $Ha \not\subseteq aH$ goes similarly by switching the operands.
- ▶ We proved that the operation does not transfer to left cosets. By a similar switch of the operand order, it could be shown that the operation does not transfer to right cosets either.

Factorization by a normal subgroup

Definition: Let (H, \circ) be a normal subgroup of (G, \circ) then $(\{aH : a \in G\}, \bullet)$, where $aH \bullet bH = (a \circ b)H$ 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 (cosets), namely A_n and its complement $S_n \setminus A_n$.

The operation \circ transfers from S_n to the quotient group S_n/A_n :

\bullet	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 $(\{1, -1\}, \cdot)$ (i.e. operations behave the same in both groups, only operations and elements have different names) as signs represent cosets and \bullet corresponds to \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 $(6|a \wedge 6|b) \implies 6|(a+b)$.
In addition, $6\mathbb{Z}$ is a *normal* subgroup, because $+$ is commutative.

The left cosets of $6\mathbb{Z}$ in \mathbb{Z} are $T_i = \{x \in \mathbb{Z} : x \equiv i \pmod{6}\}$, i.e.:
 $T_0 = \{\dots, -6, 0, 6, 12, \dots\}$, $T_1 = \{\dots, -5, 1, 7, 13, \dots\}$,
 $T_2 = \{\dots, -4, 2, 8, 14, \dots\}$, $T_3 = \{\dots, -3, 3, 9, 15, \dots\}$,
 $T_4 = \{\dots, -2, 4, 10, 16, \dots\}$, $T_5 = \{\dots, -1, 5, 11, 17, \dots\}$.

These six sets with the binary operation $+$ form the quotient group $(6\mathbb{Z}, +)$.

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

$+$	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

Questions to understand the lecture topic

- ▶ Why does every element belong to some coset?
- ▶ Why do all axioms from the definition of a group hold in a quotient group?
- ▶ Let H be a regular hexagon with vertices A, \dots, F .
Let G be the group of geometric transformations of the plane (rotations, axial and central symmetries) that preserve H .
 1. How many elements does G have?
 2. How many elements does the subgroup fixing vertex A have?
 3. How many left and right cosets does the subgroup fixing A have?
 4. Is it a normal subgroup?
 5. Do rotations by angles $0, 60, 120, 180, 240$ and 300 degrees clockwise form a normal subgroup of the group G ?