# Section 14 - Factor groups

Let $G$ be a group, $H \leq G$ a subgroup. Let $G/H$ be the set of left cosets of $H$

$$G/H = \{ aH \mid a \in G \}.$$

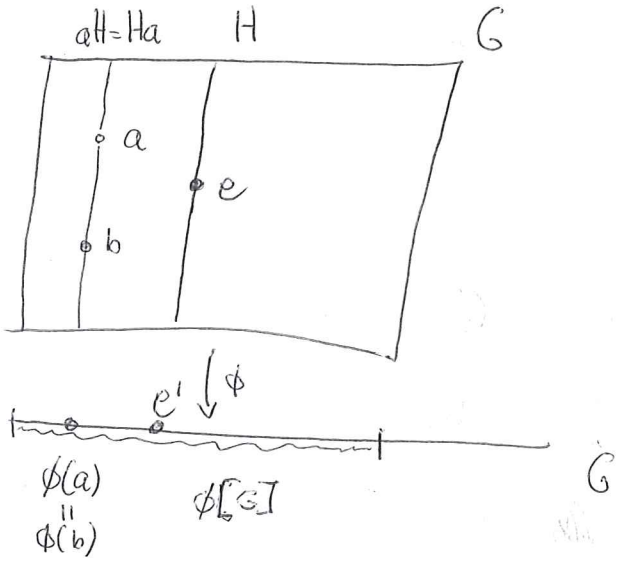
Today: Define a binary operation, on $G/H$ making it a group, for "good" $H$.

Let $\phi : G \longrightarrow G'$ be a group homomorphism,

$$H = \ker \phi = \{ x \in G \mid \phi(x) = e' \}.$$

Recall that for every $a \in G$

$$aH = Ha = \phi^{-1}[\phi(a)] = \{ x \in G \mid \phi(x) = \phi(a) \}.$$




Get a bijection

$$\mu : G/H \longrightarrow \phi[G] = \{ \phi(x) \mid x \in G \}$$

by $\mu(aH) = \phi(a)$. Know $\phi[G]$ is a group, so can induce a binary operation on $G/H$ making $\mu$ an isomorphism of groups.

Given $aH, bH \in G/H$, what is $aH\,bH$?

$\mu$ a homomorphism $\Rightarrow \mu(aH\,bH) = \mu(aH)\,\mu(bH) = \phi(a)\,\phi(b) = \phi(ab)$,

so have

$$aHbH = \{ x \in G \mid \phi(x) = \phi(ab) \} = (ab)H.$$

**Thm** There is a binary operation on $G/H$ given by

$$aH\,bH = (ab)H, \qquad \forall a, b \in G$$

making $G/H$ a group & $\mu : G/H \to \phi[G]$ an isomorphism.

**Example** $\phi : \mathbb{Z} \to \mathbb{Z}_3$, reduction modulo 3.

$\phi(n)$ = remainder of $n$ divided by 3.

$H = \ker \phi = 3\mathbb{Z}$, elements of $\mathbb{Z}/3\mathbb{Z}$ are cosets

$$3\mathbb{Z} = \{\dots, -3, 0, 3, \dots\}$$
$$1+3\mathbb{Z} = \{\dots, -2, 1, 4, \dots\}$$
$$2+3\mathbb{Z} = \{\dots, -1, 2, 5, \dots\}$$

Example addition in $\mathbb{Z}/3\mathbb{Z}$: $(2+3\mathbb{Z}) + (2+3\mathbb{Z}) = 4+3\mathbb{Z} = 1+3\mathbb{Z}$

Can also compute as $(5+3\mathbb{Z}) + (-1+3\mathbb{Z}) = 4+3\mathbb{Z} = 1+3\mathbb{Z}$

$(5+3\mathbb{Z}) + (2+3\mathbb{Z}) = 7+3\mathbb{Z} = 1+3\mathbb{Z}$.

$\mu : \mathbb{Z}/3\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}_3$ by

$$3\mathbb{Z} \to 0$$
$$1+3\mathbb{Z} \to 1$$
$$2+3\mathbb{Z} \to 2$$

---

Let $G$ be group $H \leq G$. Can we define binary operation on $G/H$ by $aH\,bH = (ab)H$?

This may be ill-defined: If $aH = a'H$, $bH = b'H$, may have

$$(ab)H \neq (a'b')H.$$

**Example** Let $H = \langle (12) \rangle \leq S_3$, $a = e$, $b = (13)$

$$aH = eH = H = \{e, (12)\}, \quad bH = \{(13), (123)\}$$

Take $a' = (12)$, $b' = (13)$. Then

- $aH = a'H$
- $bH = b'H$
- $ab = (13)$, $a'b' = (132)$, $(ab)H = (13)H \neq (132)H = (a'b')H$.

Recall $H$ is <u>normal</u> if

$$aH = Ha \qquad \forall a \in G.$$

<u>Thm</u> The formula $aHbH = (ab)H$ gives a well-defined binary operation on $G/H$ if and only if $H$ is normal.

<u>Proof of $H$ normal $\Rightarrow$ operation well defined.</u>

Let $a, b \in G$. Must show that if $a'H = aH$, $b'H = bH$, then $(ab)H = (a'b')H$.

Write $a' = ah_1$, $b' = bh_2$ $\quad h_1, h_2 \in H$.

$a'b' = ah_1bh_2$

$H$ normal $\Rightarrow Hb = bH$, $h_1b \in Hb = bH$, so $h_1b = bh_3$ $\quad h_3 \in H$.

$a'b' = ah_1bh_2 = abh_3h_2 \in abH$, so $a'b' \in abH$, hence $(a'b')H = (ab)H$. □

<u>Thm</u> Let $H \leq G$ be normal subgroup. The operation

$$aHbH = abH$$

makes $G/H$ a group.

Identity: $eHaH = (ea)H = aH = (ae)H = aHeH \Rightarrow eH$ is identity

Inverse: $a^{-1}HaH = (a^{-1}a)H = eH = (aa^{-1})H = aHa^{-1}H \Rightarrow (aH)^{-1} = a^{-1}H$.

<u>Notation</u>: $G/H$ is the quotient group / factor group of $G$ by $H$ ("kvotientgruppe")

<u>Example</u> $n\mathbb{Z} \leq \mathbb{Z}$ is normal, since $\mathbb{Z}$ is abelian.

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\}$$

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$$

$(\mathbb{R}^*, \cdot) = (\mathbb{R}\setminus\{0\}, \cdot)$, has subgroup $\{1,-1\}$, normal since $(\mathbb{R}^*, \cdot)$ is abelian.

Group $\mathbb{R}^*/_{\{1,-1\}}$ has elements $a\{1,-1\} = \{a,-a\}$ $\quad a \in \mathbb{R}^*$,

multiplication is $\{a,-a\}\{b,-b\} = \{ab,-ab\}$.

$\mathbb{R}^*/\{1,-1\} \simeq (\mathbb{R}^+, \cdot)$.

---

"Every normal subgroup is a kernel".

Thm Let $G$ be a group, $H \leq G$ normal. Then

$\gamma : G \longrightarrow G/H$ given by

$$\gamma(x) = xH$$

is a homomorphism, with kernel $H$.

Proof: $\gamma(xy) = xyH = xHyH = \gamma(x)\gamma(y)$

$\operatorname{Ker}\gamma = \{x \in G \mid \gamma(x) = eH\} = \{x \in G \mid xH = H\} = H$. □

The fundamental homomorphism theorem: Let $\phi : G \longrightarrow G'$ be a group homomorphism. Then $\phi[G] \leq G$ is a subgroup, and $\phi = \mu \circ \gamma$, $(H = \operatorname{Ker}\phi)$

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \phi[G] \leq G' \\ & \searrow^{\gamma} & \uparrow_{\mu} \\ & & G/H \end{array}$$

with $\mu$ an isomorphism.

Example Let $G'$ be a group, $a \in G'$. Define $\phi : \mathbb{Z} \longrightarrow G'$ by

$$\phi(k) = a^k,$$

$\phi$ is a homomorphism. $\operatorname{Ker}\phi = \{k \in \mathbb{Z} \mid a^k = e'\} = \begin{cases} \{0\}, & \text{or} \quad \text{I} \\ n\mathbb{Z} \text{ for some } n \geq 1 & \text{II} \end{cases}$

$\phi[\mathbb{Z}] = \langle a \rangle$.

I $\quad \mathbb{Z} \longrightarrow \langle a \rangle$, $\quad \mathbb{Z}/\{0\} \simeq \mathbb{Z}$

II $\quad \mathbb{Z} \longrightarrow \langle a \rangle$, $\quad \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$

# Criteria for normality

Given group $G$, $H \leq G$, when is $H$ normal?

Easy cases:
- $G$ abelian
- $H = \{e\}$, $H = G$
- $H = \ker \phi$ for some homomorphism $\phi$

**Thm** Let $G$ be a group, $H \leq G$. The following are equivalent:

1. $\forall g \in G, \forall h \in H, \quad ghg^{-1} \in H$
2. $\forall g \in G, \quad gHg^{-1} := \{ghg^{-1} \mid h \in H\} = H$
3. $\forall g \in G, \quad gH = Hg$
4. $H$ is normal

Note: 3 $\Leftrightarrow$ 4 by definition

Proof of 1 $\Rightarrow$ 3: Let $g \in G$, check $gH \subseteq Hg$, leave $Hg \subseteq gH$ to the book.

For $h \in H$, have $gh \in gH$, want $gh \in Hg$.

1 $\Rightarrow ghg^{-1} \in H \Rightarrow ghg^{-1} = h'$ for $h' \in H$.

$\Rightarrow gh = h'g \in Hg$. □

Example: $GL_n(\mathbb{R}) = \{\text{invertible } (n \times n)\text{-matrices}\}$ with matrix multiplication.

Let $H = \{A \in GL_n(\mathbb{R}) \mid \det(A) > 0\}$, a subgroup.

$H$ is normal, since for any $B \in GL_n(\mathbb{R})$, $A \in H$, have

$$\det(BAB^{-1}) = \det B \det A \det B^{-1} = \det B \det A (\det B)^{-1} = \det A > 0,$$

so $BAB^{-1} \in H$.

Def: An isomorphism $\phi : G \to G$ is an <u>automorphism</u> of $G$.

For $g \in G$, the map $i_g : G \to G$ given by

$$i_g(x) = gxg^{-1}$$

is an automorphism.

Proof $i_g$ a homomorphism: $i_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = i_g(x)\, i_g(y)$

$i_{g^{-1}}$ is an inverse to $i_g$: $i_{g^{-1}}(i_g(x)) = g^{-1}(gxg^{-1})g = x$

$i_g(i_{g^{-1}}(x)) = g(g^{-1}xg)g^{-1} = x,$

so $i_g$ is one-to-one & onto. □

$i_g$ is the inner automorphism of $G$ by $g$ / conjugation by $g$.

$H \leq G$ is normal $\iff i_g[H] = H \quad \forall g \in G.$