Theorem 3 (Lagrange)

If G is a finite group of order $\#G$ and H is its subgroup of order $\#H$ then $\#H$ is a divisor of $\#G$.

Def: Integer $m = \#G/\#H$ is called index of a subgroup.

Proof (Lagrange)

- let m is the number of distinct left cosets with resp. to H

$\overset{(2)}{\Rightarrow}$ each has $\#H$ elements

$\overset{(3)}{\Rightarrow}$ they have no common element

$\left.\right\}$ $\Rightarrow$ contain $m\,\#H$ elements

$\overset{(1)}{\Rightarrow}$ every $g \in G$ belongs to same $g'H$ $\Rightarrow$ $\#G = m\,\#H$ $\boxtimes$

Example: • the only 5-element group is cyclic:

$\Leftarrow$ let there be an element of order < 5 $\Rightarrow$ it generates cyclic subgroup of the same order which would divide 5 ↯

Not:

e	a	b	c	d
a	e	c	d	b
b	c	d	a	e
c	d	e	b	a
d	b	a	e	c

- satisfies the rearrangement th.
- contains $\{e, a\}$ subgroup

$\Rightarrow$?

$(ab)c = cc = b \neq a(bc) = aa = e$

$\Rightarrow$ it's not a group!

CONJUGACY CLASSES

Def: An element $g' \in G$ is said to be conjugate to $g \in G$ if $\exists h \in G: g' = hgh^{-1}$

note: conjugation is an equivalence relation (reflexivity $a \sim a$, symmetry $a \sim b \Rightarrow b \sim a$, transitivity $a \sim b$ & $b \sim c \Rightarrow a \sim c$)

- as every equivalence relation, it leads to the decomposition of G to classes of conjugate elements:

Def: A [conjugacy] class of G is a set of mutually conjugate elements:

$$C_g \equiv (g) = \{hgh^{-1} / h \in G\}$$

- elements hgh^{-1} are taken only once if repeated
- any element of (g) generates the same class

Lemma
1, Every element of G is a member of same class
2, No element of G can be a member of two dif. classes.
3, The identity e of G always forms a class on its own.
4, G is abelian $\Rightarrow (g) = \{g\} \quad \forall g \in G$

Proof: (exercise)

Theorem 4

Number of elements in any class (g) is a divisor of $\#G$.

Proof: (self-study)

- $g_j \in (g) \Rightarrow H = \{h \in G / g_j h = h g_j\}$ is a subgroup:

$$a, b \in H \Rightarrow (ab^{-1}) g_j (ab^{-1})^{-1} = ab^{-1} g_j b a^{-1} = g_j$$
$$\Rightarrow ab^{-1} \in H \quad \square$$

- let $t_k H$ is left coset and $\tau_1 \in t_k H$

$$\Rightarrow \tau_1 g_j \tau_1^{-1} = t_k h_1 g_j h_1^{-1} t_k^{-1} = /h_1 \in H/ = t_k g_j t_k^{-1} = g_k \in (g)$$

$\Rightarrow$ all elements from $t_k H$ generate from g_j through conjugation the same element of (g)

- there exist $m = \#G/\#H$ cosets, which generate m <u>different</u> elements of (g).

  $\left(\begin{array}{l} \text{let } t_\ell H \neq t_k H \ \& \ t_\ell g_j t_\ell^{-1} = t_k g_j t_k^{-1} \\ \Rightarrow t_k^{-1} t_\ell g_j t_\ell^{-1} t_k = g_j \Rightarrow t_k^{-1} t_\ell \in H \Rightarrow t_\ell \in t_k H \ \text{↯} \end{array} \right)$

- each $g' \in G$ belongs to some $t_k H$ & each $g'' \in (g)$ can be generated from g_j using some element of G

$$\Rightarrow \#(g) = m = \frac{\#G}{\#H} \qquad \boxtimes$$

$\Rightarrow$ Tutorial on point groups, examples of classes & cosets

<u>Poznámka k české terminologii:</u>

[conjugacy] class = <u>třída</u> sdružených prvků
[left] coset w.r. to H = [levá] rozkladová <u>třída</u> podle H

<u>Ex:</u> $C_{3v} = \{E, C_3, C_3^2, \sigma_v, \sigma_v', \sigma_v''\}$

1, $(E) = \{E\}$
2, $(C_3) = \{C_3, C_3^2\}$
3, $(\sigma_v) = \{\sigma_v, \sigma_v', \sigma_v''\}$

<u>Proof:</u> a, algebraic (home exercice) - find $h \in C_{3v}$ for each $g' \in (g)$: $g' = h g h^{-1}$

b, geometrical $\rightarrow$ all σ planes are "equivalent" - can be generated from σ_v using other operations from the group, namely C_3 & C_3^2

$\rightarrow$ C_3 axis has no other equiv. sym. element

INVARIANT SUBGROUPS, FACTOR GROUPS

Def: A subgroup $H \subset G$ is said to be an invariant subgroup ($H \triangleleft G$)

$$\forall g \in G \ \forall h \in H : ghg^{-1} \in H$$

- other terminology: normal subg., normal divisor
- also self-conjugate subg:

$$\forall g \in G \quad gHg^{-1} \subset H \Rightarrow \Big/ \begin{matrix} g \in H \& \\ \text{rearr.} \end{matrix} \Big/ \Rightarrow gHg^{-1} = H$$

$\Rightarrow \boxed{gH = Hg}$ ... for normal subg., left & right cosets are the same

Def: Center of a group is invariant subgr.

$$Z(G) = \{ z \in G \mid zg = gz \ \forall g \in G \}$$

Note: • G abelian $\Leftrightarrow$ $Z(G) = G$
• $Z(G)$ is an union of one-element classes

Def: Group is said to be simple (prostá) if it does not have any nontrivial invariant subgroup. It's said to be semi-simple (poloprostá) if it does not contain any non-trivial abelian inv. subgroup.

- important for classification of finite & Lie groups and, consequently, for representation theory

Theorem 5:

$H \triangleleft G \Leftrightarrow H$ consists entirely of complete classes of G.

Proof: $\Leftarrow$/ obvious

$\Rightarrow$/ • let $h \in H$ & $h \sim g \in G \Rightarrow \exists a \in G : g = aha^{-1}$

$\Rightarrow / H \triangleleft G / \Rightarrow g \in H \Rightarrow$ whole $(h) \subset H$ $\boxtimes$

Def: <u>Product of left cosets</u> with respect to normal subgroup $H \triangleleft G$ is defined by

$$g_1 H \cdot g_2 H \equiv (g_1 g_2) H \qquad (*)$$

Proof of <u>consistency</u>: $(*)$ is rewritten as

$$\{ g_1 h g_2 h' \,/\, h, h' \in H \} = \{ g_1 g_2 h \,/\, h \in H \}$$

- works for normal subgroup:

$$(g_1 H)\cdot(g_2 H) = \big/ \underline{g_2 H = H g_2} \big/ = (g_1 H)\cdot(H g_2) = \big/ \text{associativity \& rearr. theorem} \big/ = g_1 H g_2 = \big/ \ \big/ = g_1 g_2 H \quad \boxtimes$$

<u>Theorem 6:</u> The set of all distinct left cosets with resp. to an invariant subgr. $H \triangleleft G$ forms a group, with $(*)$ defining the binary operation. This group is called a <u>factor group</u> and is denoted

$$G/H \equiv \{ gH \,/\, g \in G \} \qquad \#(G/H) = \frac{\#G}{\#H} \quad (\text{Lagr.})$$

Note:
- G/H is also called quotient group
- can be equiv. defined using right cosets ($gH = Hg$ for $H \triangleleft G$ after all...)

Proof:
1. $(*)$ by itself ensure closure of G/H
2. $$\left.\begin{array}{l} (g_1 H \cdot g_2 H)(g_3 H) = (g_1 g_2 H)(g_3 H) = (g_1 g_2) g_3 H \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad ||| \\ (g_1 H)(g_2 H \cdot g_3 H) = (g_1 H)(g_2 g_3 H) = g_1 (g_2 g_3) H \end{array}\right\} \text{assoc.}$$
3. identity element is $eH = H$ (obvious)
4. $(gH)^{-1} = g^{-1} H$ (obvious) $\quad \boxtimes$

Note:
- any non-simple group can be broken into nontriv. inv. subgroup & corresp. factor group; this can be repeated $\Rightarrow$ finite groups can be "decomposed" to simple groups

HOMOMORPHIC MAPPINGS

- map(ping) $\phi: G \to G'$ is a rule which to every $g \in G$ assigns some $\phi(g) \in G'$

Def: Homomorphic mapping of a group G to a group G' is a mapping $\phi: G \to G'$ satisfying

$$\phi(g_1) \cdot \phi(g_2) = \phi(g_1 \cdot g_2) \qquad \forall g_1, g_2 \in G$$

- i.e., homomorphism preserves the algebraic structure of G (the group multiplication)

Def: Let ϕ be a homomorphism $\phi: G \to G'$. Then set of elements

$$Ker_\phi \equiv \{ g \in G \,/\, \phi(g) = e' \} \subset G$$

is called kernel of the mapping.

Def: The set $Im_\phi \equiv \{ g' \in G' \,/\, \exists g \in G \;\; \phi(g) = g' \} \subset G'$
is called image of the map $\phi: G \to G'$

Def: The mapping $\phi: G \to G'$ is said to be

1, surjective (epimorphism, onto) if $Im_\phi(G) = G'$

2, injective (monomorphism) if $g_1 \neq g_2 \Rightarrow \phi(g_1) \neq \phi(g_2)$
$\quad \Leftrightarrow \exists \phi^{-1}$ on Im_ϕ

3, bijective (isomorphism) if it is both surjective & injective. Notation:

! ISOMORPHISM is one-to-one mapping from G onto G'.

Notation: $\phi: G \to G \Rightarrow$ homomorphism $\equiv$ endomorphism
isomorphism $\equiv$ automorphism

Example: $\phi_a(g) := a g a^{-1}$ ... inner automorphism

Lemma: a, $\phi(e_G) = e_{G'}$

b, $\phi(g^{-1}) = (\phi(g))^{-1} \quad \forall g \in G$ for $\phi: G \to G'$ homom.

Proof: • exercise

Note: $(\phi(g))^{-1} \neq \phi^{-1}(g)$ ... the latter might not even $\exists$

Theorem 7

Let $\phi: G \to G'$ be a homomorphic mapping. Then

a, Ker_ϕ is a normal subgroup of G

b, Im_ϕ is a subgroup of G'

c, $Im_\phi \sim G/Ker_\phi$

Proof: a, • $Ker_\phi \leq G$ by verification of the 4 axioms (ex.)

3, $e \in Ker_\phi$ (lemma)

4, $g \in Ker_\phi \Rightarrow \phi(g) = e'$ & $\phi(g^{-1}) = (\phi(g))^{-1} = (e')^{-1} = e'$

$\Rightarrow g^{-1} \in Ker_\phi$

1, $g_1, g_2 \in Ker_\phi \Rightarrow \phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) = e' \cdot e' = e'$

• $Ker_\phi \triangleleft G$: $g \in Ker_\phi, a \in G \Rightarrow$

$\phi(aga^{-1}) = \phi(a)\phi(g)\phi(a^{-1}) = e'$ $\square$

b, $Im_\phi \leq G$ by verif. of the axioms (ex.)

c, • $Ker_\phi \triangleleft G \Rightarrow G/Ker_\phi$ is factor group

• $G = e\,Ker_\phi + g_2 Ker_\phi + \dots + g_n Ker_\phi$

• ϕ itself is the isomorphism $G/Ker_\phi \sim Im_\phi$:

$\to \phi(g_i Ker_\phi) = \phi(g_i) e' = \phi(g_i)$

$\Rightarrow$ whole coset is mapped onto a single element

$\to \phi: G/Ker_\phi \to Im_\phi$ is surjective by def. of Im_ϕ

→ it is one-to-one: let $\phi(g_1 \mathrm{Ker}_\phi) = \phi(g_2 \mathrm{Ker}\,\phi) = g'$

$\Rightarrow \phi(g_1) = \phi(g_2) = g' \qquad / \cdot\ \phi(g_1^{-1}) = (g')^{-1}$

$\Rightarrow \phi(g_1^{-1})\,\phi(g_1) = \phi(e) = e' = \phi(g_1^{-1} g_2)$

$\Rightarrow g_1^{-1} g_2 \in \mathrm{Ker}_\phi \Rightarrow g_2 \in g_1 \mathrm{Ker}_\phi \Rightarrow g_2 \mathrm{Ker}_\phi = g_1 \mathrm{Ker}_\phi$ $\boxtimes$

<u>Def:</u> Let $H \triangleleft G$ be normal subgroup of G. Then the mapping

$$\pi : G \to G/H \qquad g \mapsto gH$$

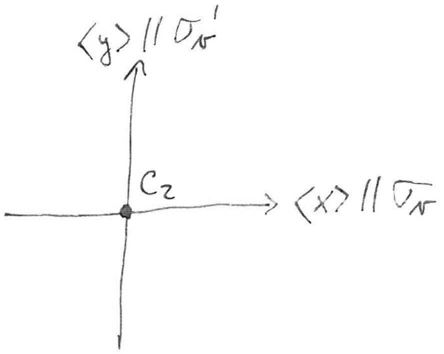
is called <u>canonical projection</u> of G onto G/H

<u>Theorem 8</u>

Canonical projection is surjective and $\mathrm{Ker}_\pi = H$.

<u>Proof:</u> analog. to T7

<u>Example:</u> homomorphisms of $C_{2v} = \{E, C_2, \sigma_v, \sigma_v'\}$



a, <u>$\varphi : C_{2v} \to M^{3\times 3}$</u> ($\sim$ trans. of $\mathbb{R}^3$)

$g \mapsto D(g) \qquad D(g)\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$

$D(E) = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix} \qquad D(C_2)\begin{pmatrix} \vec{x} \end{pmatrix} = \begin{pmatrix} -x \\ -y \\ z \end{pmatrix} \Rightarrow D(C_2) = \begin{pmatrix} -1 & & 0 \\ & -1 & \\ 0 & & 1 \end{pmatrix}$

$D(\sigma_v) = \begin{pmatrix} 1 & & 0 \\ & -1 & \\ 0 & & 1 \end{pmatrix} \qquad D(\sigma_v') = \begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}$

- injective map $C_{2v} \to M^{3\times 3}$
- <u>faithful</u> matrix <u>representation</u>

b, <u>$\varphi_x : C_{2v} \to M^{1\times 1}$</u> (transf. on the x-axis)

$x' = D_x(g)\, x \qquad D_x(E) = 1 \quad D(C_2) = -1$

$D_x(\sigma_v) = 1 \quad D_x(\sigma_v') = -1$

- surjective map $C_{2v} \to (\{1, -1\}, \cdot)$

(15)

c) $\varphi_y : C_{2v} \to (\{1,-1\}, \cdot)$ $\qquad y' = D_y(g)\, y$

$$D_y(E) = 1 \quad D_y(C_2) = -1, \quad D_y(\sigma_v) = -1, \quad D_y(\sigma_v') = 1$$

d) $\varphi_z : D_z(E) = D_z(C_2) = D_z(\sigma_v) = D_z(\sigma_v') = 1$

$$C_{2v} \to (\{1\}, \cdot) \equiv \underline{\text{trivial representation}}$$

- (home ex): show that all maps are homomorphisms
- $Ker_\varphi = \{E\}$, $Ker\varphi_x = \{E, \sigma_v\}$, $Ker\varphi_y = \{E, \sigma_v'\}$, $Ker\varphi_z = C_{2v}$
- $\{E, C_2\} \triangleleft C_{2v}$ is normal $\Rightarrow \exists\, \overline{u} : C_{2v} \to C_{2v}/\{E, C_2\}$

$$\Rightarrow D_{\overline{u}}(E) = 1, \; D_{\overline{u}}(C_2) = 1, \; D_{\overline{u}}(\sigma_v) = -1, \; D_{\overline{u}}(\sigma_v') = -1$$

$\Rightarrow$ we have found 4 non-equiv. homomorphisms

$$C_{2v} \to M^{1\times 1}$$

(they comprise complete set of $\underline{\text{irreducible representations}}$)

DIRECT & SEMI-DIRECT PRODUCT GROUPS

Def: Group G is said to be a direct product group if it is isomorphic to a group $G_1 \otimes G_2$ of ordered pairs (g_1, g_2) for $g_1 \in G_1$ & $g_2 \in G_2$ with binary operation

$$(g_1, g_2) \cdot (g_1', g_2') \equiv (g_1 g_1', g_2 g_2') \quad \forall g_1, g_1' \in G_1 \quad \forall g_2, g_2' \in G_2$$

Notes:
- $G_1 \otimes G_2$ is a group: $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$
  $e_{G_1 \otimes G_2} = (e_1, e_2)$
- for finite groups, $\#(G_1 \otimes G_2) = (\#G_1) \cdot (\#G_2)$
- set $((g_1, e_2), \cdot)$ forms a normal subgr. of $G_1 \otimes G_2$, which is isomorphic to G_1
- same for $((e_1, g_2), \cdot) \sim G_2$
- (g_1, e_2) & (e_1, g_2) commute, both sets have only one common element (e_1, e_2) and any element of $G_1 \otimes G_2$ can be expressed as a product of elements from the two subgroups $\Rightarrow$

Theorem 9

Let G has two subgroups G_1 and G_2 such, that
- a, all elements of G_1 commute with all elements of G_2
- b, $G_1 \cap G_2 = \{e\}$
- c, $\forall g \in G \;\; \exists g_1 \in G_1 \;\; \exists g_2 \in G_2 : g = g_1 g_2$

then $G \sim G_1 \otimes G_2$

Note: • a, can be replaced by an assumption that both G_1 & G_2 are normal subgr.

Proof: (Cornwell p. 39)
1, $g = g_1 \cdot g_2$ is unique (by contradiction)
2, $\vartheta : G \to G_1 \otimes G_2 : g \mapsto (g_1, g_2)$ is isomorph.

Examples

- $O(3) \sim SO(3) \otimes C_i \qquad C_i = \{E, i\}$
- $C_6 = \{e, a, a^2, a^3, a^4, a^5\} \sim \{e, a^2, a^4\} \otimes \{e, a^3\}$
- $Sym(n = n_1 + n_2) \supset Sym(n_1) \otimes Sym(n_2)$
  - -> $Sym(n_1) \triangleleft Sym(n)$ (does not "touch" $n_1+1, \dots, n_1+n_2$), same for $Sym(n_2)$
  - -> however, $Sym(n_1) \otimes Sym(n_2)$ does not contain permutations between $\{1, \dots, n_1\}$ & $\{n_1+1, \dots, n_1+n_2\}$
- $D_6 \sim D_3 \otimes C_2$ ... see homework #1

Def: G is called to be a semi-direct product group ($G \sim G_1 \circledS G_2$, $G \sim G_1 \wedge G_2$) if it possesses ~~two~~ subgroups G_1 and G_2 such that

a, $G_1 \triangleleft G$ is a normal subgr.

b, $G_1 \cap G_2 = \{e\}$

c, $\forall g \in G \; \exists g_1 \in G_1 \; \exists g_2 \in G_2 : g = g_1 \cdot g_2$

Note: b, implies that the decomposition c, is unique

Examples

- $Sym(3) = A_3 \wedge Sym(2)$
  - -> $A_3 = \{e, (312), (231)\}$ is "alternating group" (even permutations)

    $A_3 \triangleleft Sym(3)$
  - -> $Sym(2) = \{e, (21)\}$ is not invariant
  - -> in general: A_n is the kernel of an homomorphism $sgn : Sym(n) \to (\{1, -1\}, \circ) \Rightarrow$ is invariant by Th 7

- <u>Euklidean group</u> $E(3) \sim (\text{transl.}) \wedge (\text{rotations})$

$\rightarrow g \in E(3) \Rightarrow g \equiv (R(g) | \vec{t}(g))$

$\vec{r}\,' = R(g)\vec{r} + \vec{t}(g) \Rightarrow \vec{r} = R(g)^{-1}\vec{r}\,' - R(g)^{-1}\vec{t}(g)$

$\rightarrow \boxed{g^{-1} = (R(g)^{-1} | -R(g)^{-1}\vec{t}(g))}$

$\rightarrow \boxed{(R(g_1 g_2) | \vec{t}(g_1 g_2)) = (R(g_1)R(g_2) | R(g_1)\vec{t}(g_2) + \vec{t}(g_1))}$

$\rightarrow (\mathbb{1}, \vec{t}(g)) \triangleleft E(3)$:

$(R(h) | \vec{t}(h)) \cdot (\mathbb{1}, t(g)) \cdot (R(h)^{-1} | -R(h)^{-1} t(h))$

$= (R(h) | t(h)) \cdot (R(h)^{-1} | -R(h^{-1}) t(h) + t(g))$

$= (\mathbb{1}, -t(h) + R(h)t(g) + t(h)) = (\mathbb{1}, R(h)t(g)) \in (\text{transl.})$

$\rightarrow (R(g) | t(g)) = (\mathbb{1} | t(g)) \cdot (R(g) | \vec{0})$

$\rightarrow (\text{transl.}) \cap (\text{rot.}) = (\mathbb{1} | \vec{0})$ is obvious

- <u>Poincaré group</u> analog.

$x' = \Lambda(g)x + t(g)$