1. OPAKOVÁNÍ

GROUPS, LAGRANGE THEOREM, ISOMORPHISM THEOREMS

Definition: A *group* is a set, say, G with a binary operation $\cdot$ s.t

1) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (\forall a, b, c \in G)$ — $\cdot$ is associative
2) There is an element $1 \in G$ s.t $\quad a \cdot 1 = a = 1 \cdot a \quad (\forall a \in G)$ — 1 is called a unit of G
3) For every $a \in G$, there is $a^{-1} \in G$ s.t $\quad aa^{-1} = a^{-1}a = 1$ — a^{-1} is called an inverse of a

A group G is *abelian* if

4) $a \cdot b = ba \quad (\forall a, b \in G)$

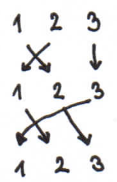
Remarks:

- A unit element is unique
- For every $a \in G$, the inverse element is unique
- The following holds true in a group:
  1) $a \cdot b = ac \Rightarrow b = c$
  2) $b \cdot a = ca \Rightarrow b = c$
  3) Every equation $a \cdot x = b$ with a variable x has a solution
  4) Every equation $xa = b$ with a variable x has a solution

Joseph Louis Lagrange
1736 – 1813

Examples of groups:

1) The *Symmetric group* S_n: the group of all permutations of an n-element set with the operation of composition. We compose permutations from the right to the left as maps: $(123)(12) = (13)$

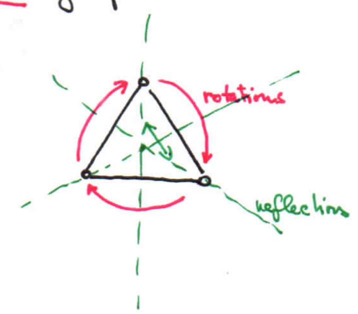


2) The *alternating group* A_n: the group of all even permutations of an n-element set.

   Recall: A permutation is even if it is a product of even number of transpositions.

3) *Dihedral group* D_n: the group of all symmetries of a regular polygon

D_3:



4) Some matrix groups: $\mathbb{F}$ - a field

general linear group → • $GL_n(\mathbb{F})$ = the group of all regular $n\times n$ matrices with n-ties from a field $\mathbb{F}$

• $SL_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid \det A = 1\}$. This is a special linear group

• $O_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid AA^T = I_n\}$. The orthogonal group.
the unit $n\times n$ matrix

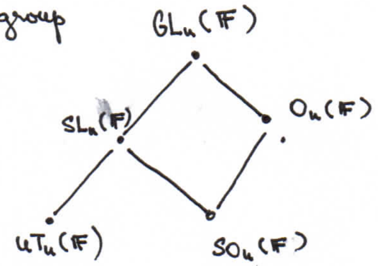
• $SO_n(\mathbb{F}) = \{A \in \cancel{GL} O_n(\mathbb{F}) \mid \det A = 1\}$. The special orthogonal group or the group of all rotations.

• $UT_n(\mathbb{F})$ = upper triangular matrices with 1 on diagonal. Unitriangular group.

5) Commutative groups

Remark: Finite fields are uniquely (up to isomorphism) determined by their size which is a power $q = p^k$ of a prime. We write $GL_n(q)$ for $GL_n(\mathbb{F})$ then.

Definition: A subgroup of a group G is a subset $H \subseteq G$ ~~so~~ that is a group w.r.t. the same operation. A subgroup H is proper if $H \subsetneq G$. We denote $H \leq G$ ($H < G$) that H is a subgroup of G (H is a proper subgroup of G).



Definition: A homomorphism is a map $\phi: G \to H$ from a group G to a group H such that $\phi(a.b) = \phi(a)\phi(b)$ for all $a, b \in G$.

⚠ • $\phi(1) = 1$
• $\phi(a^{-1}) = \phi(a)^{-1}$

Types of homomorphisms:

• monomorphism (or embedding): ϕ is 1-1
• epimorphism: $\phi(G) = H$
• isomorphism: ϕ is bijection

Definition: • An order of an element $a \in G$ is $\begin{cases} \text{the smalles positive } n \text{ s.t } a^n = 1 \\ \infty \text{ if no such } n \text{ exists.} \end{cases}$ We denote it by $|a|$.

• An order of a group G is its size. Denoted $|G|$.

• A ~~group~~ finite group G is a p-group, p is a prime, if $|G| = p^k$.

- $a^n = 1$ iff $|a| \mid n$
- If $ab = ba$ and $\gcd(|a|, |b|) = 1$, then $o(ab) = o(a)\,o(b)$.

Definition: For a subset X of a group G we denote by $\langle X \rangle$ the smallest subgroup of G containing X and call this subgroup the (sub)group generated by X. A group is cyclic if it is generated by a single element.

$$\langle X \rangle = \bigcap \{ H \leq G \mid X \subseteq H \} = \{ a_1^{\alpha_1} \cdots a_m^{\alpha_m} \mid m \in \mathbb{N}, \alpha_i \in \mathbb{Z}, a_i \in X \}.$$

Theorem 1.1: • An infinite cyclic group is isomorphic to $\mathbb{Z}$.
• A finite cyclic group is isomorphic to $\mathbb{Z}_n$, where n is the order of the group.

Proof: Define $\phi : \mathbb{Z} \to G$, $z \mapsto a^z$ $\qquad G = \langle a \rangle$

- $\phi(u+v) = a^{u+v} = a^u a^v = \phi(u)\phi(v)$

$\to$ If $|a| = \infty$, then ϕ is one-to-one and so $G \simeq \mathbb{Z}$.

$\to$ If $|a| = n$, then $\phi(k) = \phi(m)$ iff $m \equiv k \pmod n$ and so $G \simeq \mathbb{Z}_n$. $\square$

Theorem 1.2: A subgroup of a cyclic group is cyclic

Proof: Let $G = \langle a \rangle$ be a cyclic group and $H \leq G$. If $H = \langle 1 \rangle$, a trivial group, it is cyclic (generated by 1). If H is non-trivial, we denote by m the least positive integer such that $a^m \in H$. Then $\langle a^m \rangle = H$. $\square$

Remark: It can be refined:

- Subgroups of $\mathbb{Z}$ are exactly of the form $m\mathbb{Z}$
- Subgroups of $\mathbb{Z}_n$ are in one-to-one correspondence with divisors of n.

Lagrange's theorem

Definition: Let G be a group and H a subgroup of G.

A left coset = a subset $gH = \{ gh \mid h \in H \}$

A right coset = a subset $Hg = \{ hg \mid h \in H \}$

$$g_1 H = g_2 H \iff g_2^{-1} g_1 \in H \iff g_1^{-1} g_2 \in H$$

Lemma 1.3: $|\{gH \mid g \in G\}| = |\{Hg \mid g \in G\}|$

Proof: Define a bijection $\{gH \mid g \in G\} \longrightarrow \{Hg \mid g \in G\}$

$$gH \longmapsto Hg^{-1}$$

$\square$

Definition: The size $|\{gH \mid g \in G\}|$ of the set of left cosets is called the index of H in G and it is denoted by $|G:H|$

Theorem 1.4 (Lagrange): Let H be a subgroup of a finite group G. Then

$$|G| = |H| \cdot |G:H| \qquad (*)$$

Proof:
- $\begin{aligned} H &\longrightarrow gH \\ h &\longmapsto gh \end{aligned}$ is a bijection, so $|H| = |gH|$

- $g_1H \cap g_2H \neq \emptyset$ iff $g_1H = g_2H$

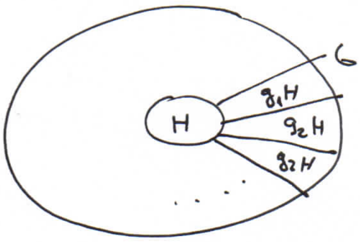
  $\Rightarrow$ $g_1H \cap g_2H \neq 0$

  ~~Take exist~~ then $g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$.

  Hence $g_2^{-1}g_1 = h_2h_1^{-1} \in H$, whence $g_1H = g_2H$.

  $\Leftarrow$ trivial.

We have a partition of G into $|G:H|$ blocks of the same size. $(*)$ follows.



$\square$

Definition: A subgroup H of a group G is normal if $gH = Hg$ for all $g \in G$.

We denote by $H \trianglelefteq G$ that H is a normal subgroup of G.

$H \trianglelefteq G$ iff $gHg^{-1} = H$ for all $g \in G$.

Lemma 1.5: A subgroup H of a group G is normal iff the product of two left cosets of H is again a left ~~coset~~ coset of H.

- $A, B \subseteq G$. Define

$$A \cdot B = \{ab \mid a \in A, b \in B\}.$$

Proof: ($\Rightarrow$) Suppose that $H \trianglelefteq G$. Then

$$g_1 H g_2 H = g_1 H H g_2 = g_1 H g_2 = g_1 g_2 H$$

Note: $HH = H$

($\Leftarrow$) $1 \in gHg^{-1}H$, and so $gHg^{-1}H = 1H = H$

It follows that $gHg^{-1} \subseteq H$, hence ~~$gHg^{-1} = H$~~ $gH \subseteq Hg$.

Opposite inclusion similarly.

$\square$

- If $H \trianglelefteq G$, then $\{gH \mid g \in G\}$ forms a group.

  $H \cdot gH = gH = gH \cdot H$

  $g^{-1}H\, gH = H = gH g^{-1}H$

Definition: We denote this group by G/H and call the quotient (or factor) group of G by H.

$$|G/H| = |G : H|$$

Homomorphism theorems

$\phi : G \longrightarrow G_1$ a homomorphism

- $\operatorname{Ker} \phi = \{ g \in G \mid \phi(g) = 1 \}$
- $\operatorname{Im} \phi = \phi(G) = \{ \phi(g) \mid g \in G \}$

Lemma 1.6: Kernels of homomorphisms are exactly normal subgroups.

Proof: • Kernels are normal subgroups:

$\phi : G \to G_1$ a homomorphism

$H = \operatorname{Ker} \phi$

$g \in G,\ h \in H:\quad \phi(ghg^{-1}) = \phi(g)\,\phi(h)\,\phi(g^{-1}) = \phi(g) \cdot 1\, \phi(g)^{-1} = 1$

$\Rightarrow ghg^{-1} \in H$ so $H \trianglelefteq G$.

• If $H \trianglelefteq G$ then $\pi_H : G \longrightarrow G/H$, $g \longmapsto gH$ is a homomorphism with $H = \operatorname{Ker} \pi_H$. $\square$

Lemma 1.7: Let $\phi : G \to G_1$ be a group homomorphism. Then for every non-empty subset A of G:

$$A \cdot \ker \phi = \phi^{-1}(\phi(A))$$

Remark: Here the notation is

- $\phi(A) = \{\phi(a) \mid a \in A\} \subseteq G_1$
- $\phi^{-1}(B) = \{g \in G \mid \phi(g) \in B\}$ for $B \subseteq G_1$.

Proof: From

$$\phi(A \cdot \ker \phi) = \phi(A) \cdot \phi(\ker \phi) = \phi(A) \cdot \{1\} = \phi(A),$$

we infer that $A \cdot \ker\phi \subseteq \phi^{-1}(\phi(A))$.

On the other hand, if $\phi(g) \in \phi(A)$, then $\phi(g) = \phi(a)$ for some $a \in A$. It follows that $\phi(ga^{-1}) = 1$, hence $ga^{-1} \in \ker\phi$, whence $g \in a \ker\phi \subseteq A \ker\phi$. Therefore $\phi^{-1}(\phi(A)) \subseteq A \cdot \ker\phi$. □

Lemma 1.8: Let $\phi : G \to G_1$ be a group homomorphism ~~onto a group G_1~~. Then for non-empty subsets A, B of G:

$$\phi(A) = \phi(B) \quad \text{iff} \quad A \cdot \ker\phi = B \cdot \ker\phi$$

Proof. It follows readily from $\phi(A) = \phi(B)$ iff $\phi^{-1}(\phi(A)) = \phi^{-1}(\phi(B))$. □

Notation:

- $\mathrm{Sub}(G)$ denotes the poset of all subgroups of G.
- If $H \leq G$, then $\mathrm{Sub}(G, H)$ denotes the poset of all subgroups of G that contain H, i.e., $\mathrm{Sub}(G,H) = \{J \in \mathrm{Sub}(G) \mid H \leq J\}$.

Note: $\mathrm{Sub}(G) = \mathrm{Sub}(G, \{1\})$.

Theorem 1.9: Let $\phi : G \to G_1$ be a homomorphism onto a group G_1. Then ~~the two~~

1. The mapping
$$\phi^* : \mathrm{Sub}(G, \ker\phi) \to \mathrm{Sub}(G_1)$$
$$H \longmapsto \phi(H)$$
is a bijection.

2. If $\ker\phi \leq H_1 \leq H_2$, then $|H_2 : H_1| = |\phi^*(H_2) : \phi^*(H_1)|$ (i.e., the bijection ϕ^* preserves indexes).

3. If $\ker\phi \leq H_1 \leq H_2$, ~~and~~ then $H_1 \trianglelefteq H_2$ iff $\phi^*(H_1) \trianglelefteq \phi^*(H_2)$.

Proof.

1. By lemma above $\phi^{-1}(\phi(H)) = H \cdot \ker\phi$. If $\ker\phi \leq H$, then $H \cdot \ker\phi = H$, hence ϕ^* is one-to one.

Observe that for every $H_1 \leq G_1$, $\phi(\phi^{-1}(H_1)) = H_1 \cap \phi(G)$. Since ϕ is onto G_1, $\phi(G) = G_1$, hence $\phi(\phi^{-1}(H_1)) = H_1$. It follows that ϕ^* is onto.

2. Let $x, y \in H_2$. Since $\ker\phi \leq H_1$, $H_1 \cdot \ker\phi = H_1$. Applying above lemma, we get

$$xH_1 = xH_2 \quad \text{iff} \quad xH_1\ker\phi = yH_1\ker\phi \quad \text{iff} \quad \underbrace{\phi(x)\cdot\phi(H_1)}_{\phi(xH_1)} = \underbrace{\phi(y)\phi(H_1)}_{\phi(yH_1)}.$$

Moreover $x \in H_2$ iff $\phi(x) \in \phi(H_2)$. Therefore the mapping

$$x \cdot H_1 \longmapsto \phi(x)\phi(H_1) \quad ; \ (x \in H_2)$$

is a bijection from the set of left cosets of H_1 in H_2 to the set of left coset of $\phi(H_1)$ in $\phi(H_2)$. It follows that $|H_2 : H_1| = |\phi(H_2) : \phi(H_1)|$; indeed, the index of a subgroup is the number of left cosets.

3. Since $\ker\phi$ is a normal subgroup of G, $x\ker\phi = \ker\phi\, x$ for all $x \in G$. Given $x \in H_2$, we have

$$xH_1 = H_1 \cdot x \quad \text{iff} \quad xH_1\ker\phi = H_1\ker\phi \cdot x \quad (\text{here we use the fact that } \ker\phi \leq H_1)$$

$$\text{iff} \quad xH_1\ker\phi = H_1 x\ker\phi \quad (\text{as } \ker\phi \cdot x = x \cdot \ker\phi) \quad \text{iff} \quad \underbrace{\phi(xH_1)}_{\phi(x)\phi(H_1)} = \underbrace{\phi(H_1 x)}_{\phi(x)\phi(H_1)}.$$

Therefore $H_1 \trianglelefteq H_2$ iff $\phi(H_1) \trianglelefteq \phi(H_2)$. $\square$

Theorem: 1.10 If $\phi : G \longrightarrow G_1$ is a homomorphism, then $G/_{\ker\phi} \simeq \operatorname{Im}\phi$

Proof: Since $g\ker\phi = h\ker\phi$ iff $\phi(g) = \phi(h)$ for all $g, h \in G$, by above lemma, the mapping $g \cdot \ker\phi \mapsto \phi(g)$ is an isomorphism from $G/_{\ker\phi}$ onto $\operatorname{Im}\phi$. $\square$

Theorem: 1.11 Let $A \leq B \leq G$ and both A, B are normal subgroups of G. Then $B/A \trianglelefteq G/A$ and

$$G/A \big/ B/A \simeq G/B.$$

Proof: Let $g \in G$ and $b \in B$. As $B \trianglelefteq G$, $gbg^{-1} \in B$. Since $A \trianglelefteq G$, $gA = Ag$, $bA = Ab$ and $g^{-1}A = Ag^{-1}$. It follows that $(gA)(bA)(g^{-1}A) = (gbg^{-1}) \cdot A \in B \cdot A$. Hence $B/A \trianglelefteq G/A$.

Define a map $\phi : G/A \longrightarrow G/B$

$$gA \mapsto gB$$

- The map is well defined as $gA = hA \Rightarrow gB = hB$ (indeed, $A \le B$).
- For $g, h \in G$: $\phi(gA)\,\phi(hA) = gBhB \underset{\text{Since } B \trianglelefteq G}{=} ghB = \phi(ghA) = \phi(gAhA)$.

  Thus ϕ is a homomorphism.
- ϕ is clearly onto G/B.
- $gA \in \ker\phi$ iff $gB = B$ iff $g \in B$. Hence $\ker\phi = B/A$. $\square$

Theorem 1.12: Let $H \trianglelefteq G$ and $B \le G$. Then $BH/H \simeq B/B\cap H$.

Proof: Consider the map

$$\phi : BH \longrightarrow B/B\cap H$$
$$bH \longmapsto b\cdot(B\cap H)$$

and prove that:

1) ϕ is well defined: for $b_1, b_2 \in B$, $b_1H = b_2H \Rightarrow b_2^{-1}b_1 \in B\cap H \Rightarrow b_1(B\cap H) = b_2(B\cap H)$.

2) ϕ is a homomorphism: for $b_1, b_2 \in B$: $\phi(b_1Hb_2H) = \phi(b_1b_2H) = b_1b_2(B\cap H)$

   Since $H \trianglelefteq G$, ~~bh = hb~~ for every $b \in B$ and $h \in H$, there is $h' \in H$ s.t. $bh = h'b$.
   If $h \in B\cap H$, then $h' = bhb^{-1} \in B\cap H$. Therefore $b(B\cap H) = (B\cap H)b$ for all $b \in B$,
   thus $B\cap H \trianglelefteq B$. We get that $b_1b_2(B\cap H) = b_1b_2(B\cap H)(B\cap H) = b_1(B\cap H)b_2(B\cap H)$
   $= \phi(b_1H)\,\phi(b_2H)$.

3) ϕ is one-to-one: Let $b_1, b_2 \in B$. If $b_1\cdot(B\cap H) = b_2(B\cap H)$, then $b_2^{-1}b_1 \in B\cap H \le H$, hence $b_1H = b_2H$.

4) ϕ is clearly onto. $\square$

We can depict the last theorem as follows: