LECTURE 7
The homomorphism and isomorphism theorems

PAVEL RŮŽIČKA

Abstract. We prove the homomorphism theorem and the three isomorphism theorems for groups. We show that the alternating group of permutations $\boldsymbol{A_n}$ is simple for all $n \neq 4$.

7.1. **The homomorphism theorem.** We prove a theorem relating homomorphisms, kernels, and normal subgroups.

Theorem 7.1 (The homomorphism theorem)**.** *Let $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ be a group homomorphism and $\boldsymbol{N}$ a normal subgroup of $\boldsymbol{G}$. There is a homomorphism $\psi\colon \boldsymbol{G/N} \to \boldsymbol{H}$ such that $\varphi = \psi \circ \pi_{\boldsymbol{G/N}}$ if and only if $N \subseteq \ker\varphi$. The homomorphism ψ is necessarily unique.*

Moreover ψ is a group embedding if and only if $\boldsymbol{N} = \ker\varphi$.

$$\begin{tikzcd}
 & \boldsymbol{N} \arrow[d, hook, "\subseteq"] \arrow[dl, dashed, bend right, "\supseteq"'] & \\
\ker\varphi \arrow[r, hook, "\subseteq"] & \boldsymbol{G} \arrow[r, "\varphi"] \arrow[d, "\pi_{\boldsymbol{G/N}}"] & \boldsymbol{H} \\
 & \boldsymbol{G/N} \arrow[ur, dashed, bend right, "\exists!\psi"'] &
\end{tikzcd}$$

Figure 1. The homomorphism theorem

Proof. ($\Rightarrow$) Suppose that $\varphi = \psi \circ \pi_{\boldsymbol{G/N}}$ for some $\psi\colon \boldsymbol{G/N} \to \boldsymbol{H}$ and let $n \in N$. Then $\varphi(n) = \psi \circ \pi_{\boldsymbol{G/N}}(n) = \psi(N) = u_{\boldsymbol{H}}$, hence $n \in \ker\varphi$. It folows that $N \subseteq \ker\varphi$.

($\Leftarrow$) Suppose that $N \subseteq \ker\varphi$. If $f \cdot N = g \cdot N$, for some $f, g \in G$, then $g^{-1} \cdot f \in N$ due to Lemma 4.2 $(iii) \Rightarrow (i)$. Since $N \subseteq \ker\varphi$, we have that $u_{\boldsymbol{H}} = \varphi(g^{-1} \cdot f) = \varphi(g)^{-1} \cdot \varphi(f)$, hence $\varphi(g) = \varphi(f)$. Therefore we can define a map $\psi\colon G/N \to H$ by $g \cdot N \mapsto \varphi(g)$. From $\psi((f \cdot N) \cdot (g \cdot N)) = \psi(f \cdot g \cdot N) = \varphi(f \cdot g) = \varphi(f) \cdot \varphi(g) = \psi(f \cdot N) \cdot \psi(g \cdot N)$, for all $f, g \in G$, we

The Lecture and the tutorial took place in Malá strana, room S11, on November 20, 2018.

infer that $\psi\colon \boldsymbol{G/N} \to \boldsymbol{H}$ is a group homomorphism. It is straightforward that $\varphi = \psi \circ \pi_{\boldsymbol{G/N}}$ and that ψ is unique with the required properties.

Suppose that ψ is a group embedding. Let $g \in \ker \phi$. We compute that $\psi(N) = u_{\boldsymbol{H}} = \varphi(g) = \psi(\pi_{\boldsymbol{G/N}}(g)) = \psi(N \cdot g)$, hence $N = N \cdot g$, whence $g \in N$. It follows that $\ker\varphi \subseteq N$. Since $N \subseteq \ker\varphi$ due to the first part of the theorem, we conclude that $\boldsymbol{N} = \ker\varphi$.

Coversely, suppose that $\boldsymbol{N} = \ker\varphi$. Let $f, g \in G$ satisfy $\psi(f \cdot N) = \psi(g \cdot N)$. It follow that $\varphi(f) = \varphi(g)$, hence $\varphi(g^{-1} \cdot f) = \varphi(g)^{-1} \cdot \varphi(f) = u_{\boldsymbol{H}}$, whence $g^{-1} \cdot f \in \ker\varphi = N$. We get that $f \cdot N = g \cdot N$, due to Lemma 4.2. We conclude that ψ is an embedding. □

Corollary 7.2. *A group homomorphism $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ is an embedding if and only if* $\ker\varphi = \{u_{\boldsymbol{G}}\}$.

7.2. **The isomorphisms theorems.**

Theorem 7.3 (The 1st isomorphism theorem)**.** *Let $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ be a group homomorphism. Then $\varphi(\boldsymbol{G})$ is a subgroup of $\boldsymbol{H}$ isomorphic to $\boldsymbol{G}/\ker\boldsymbol{\varphi}$.*

$$\begin{tikzcd}
 & \mathbf{ker}\,\boldsymbol{\varphi} \arrow[dl, bend right, "="'] \arrow[d, hook, "\subseteq"] & \\
\mathbf{ker}\,\boldsymbol{\varphi} \arrow[r, hook, "\subseteq"] & \boldsymbol{G} \arrow[r, "\varphi"] \arrow[d, "\pi_{\boldsymbol{G}/\mathbf{ker}\,\boldsymbol{\varphi}}"] & \boldsymbol{H} \\
 & \boldsymbol{G}/\mathbf{ker}\,\boldsymbol{\varphi} \arrow[ur, hook, bend right, "\psi"'] &
\end{tikzcd}$$

FIGURE 2. The 1st isomorphism theorem

Proof. Since φ is a group homomorphism, we have that

$$\varphi(g) \cdot \varphi(h)^{-1} = \varphi(g \cdot h^{-1}) \in \varphi(G),$$

for all $g, h \in G$. Therefore $\varphi(\boldsymbol{G})$ is a subgroup of $\boldsymbol{H}$. It follow from Theorem 7.1 that there is an embedding $\psi\colon \boldsymbol{G}/\mathbf{ker}\,\boldsymbol{\varphi} \to \varphi(\boldsymbol{G})$ such that $\varphi = \psi \circ \pi_{\boldsymbol{G}/\mathbf{ker}\,\boldsymbol{\varphi}}$. Thus ψ induces an isomorphism between $\boldsymbol{G}/\mathbf{ker}\,\boldsymbol{\varphi}$ and $\varphi(\boldsymbol{G})$. □

Lemma 7.4. *Let $\boldsymbol{N}$, $\boldsymbol{K}$ be subgroups of a group $\boldsymbol{G}$.*

(i) *If $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ or $\boldsymbol{K} \trianglelefteq \boldsymbol{G}$, then $\boldsymbol{N} \cdot \boldsymbol{K}$ is a subgroup of $\boldsymbol{G}$.*

(ii) *If both $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ and $\boldsymbol{K} \trianglelefteq \boldsymbol{G}$, then $\boldsymbol{N} \cdot \boldsymbol{K}$ is a normal subgroup of $\boldsymbol{G}$.*

Proof. (i) Since $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$ or $\boldsymbol{K} \trianglelefteq \boldsymbol{G}$, the equality $N \cdot K = K \cdot N$ holds true. It follows that

$$(N \cdot K) \cdot (N \cdot K) = N \cdot N \cdot K \cdot K = N \cdot K,$$

hence $N \cdot K$ is a sub-universe of $\boldsymbol{G}$. For all $n \in N$ and $k \in K$ we have that $(n \cdot k)^{-1} = k^{-1} \cdot n^{-1} \in K \cdot N = N \cdot K$. Therefore $\boldsymbol{N} \cdot \boldsymbol{K}$ is a subgroup of $\boldsymbol{G}$.

(ii) If both $\boldsymbol{N}$ and $\boldsymbol{K}$ are normal subgroup of $\boldsymbol{G}$, then $g \cdot N \cdot K = N \cdot g \cdot K = N \cdot K \cdot g$, for all $g \in G$. It follows the subgroup $\boldsymbol{N} \cdot \boldsymbol{K}$ is normal due to Lemma 4.11. □

Observe that if at least one of subgroups $\boldsymbol{N}$ and $\boldsymbol{K}$ of a group $\boldsymbol{G}$ is normal (resp. if both the subgroups $\boldsymbol{N}$ and $\boldsymbol{K}$ are normal in $\boldsymbol{G}$), $\boldsymbol{N} \cdot \boldsymbol{K}$ is the least subgroup (resp. the least normal subgroup) of $\boldsymbol{G}$ containing both the groups $\boldsymbol{N}$ and $\boldsymbol{K}$. On the other hand the intersection $\boldsymbol{N} \cap \boldsymbol{K}$ is the largest common subgroup (resp. the largest common normal subgroup if both $\boldsymbol{N}$ and $\boldsymbol{K}$ are normal in $\boldsymbol{G}$) of $\boldsymbol{N}$ and $\boldsymbol{K}$.

Theorem 7.5 (The 2nd isomorphism theorem)**.** *Let $\boldsymbol{G}$ be a group, $\boldsymbol{H}$ a subgroup of $\boldsymbol{G}$, and $\boldsymbol{N}$ a normal subgroups of $\boldsymbol{G}$. Then*

$$(\boldsymbol{N} \cap \boldsymbol{H}) \trianglelefteq \boldsymbol{H}, \qquad \textit{and} \qquad (\boldsymbol{N} \cdot \boldsymbol{H})/\boldsymbol{N} \simeq \boldsymbol{H}/(\boldsymbol{N} \cap \boldsymbol{H}).$$

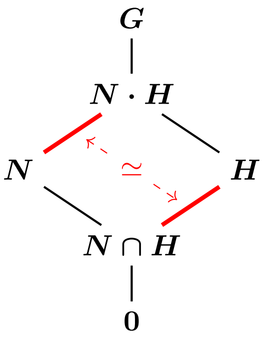
$\boldsymbol{G}$
$\boldsymbol{N} \cdot \boldsymbol{H}$
$\boldsymbol{N}$
$\simeq$
$\boldsymbol{H}$
$\boldsymbol{N} \cap \boldsymbol{H}$
$\boldsymbol{0}$

FIGURE 3. The 2nd isomorphism theorem

Proof. The product $\boldsymbol{N} \cdot \boldsymbol{H}$ is a subgroup of $\boldsymbol{G}$ due to Lemma 7.4 (i). Since $\boldsymbol{N}$ is a normal subgroup of $\boldsymbol{H}$, we have that $g \cdot N \cdot g^{-1} \subseteq N$ for all $g \in G$ (and *a fortiori* for all $h \in H$) due to Lemma 5.1. It follows that $h \cdot (N \cap H) \cdot h^{-1} \subseteq N \cap H$, for all $h \in H$. Therefore $\boldsymbol{N} \cap \boldsymbol{H}$ is a normal subgroup of $\boldsymbol{H}$. Since clearly

$$g \cdot h^{-1} \in N \cap H \text{ if and only if } g \cdot h^{-1} \in N,$$

for all $g, h \in H$, we have that

$$g \cdot (N \cap H) = h \cdot (N \cap H) \text{ if and only if } g \cdot N = h \cdot N,$$

for all $g, h \in H$. Therefore the maps

$$\begin{tikzcd}
\boldsymbol{H}/(\boldsymbol{N} \cap \boldsymbol{H}) \arrow[r, shift left] & (\boldsymbol{N} \cdot \boldsymbol{H})/\boldsymbol{N} \arrow[l, shift left] \\
h \cdot (N \cap H) \arrow[r, mapsto, shift left] & h \cdot N \arrow[l, mapsto, shift left]
\end{tikzcd}$$

are well defined. It is straightforward to verify that they are mutually inverse group isomorphisms. □

Theorem 7.6 (The 3rd isomorphism theorem)**.** *Let $\boldsymbol{G}$ be a group and $\boldsymbol{N}$, $\boldsymbol{K}$ normal subgroups of $\boldsymbol{G}$. If $K \subseteq N$, then*

$$\boldsymbol{N/K} \trianglelefteq \boldsymbol{G/K} \quad \textit{and} \quad \boldsymbol{G/N} \simeq (\boldsymbol{G/K})/(\boldsymbol{N/K}).$$

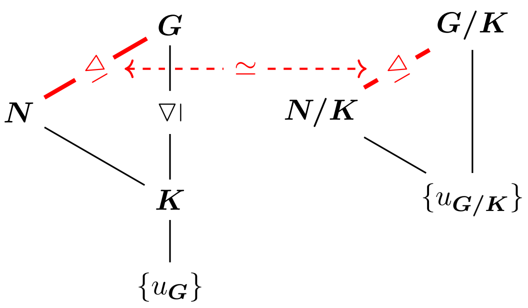

Figure 4. The 3rd isomorphism theorem

Proof. Since $\boldsymbol{K} \trianglelefteq \boldsymbol{G}$, we have that

$$(g\cdot K)\cdot(n\cdot K)\cdot(g\cdot K)^{-1} = g\cdot K\cdot n\cdot K\cdot g^{-1}\cdot K = g\cdot n\cdot g^{-1}\cdot K$$

for all $n \in N$ and $g \in G$. Since $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$, there is $n' \in N$ such that $g\cdot n\cdot g^{-1} = n'$, hence

$$(g\cdot K)\cdot(n\cdot K)\cdot(g\cdot K)^{-1} = n'\cdot K,$$

for some $n' \in N$. According to Lemma 5.1 we have that $\boldsymbol{N/K} \trianglelefteq \boldsymbol{G/K}$.

From

$$g\cdot h^{-1} \in N \text{ if and only if } g\cdot h^{-1}\cdot K \in N/K, \text{ for all } g,h \in G,$$

we infer that

$$g\cdot N = h\cdot N \text{ if and only if } (g\cdot K)\cdot N/K = (h\cdot K)\cdot N/K,$$

for all $g, h \in G$. Therefore the maps

$$\boldsymbol{G/N} \rightleftarrows (\boldsymbol{G/K})/(\boldsymbol{N/K})$$

$$g\cdot N \rightleftarrows (g\cdot K)\cdot(N/K)$$

are well defined. It is straightforward to verify that the maps are mutually inverse isomorphisms of the groups. □

7.3. **Simplicity of the alternating groups.** A (non-trivial) group has two trivial subgroups, the singleton subgroup containing only the unit element and the group itself. These two subgroups are necessarily normal and they are the only subgroups of finite groups of a prime order due to the Langrange theorem. Infinite groups and finite groups of a composite order have non-trivial subgroups. However it can still happen that they have only trivial normal subgroups. The groups whose only normal subgroups are the trivial ones are called *simple*. We prove that this is the case of the alternating groups with the only exception of $\boldsymbol{A_4}$.

Theorem 7.7. *The alternating group of permutations $\boldsymbol{A_n}$ is simple for all $n \neq 4$.*

Proof. Alternating groups $\boldsymbol{A_2}$ and $\boldsymbol{A_3}$ are of a prime order, and so they are simple. Therefore we can assume that $5 \leq n$. It follows from Lemma 5.7 that the group $\boldsymbol{A_n}$ is generated by 3-cycles. Using the assumption that $n \geq 5$, we show that

Claim 1. All 3-cycles are conjugated in $\boldsymbol{A_n}$.

Proof of Claim 1. Let $\pi = (a, b, c)$ and $\rho = (d, e, f)$ be 3-cycles (with not necessarily disjoint supports). According to formula (5.2), ρ is conjugated to π by a permutation σ satisfying $\sigma(a) = d$, $\sigma(b) = e$ and $\sigma(c) = f$. If σ is even, we are done. If σ is odd, we find g, h distinct from d, e, f and replace σ with the even permutation $\hat{\sigma} = (g, h) \cdot \sigma$. We still have that $\hat{\sigma}(a) = d$, $\hat{\sigma}(b) = e$ and $\hat{\sigma}(c) = f$, and so $\rho = {}^{\hat{\sigma}}\pi$. This is possible since $n \geq 5$. □ Claim 1.

Claim 2. Avery non-singleton normal subgroup of $\boldsymbol{A_n}$ contains a 3-cycle.

Proof of Claim 2. Let $\boldsymbol{N}$ be a non-singleton normal subgroup of the alternating group. Let us denote by π a non-unit permutation from $\boldsymbol{N}$ with $\operatorname{supp}\pi$ of the least possible size (among non-unit permutations from $\boldsymbol{N}$). We discus two complementary cases.

First suppose that in the decomposition of π into the product of independent cycles there is a cycle $(a, b, c, \dots)$ of the length at least 3. If π is a 3-cycle, we are done. It this not the case, there is $e \in \operatorname{supp}\pi$ not in $\{a, b, c\}$. Set $f := \pi(e)$ and observe that $f \notin \{b, c\}$. It follows that the permutation $\sigma = (a, e) \cdot (b, f)$ is even and $c \notin \operatorname{supp}\sigma$. We put $\rho = \pi^{-1} \cdot {}^{\sigma}\pi = \pi^{-1} \cdot \sigma \cdot \pi \cdot \sigma^{-1}$. Observe that $\operatorname{supp}\rho \subseteq \operatorname{supp}\pi$ and, since $\boldsymbol{N} \trianglelefteq \boldsymbol{A_n}$, the permutation ρ belongs to $\boldsymbol{N}$. Applying (5.2) we compute from $f = \sigma(b)$ and $c = \sigma(c)$ that

$$\rho(f) = \pi^{-1} \cdot {}^{\sigma}\pi(f) = \pi^{-1} \cdot \sigma(\pi(b)) = \pi^{-1} \cdot \sigma(c) = \pi^{-1}(c) = b.$$

Since $f \neq b$, the permutation ρ is not the unit. Next we compute that

$$\rho(a) = \pi^{-1}({}^{\sigma}\pi(a)) = \pi^{-1} \cdot \sigma \cdot \pi(e) = \pi^{-1}(b) = a,$$

hence $\operatorname{supp}\rho \subsetneq \operatorname{supp}\pi$. This contradicts the choice of π.

The remaining case is when $\pi = (a, b) \cdot (c, d) \cdots$ is a product of independent transpositions. Since $n \geq 5$, we can pick $e \notin \{a, b, c, d\}$ and put

$\sigma = (a, b) \cdot (c, e)$. As in the previous case let $\rho = \pi^{-1} \cdot {}^{\sigma}\pi$ (which here equals to $\pi \cdot {}^{\sigma}\pi$). Observe that $\operatorname{supp} \rho \subseteq \operatorname{supp} \pi \cup \{e\}$ and as above $\rho \in \boldsymbol{N}$. We easily compute that $\rho(a) = a$, $\rho(b) = b$ and $\rho(e) = \pi^{-1}(d) = c \neq e$. It follows that ρ is a non-unit permutation and $a, b \notin \operatorname{supp} \rho$. We conclude that $|\operatorname{supp} \rho| < |\operatorname{supp} \pi|$, which is a contradiction. □ Claim 2.

From Claim 1 and Claim 2 we conclude that $\boldsymbol{N}$ contains all 3-cycles. It follows that $\boldsymbol{N} = \boldsymbol{A_n}$ due to Lemma 5.7. Therefore the group $\boldsymbol{A_n}$ is simple. □

Remark 7.8. Note that all the Klein's Vierergrupe $\boldsymbol{V}$ is a non-trivial normal subgroup of $\boldsymbol{A_4}$ (cf. Example 6.9).

Exercises

Exercise 7.1. *Recall that $\boldsymbol{V}$ denotes the Klein's Vierergrupe*

$$\boldsymbol{V} = \{\upsilon_4, (1,2)\cdot(3,4), (1,3)\cdot(2,4), (1,4)\cdot(2,3)\}.$$

Prove that $\boldsymbol{S_4}/\boldsymbol{V} \simeq \boldsymbol{S}_3$.

Exercise 7.2. *Let $\mathbb{Z}$ be the group of all integers with the operation of addition. For each non-negative integer n put*

$$n \cdot \mathbb{Z} := \{n \cdot z \mid z \in \mathbb{Z}\} = \{w \in \mathbb{Z} \mid w \textit{ is divisible by } n\}.$$

Prove that the $n \cdot \mathbb{Z}$ are subgroups of $\mathbb{Z}$ and all subgroups of $\mathbb{Z}$ are of this form.

Exercise 7.3. *For a positive integer n and an integer z let $z \pmod n$ denote the reminder of z when dividing by n. Let $\mathbb{Z}_n$ denote the set $\{0, 1, \dots, n-1\}$ with the binary operation $+_n$ defined by $a +_n b = a + b \pmod n$. Prove that $\mathbb{Z}_n$ is a group isomorphic to $\mathbb{Z}/n \cdot \mathbb{Z}$.*

Exercise 7.4. *Let m, n be positive integers such that $n \mid m$. Prove that*

$$n \cdot \mathbb{Z} \Big/ m \cdot \mathbb{Z} \simeq \mathbb{Z}_{\frac{m}{n}}.$$

Exercise 7.5. *Let m, n be positive integers. Let d denote their greatest common divisor and l their least common multiple.*

(i) *Prove that*

$$n \cdot \mathbb{Z} \cap m \cdot \mathbb{Z} = l \cdot \mathbb{Z} \qquad \textit{and} \qquad n \cdot \mathbb{Z} + m \cdot \mathbb{Z} = d \cdot \mathbb{Z}$$

(ii) *Prove that*

$$n \cdot \mathbb{Z} \Big/ (m \cdot \mathbb{Z} \cap n \cdot \mathbb{Z}) \simeq (n \cdot \mathbb{Z} + m \cdot \mathbb{Z}) \Big/ m \cdot \mathbb{Z} \simeq \mathbb{Z}_{\frac{n}{d}} = \mathbb{Z}_{\frac{l}{m}}.$$