ALGEBRA I (LECTURE NOTES 2017/2018)
LECTURE 7 - HOMOMORPHISMS AND KERNELS

PAVEL RŮŽIČKA

7.1. **Group homomorphisms.** Let $\boldsymbol{G} = (G, \cdot)$ and $\boldsymbol{H} = (H, \cdot)$ be groups. A *(group) homomorphism* $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ is a map φ from the set G to H such that $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$, for all $f, g \in G$.

Lemma 7.1. *Let $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ be a group homomorphism, $u_{\boldsymbol{G}}$ and $u_{\boldsymbol{H}}$ respectively the units of $\boldsymbol{G}$ and $\boldsymbol{H}$. Then $\varphi(u_{\boldsymbol{G}}) = u_{\boldsymbol{H}}$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$, for all $g \in G$.*

Proof. We have from the definition that

$$u_{\boldsymbol{H}} \cdot \varphi(u_{\boldsymbol{G}}) = \varphi(u_{\boldsymbol{G}}) = \varphi(u_{\boldsymbol{G}} \cdot u_{\boldsymbol{G}}) = \varphi(u_{\boldsymbol{G}}) \cdot \varphi(u_{\boldsymbol{G}})$$

Since the group operation is right cancellative, we infer that $u_{\boldsymbol{H}} = \varphi(u_{\boldsymbol{G}})$. For an element $g \in G$ we have that

$$\begin{aligned}\varphi(g^{-1}) &= u_{\boldsymbol{H}} \cdot \varphi(g^{-1}) = (\varphi(g)^{-1} \cdot \varphi(g)) \cdot \varphi(g^{-1}) \\ &= \varphi(g)^{-1} \cdot (\varphi(g) \cdot \varphi(g^{-1})) = \varphi(g)^{-1} \cdot (\varphi(g \cdot g^{-1}) \\ &= \varphi(g)^{-1} \cdot \varphi(u_{\boldsymbol{G}}) = \varphi(g)^{-1} \cdot u_{\boldsymbol{H}} = \varphi(g)^{-1}.\end{aligned}$$

□

A *(group) embedding* is an one-to-one group homomorphism. We say that a group $\boldsymbol{G}$ can be *embedded* into a group $\boldsymbol{H}$ if there is a group embedding $\boldsymbol{G} \to \boldsymbol{H}$.

A *(group) isomorphism* is a group homomorphism that is both one-to-one and onto. Groups $\boldsymbol{G}$ and $\boldsymbol{H}$ are called *isomorphic* provided that there is a group isomorphism $\boldsymbol{G} \to \boldsymbol{H}$.

For each group $\boldsymbol{G}$ let us denote by $\mathbf{1}_{\boldsymbol{G}}$ the identity map $G \to G$. The map is clearly a (group) homomorphism and we will call the *identity isomorphism* of $\boldsymbol{G}$.

Lemma 7.2. *A group homomorphism $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ is an isomorphism if and if there is a group homomorphism $\psi\colon \boldsymbol{H} \to \boldsymbol{G}$ such that $\psi \circ \phi = \mathbf{1}_{\boldsymbol{G}}$ and $\phi \circ \psi = \mathbf{1}_{\boldsymbol{H}}$. That is, a group homomorphism is an isomorphism if and only if it has an inverse.*

Date: November 20, 2017.

Proof. ($\Leftarrow$) It follows from $\psi \circ \phi = \mathbf{1}_{\boldsymbol{G}}$ that ϕ is one-to-one. From $\phi \circ \psi = \mathbf{1}_{\boldsymbol{H}}$ we infer that ϕ maps G onto H. ($\Rightarrow$) Since φ is a one-to-one map from G onto H, each $h \in H$ has a unique $g \in G$ with $\varphi(g) = h$. We define $\psi(h) = g$. From $\varphi(\psi(h)) = \varphi(g) = h$ we get that $\varphi \circ \psi = \mathbf{1}_{\boldsymbol{H}}$. From the choice of $\psi(\varphi(g))$ as the unique φ-preimage $\varphi(g)$, we see that $\psi(\varphi(g)) = g$, for all $g \in G$. Therefore $\psi \circ \varphi = \mathbf{1}_{\boldsymbol{G}}$. Let f and h be arbitrary elements of H. Since φ is a homomorphism, we have that

$$\begin{aligned}\psi(f \cdot h) &= \psi((\varphi \circ \psi)(f) \cdot (\varphi \circ \psi)(h)) = \psi(\varphi(\psi(f)) \cdot \varphi(\psi(h)))) \\ &= \psi(\varphi(\psi(f) \cdot \psi(h))) = (\psi \circ \varphi)(\psi(f) \cdot \psi(h)) = \psi(f) \cdot \psi(h).\end{aligned}$$

It follows that $\psi\colon \boldsymbol{H} \to \boldsymbol{G}$ is a group homomorphism. □

We say that groups $\boldsymbol{G}$ and $\boldsymbol{H}$ are *isomorphic*, which we denote by $\boldsymbol{G} \simeq \boldsymbol{H}$, if there is an isomorphism $\boldsymbol{G} \to \boldsymbol{H}$. Observe that the inverse to an isomorphism is again an isomorphism and a composition of isomorphisms gives an isomorphism. It follows that the binary relation $\simeq$ defined on the class of all groups is symmetric and transitive. Since each group is isomorphic to itself via the identity isomorphism, $\simeq$ is an equivalence relation.

Obviously, a group isomorphism $\boldsymbol{G} \to \boldsymbol{H}$ transfers properties of the group $\boldsymbol{G}$ to properties of $\boldsymbol{H}$. Thus saying that some (group) property is unique up to isomorphism means that the property determines a group up to its isomorphism class (i.e, the block of $\simeq$).

Given a set X we denote by S_X the set of all one-to-one maps from X onto X. The set is equipped with the binary operation $\circ$ of composition of maps and thus it forms a group called the *symmetric group of the set* X and denote by $\boldsymbol{S}_X$. Clearly, for finite sets X and Y the groups $\boldsymbol{S}_X$ and $\boldsymbol{S}_Y$ are isomorphic if and only if the sets X and Y have the same size. In particular, if X is an n-element set, then $\boldsymbol{S}_X \simeq \boldsymbol{S}_{\boldsymbol{n}}$.

Theorem 7.3 (Cayley)**.** *Every group can be embedded into a symmetric group of its underlying set.*

Proof. Let $\boldsymbol{G} = (G, \cdot)$ be a group. For each $f, g \in G$ we set $\lambda(f)(g) = f \cdot g$. Thus we have defined a map $\lambda(f)\colon G \to G$ for all $f \in G$. From the left cancellativity of the group operation it follows that $\lambda(f)(g) \neq \lambda(f)(h)$ whenever $g \neq h$, hence the mat $\lambda(f)$ is one-to-one. The left divisibility of the group operation implies that $\lambda(f)$ maps G onto G. Therefore λ can be regarded as a map from G to S_G. Since

$$\lambda(f \cdot g)(h) = (f \cdot g) \cdot h = f \cdot (g \cdot h) = \lambda(f)(\lambda(g)(h)) = (\lambda(f) \circ \lambda(g))(h),$$

for all $f, g, h \in G$, and so $\lambda(f \cdot g) = \lambda(f) \circ \lambda(g)$, the map is a group homomorphism $\lambda\colon \boldsymbol{G} \to \boldsymbol{S}_G$. Let u denote the unit of $\boldsymbol{G}$. If $f \neq g$ in

G, then

$$\lambda(f)(u) = f \cdot u = f \neq g = g \cdot u = \lambda(g)(u), \tag{7.1}$$

in particular $\lambda(f) \neq \lambda(g)$. We conclude that λ is a group embedding. □

Corollary 7.4. *A finite group embeds into $\boldsymbol{S_n}$, where n is the size of the group.*

Remark 7.5. The map $\lambda\colon \boldsymbol{G} \to \boldsymbol{S}_G$ is called a *left translation* in $\boldsymbol{G}$. Similarly we can define a *right translation*, say ρ, by $\rho(f)(g) = g \cdot f^{-1}$ (we need the inverse of f to make ρ an homomorphism) and prove that it induces another embedding $\rho\colon \boldsymbol{G} \to \boldsymbol{S}_G$. Observe that in the proof of Theorem 7.3 we only needed the left cancellativity, the left divisibility, and the existence of a right unit (respectively the right cancellativity, the right divisibility, and the existence of a left unit if we argue using ρ instead of λ). This gives an elegant solution of Exercies 2.4.

7.2. Kernels of group homomorphisms.

Definition 7.6. Let $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ be a group homomorphism. A *kernel* of the homomorphism φ is the set

$$\ker \varphi := \{g \in G \mid \varphi(g) = u_{\boldsymbol{H}}\},$$

where $u_{\boldsymbol{H}}$ denotes the unit of $\boldsymbol{H}$.

Observe that the kernel of a homomorphism contains the unit of $\boldsymbol{G}$, and so it is non-empty. Much more holds true:

Lemma 7.7. *The kernel of a group homomorphism $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ is a normal subgroup of $\boldsymbol{G}$.*

Proof. If $g, h \in \ker\varphi$, then

$$\varphi(g \cdot h^{-1}) = \varphi(g) \cdot \varphi(h)^{-1} = u_{\boldsymbol{H}} \cdot u_{\boldsymbol{H}}^{-1} = u_{\boldsymbol{H}},$$

and so $g \cdot h^{-1} \in \ker\varphi$. Therefore $\ker\varphi$ is a subgroup of $\boldsymbol{G}$.

Let $k \in \ker\varphi$ and $g \in G$. Then

$$\varphi(g \cdot k \cdot g^{-1}) = \varphi(g) \cdot \varphi(k) \cdot \varphi(g^{-1}) = \varphi(g) \cdot u_{\boldsymbol{H}} \cdot \varphi(g)^{-1} = u_{\boldsymbol{H}}.$$

Therefore $g \cdot k \cdot g^{-1} \in \ker\varphi$, and so the subgroup $\ker\varphi$ is normal due to Lemma 6.8. □

Let $\boldsymbol{N}$ be a normal subgroup of a group $\boldsymbol{G}$. The map $\pi_{\boldsymbol{G}/\boldsymbol{N}}\colon \boldsymbol{G} \to \boldsymbol{G}/\boldsymbol{N}$ defined by $g \mapsto N \cdot g = g \cdot N$ is a group homomorphism[1], indeed

$$\pi_{\boldsymbol{G}/\boldsymbol{N}}(g \cdot h^{-1}) = N \cdot g \cdot h^{-1} = N \cdot g \cdot N \cdot h^{-1} = (N \cdot g) \cdot (N \cdot h)^{-1},$$

[1] Note that since $\boldsymbol{N} \trianglelefteq \boldsymbol{G}$, we have that $N \cdot g = g \cdot N$, for all $g \in G$.

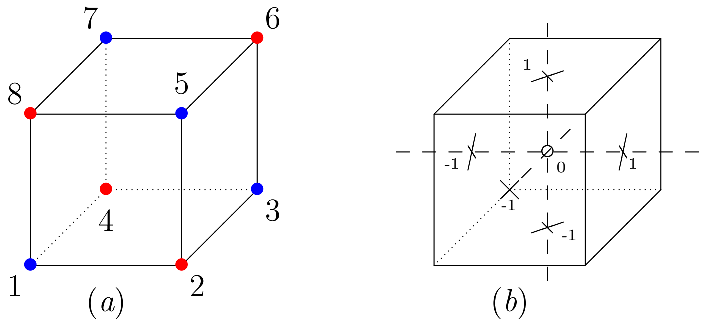
for all $g, h \in G$. By the definition,

$$\ker \pi_{\boldsymbol{G/N}} = \{g \in G \mid \pi_{\boldsymbol{G/N}} = N\} = \{g \in G \mid N \cdot g = N\} = N.$$

Therefore

Corollary 7.8. *Normal subgroups correspond to kernels of group homomorphisms.*

Example 7.9. *Similarly as in Example 6.11 let $\boldsymbol{R}$ denote the group of all symmetries of a cube. We showed that $\boldsymbol{R}$ is isomorphic to the group of permutations $\boldsymbol{S_4}$. The numbering vertices of the cube as in Figure 1 induces an embedding $\alpha\colon \boldsymbol{R} \to \boldsymbol{S_8}$. Similar numbering of edges or faces of the cube respectively induces embeddings $\beta\colon \boldsymbol{R} \to \boldsymbol{S_{12}}$ or $\gamma\colon \boldsymbol{R} \to \boldsymbol{S_6}$.*



(a) (b)

Figure 1. The cube

Color vertices of the cube blue and red as in Figure 1 (a). Observe that each rotation of the cube either leaves or changes the color of all vertices. Thus the coloring induces a homomorphism $\delta\colon \boldsymbol{R} \to \boldsymbol{S_2}$ from $\boldsymbol{R}$ onto $\boldsymbol{S_2}$. Note that the kernel of the homomorphism corresponds to the subgroup of all even permutations of the four diagonals of the cube.

We can number (and color) the faces of the cube by $\{1, 2, 3\}$ so that the opposite faces have the same number (color) as in Figure 2. This induces a homomorphism $\varepsilon\colon \boldsymbol{R} \to \boldsymbol{S_3}$ from $\boldsymbol{R}$ onto $\boldsymbol{S_3}$.

We can insert the cube into the 3-dimensional real real vector space so that the center of the cube correspond do the zero vector and the centers of faces of the cube to the vectors of the canonical basis of $\mathbb{R}^3$ and their inverses, as in Figure 1 (b). We can view the rotations of the cube as restrictions of one-to-one linear maps $\mathbb{R}^3 \to \mathbb{R}^3$. The matrices of these linear maps with respect to the canonical basis have one non-zero entry in each line and each column, the non-zero entries are 1 or -1, and the determinants of these matrices all equal to 1. On the other

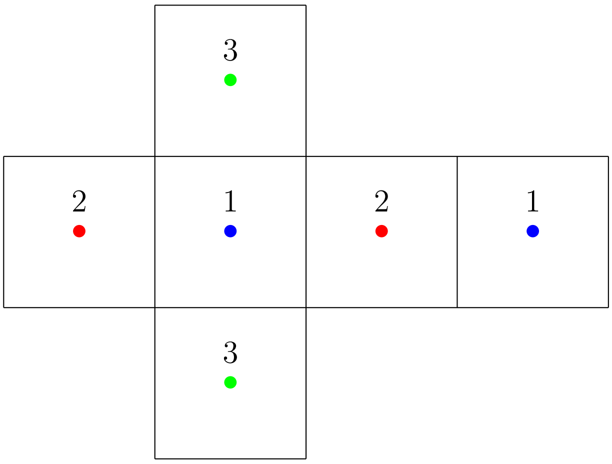


FIGURE 2. The surface of the cube

hand every such matrix correspond to some rotation of the cube. In particular, we have an embedding $\phi\colon \boldsymbol{R} \to \mathrm{GL}(3,\mathbb{R})$.

Consider all matrices from $\mathrm{GL}(3,\mathbb{R})$ *that have one non-zero entry in each line and each column and the non-zero entries are* 1 *or* -1*. There are* 48 *of them and they form a group (together with the matrix multiplication). The matrices correspond to linear maps* $\mathbb{R}^3 \to \mathbb{R}^3$ *whose restriction to the cube map bijectively vertices to vertices, edges to edges, and faces to faces. These are called* symmetries *of the cube. The* 48*-element group of all symmetries of the cube will be denoted by* $\boldsymbol{S}$*. The symmetries that are not rotations are called* reflections*. Unlike rotations, reflections cannot be realized with a real cube in our* 3*-dimensional world. However we could have realized them if we had lived in a four-dimensional world.*

Exercise 7.1. *Let* $\alpha\colon \boldsymbol{R} \to \boldsymbol{S_8}$, $\beta\colon \boldsymbol{R} \to \boldsymbol{S_{12}}$, $\gamma\colon \boldsymbol{R} \to \boldsymbol{S_6}$, *be as in Example 7.9.*

(i) *Prove that* $\alpha(\boldsymbol{R}) \subseteq \boldsymbol{A_8}$.
(ii) *Decide whether* $\beta(\boldsymbol{R}) \subseteq \boldsymbol{A_{12}}$, $\gamma(\boldsymbol{R}) \subseteq \boldsymbol{A_6}$.

Exercise 7.2. *Let* $\delta\colon \boldsymbol{R} \to \boldsymbol{S_2}$ *and* $\varepsilon\colon \boldsymbol{R} \to \boldsymbol{S_3}$ *be as in Example 7.9.*

(i) *Find kernels of the group homomorphisms* δ *and* ε.
(ii) *Show that* $\varepsilon(\boldsymbol{R}) = \boldsymbol{S_3}$.

Exercise 7.3. *Describe all conjugacy classes of the group* $\boldsymbol{S}$ *of all symmetries of a cube. Compute characteristic polynomials and Jordan canonical forms of corresponding matrices.*

Exercise 7.4. *Analyze the group of all rotations and the group of all symmetries of*

(i) *a square.*
(ii) *a regular tetrahedron.*

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

Theorem 7.10 (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 $\psi\colon \boldsymbol{G}/\boldsymbol{N} \to \boldsymbol{H}$ such that $\varphi = \psi \circ \pi_{\boldsymbol{G}/\boldsymbol{N}}$ if and only if $N \subseteq \ker\varphi$. The homomorphism ψ is necessarily unique.*

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

$$\begin{tikzcd}
\ker\varphi \arrow[dr, hook, "\subseteq"] & & \\
\boldsymbol{N} \arrow[u, dotted, "\subseteq"] \arrow[r, hook, "\subseteq"'] & \boldsymbol{G} \arrow[r, "\pi_{\boldsymbol{G}/\boldsymbol{N}}"] \arrow[dr, "\varphi"'] & \boldsymbol{G}/\boldsymbol{N} \arrow[d, dotted, "\exists\,\psi"] \\
& & \boldsymbol{H}
\end{tikzcd}$$

FIGURE 3. The homomorphism theorem

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

($\Leftarrow$) 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 5.2 (*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 $\varphi(g) = \varphi(f)$. It follows that we can define a map $\psi\colon G/N \to H$ by $g \cdot N \mapsto \varphi(g)$. Clearly $\psi((f \cdot N) \cdot (g \cdot N)) = \psi(f \cdot g \cdot N) = \varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$, for all $f, g \in G$, thus $\psi\colon \boldsymbol{G}/\boldsymbol{N} \to \boldsymbol{H}$ is a group homomorphism. It is straightforward that $\varphi = \psi \circ \pi_{\boldsymbol{G}/\boldsymbol{N}}$ and that ψ is unique with the required properties.

Suppose that ψ is a group embedding. Let $g \in \ker\phi$. We compute that $\psi(N) = u_{\boldsymbol{H}} = \varphi(g) = \psi(\pi_{\boldsymbol{G}/\boldsymbol{N}}(g)) = \psi(N \cdot g)$, 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 Corollary 5.3. We conclude that ψ is an embedding. □

Corollary 7.11. *A group homomorphism* $\varphi\colon \boldsymbol{G} \to \boldsymbol{H}$ *is an embedding if and only if* $\ker\varphi = \{u_{\boldsymbol{G}}\}$.