

## LECTURE 6

### Group homomorphisms and their kernels

PAVEL RŮŽIČKA

ABSTRACT. We define and study the notions of a group homomorphism and the kernel of a group homomorphism. We prove that the kernels correspond to normal subgroups. We examine some examples of group homomorphisms that are based on geometric intuition.

---

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

**Lemma 6.1.** *Let  $\varphi: \mathbf{G} \rightarrow \mathbf{H}$  be a group homomorphism,  $u_{\mathbf{G}}$  and  $u_{\mathbf{H}}$  respectively the units of  $\mathbf{G}$  and  $\mathbf{H}$ . Then  $\varphi(u_{\mathbf{G}}) = u_{\mathbf{H}}$  and  $\varphi(g^{-1}) = \varphi(g)^{-1}$ , for all  $g \in G$ .*

*Proof.* We have from the definition that

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

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

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

Since  $\mathbf{H}$  is left-cancellative we infer that  $\varphi(g^{-1}) = \varphi(g)^{-1}$ . □

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

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

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

**Lemma 6.2.** *A group homomorphism  $\varphi: \mathbf{G} \rightarrow \mathbf{H}$  is an isomorphism if and if there is a group homomorphism  $\psi: \mathbf{H} \rightarrow \mathbf{G}$  such that  $\psi \circ \varphi = \mathbf{1}_{\mathbf{G}}$  and*

---

The Lecture and the tutorial took place in Malá strana, room S11, on November 13, 2018.

$\phi \circ \psi = \mathbf{1}_H$ . That is, a group homomorphism is an isomorphism if and only if it has an inverse.

*Proof.* ( $\Leftarrow$ ) It follows from  $\psi \circ \phi = \mathbf{1}_G$  that  $\phi$  is one-to-one. From  $\phi \circ \psi = \mathbf{1}_H$  we infer that  $\phi$  maps  $G$  onto  $H$ . ( $\Rightarrow$ ) Since  $\varphi$  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  $\varphi \circ \psi = \mathbf{1}_H$ . From the choice of  $\psi(\varphi(g))$  as the unique  $\varphi$ -preimage  $\varphi(g)$ , we see that  $\psi(\varphi(g)) = g$ , for all  $g \in G$ . Therefore  $\psi \circ \varphi = \mathbf{1}_G$ . Let  $f$  and  $h$  be arbitrary elements of  $H$ . Since  $\varphi$  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  $\psi: H \rightarrow G$  is a group homomorphism.  $\square$

We say that groups  $G$  and  $H$  are *isomorphic*, which we denote by  $G \simeq H$ , if there is an isomorphism  $G \rightarrow H$ . 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  $G \rightarrow H$  transfers properties of the group  $G$  to properties of  $H$ . 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  $\mathbf{S}_X$ . Clearly, for finite sets  $X$  and  $Y$  the groups  $\mathbf{S}_X$  and  $\mathbf{S}_Y$  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  $\mathbf{S}_X \simeq \mathbf{S}_n$ .

**Theorem 6.3** (Cayley). *Every group can be embedded into a symmetric group of its underlying set.*

*Proof.* Let  $G = (G, \cdot)$  be a group. For each  $f, g \in G$  we set  $\lambda(f)(g) = f \cdot g$ . Thus we have defined a map  $\lambda(f): G \rightarrow G$  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 map  $\lambda(f)$  is one-to-one. The left divisibility of the group operation implies that  $\lambda(f)$  maps  $G$  onto  $G$ . Therefore  $\lambda$  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  $\lambda: G \rightarrow S_G$ . Let  $u$  denote the unit of  $G$ . If  $f \neq g$  in  $G$ , then

$$(6.1) \quad \lambda(f)(u) = f \cdot u = f \neq g = g \cdot u = \lambda(g)(u),$$

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

**Corollary 6.4.** *A finite group embeds into  $S_n$ , where  $n$  is the size of the group.*

**Remark 6.5.** The map  $\lambda: G \rightarrow S_G$  is called a *left translation* in  $G$ . Similarly we can define a *right translation*, say  $\rho$ , by  $\rho(f)(g) = g \cdot f^{-1}$  (we need the inverse of  $f$  to make  $\rho$  an homomorphism) and prove that it induces another embedding  $\rho: G \rightarrow S_G$ . Observe that in the proof of Theorem 6.3 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  $\rho$  instead of  $\lambda$ ). This leads to an elegant solution of Exercices 2.4.

**Lemma 6.6.** *Let  $\varphi: G \rightarrow H$  be a group homomorphism. The following hold true:*

(a) *Let  $K$  be a subgroup of the group  $G$ . Then*

$$\varphi(K) := \{\varphi(k) \mid k \in K\}$$

*is the universe of a subgroup of  $H$ . Moreover if  $\varphi$  is an epimorphism and the subgroup  $K$  is normal in  $G$ , the image  $\varphi(K)$  is a normal subgroup of  $H$ .*

(b) *Let  $L$  be a subgroup of the group  $H$ . Then*

$$\varphi^{-1}(L) := \{g \in G \mid \varphi(g) \in L\}$$

*is a universe of a subgroup of  $G$ . Moreover if  $L$  is a normal subgroup of the group  $H$ , then  $\varphi^{-1}(L)$  is a normal subgroup of  $G$ .*

*Proof.* We prove the two parts (a) and (b) separately.

(a) Let  $g, h \in \varphi(K)$ . There are  $k, l \in K$  such that  $g = \varphi(k)$  and  $h = \varphi(l)$ . Computing that  $g \cdot h^{-1} = \varphi(k \cdot l^{-1}) \in \varphi(K)$ , we prove that  $\varphi(K)$  is the universe of a subgroup of  $H$ .

Suppose that  $K$  is a normal subgroup of  $G$  and that  $\varphi$  is an epimorphism. Then for every  $h \in H$  there is  $g \in G$  with  $\varphi(g) = h$ . Applying the normality of  $K$  in  $G$  we get that

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

for all  $k \in K$ . Therefore  $\varphi(K) \trianglelefteq H$ .

(b) Let  $g, h \in \varphi^{-1}(L)$ . From

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

we infer that  $g \cdot h^{-1} \in \varphi^{-1}(L)$ , hence  $\varphi^{-1}(L)$  is a subgroup of the group  $G$ .

Suppose that  $L$  is a normal subgroup of  $H$ . Let  $k \in \varphi^{-1}(L)$  and  $g \in G$ . We compute that

$$\varphi(g \cdot k \cdot g^{-1}) = \varphi(g) \cdot \varphi(k) \cdot \varphi(g)^{-1} \in \varphi(g) \cdot L \cdot \varphi(g)^{-1} \subseteq L,$$

since  $L \trianglelefteq H$ . We conclude that  $\varphi^{-1}(L)$  is a normal subgroup of  $G$ . □

**Lemma 6.7.** *lemma:podgrupy homomorfismus* Let  $\varphi: G \rightarrow H$  be a group homomorphism. The mapping  $K \mapsto \varphi(K)$  is a bijection between the set of all subgroups  $K$  of  $G$  such that  $\ker \varphi \subseteq K$  and the set of all subgroups of  $\varphi(G)$ .

*Proof.* Observe that  $K \subseteq \varphi^{-1}(\varphi(K))$  for every subset  $K \subseteq G$ . Let  $K$  be a subgroup containing  $\ker \varphi$ . Let  $g \in \varphi^{-1}(\varphi(K))$ . Then  $\varphi(g) \in \varphi(K)$ , and so there is  $k \in K$  such that  $\varphi(g) = \varphi(k)$ . It follows that  $\varphi(k^{-1} \cdot g) = u_H$ , hence  $k^{-1} \cdot g \in \ker \varphi$ , hence  $g \in k \cdot \ker \varphi$ . Since  $k \in K$  and  $\ker \varphi \subseteq K$ , we conclude that  $g \in K$ . Therefore  $K = \varphi^{-1}(\varphi(K))$ .

Clearly  $\varphi(\varphi^{-1}(L)) = L$  for every  $L \subseteq \varphi(G)$ . According to Lemma 6.6 the maps

$$K \mapsto \varphi(K) \quad \text{and} \quad L \mapsto \varphi^{-1}(L)$$

are mutually inverse bijections between the set of all subgroups of  $G$  containing  $\ker \varphi$  and the set of all subgroups of  $\varphi(G)$ . □

## 6.2. Kernels of group homomorphisms.

**Definition 6.8.** Let  $\varphi: G \rightarrow H$  be a group homomorphism. A *kernel* of the homomorphism  $\varphi$  is the set

$$\ker \varphi := \{g \in G \mid \varphi(g) = u_H\},$$

where  $u_H$  denotes the unit of  $H$ .

Observe that the kernel of a homomorphism contains the unit of  $G$ , and so it is non-empty. However, even more holds true:

**Lemma 6.9.** *The kernel of a group homomorphism  $\varphi: G \rightarrow H$  is a normal subgroup of  $G$ .*

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

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

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

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

$$\varphi(g \cdot k \cdot g^{-1}) = \varphi(g) \cdot \varphi(k) \cdot \varphi(g^{-1}) = \varphi(g) \cdot u_H \cdot \varphi(g)^{-1} = u_H.$$

Therefore  $g \cdot k \cdot g^{-1} \in \ker \varphi$ , and so the subgroup  $\ker \varphi$  is normal due to Lemma 5.1. □

Let  $N$  be a normal subgroup of a group  $G$ . The map  $\pi_{G/N}: G \rightarrow G/N$  defined by  $g \mapsto N \cdot g = g \cdot N$  is a group homomorphism<sup>1</sup>, indeed

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

<sup>1</sup>Note that since  $N \trianglelefteq G$ , we have that  $N \cdot g = g \cdot N$ , for all  $g \in G$ .

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

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

Therefore

**Corollary 6.10.** *Normal subgroups correspond to kernels of group homomorphisms.*

**Example 6.11.** *As in Example 5.6 let  $\mathbf{R}$  denote the group of all rotations of a cube. We showed that  $\mathbf{R}$  is isomorphic to the group of permutations  $\mathbf{S}_4$ . A numbering of vertices of the cube induces an embedding  $\alpha: \mathbf{R} \rightarrow \mathbf{S}_8$ . Similarly a numbering of edges and a numbering of faces of the cube induce embeddings  $\beta: \mathbf{R} \rightarrow \mathbf{S}_{12}$  and  $\gamma: \mathbf{R} \rightarrow \mathbf{S}_6$ , respectively.*

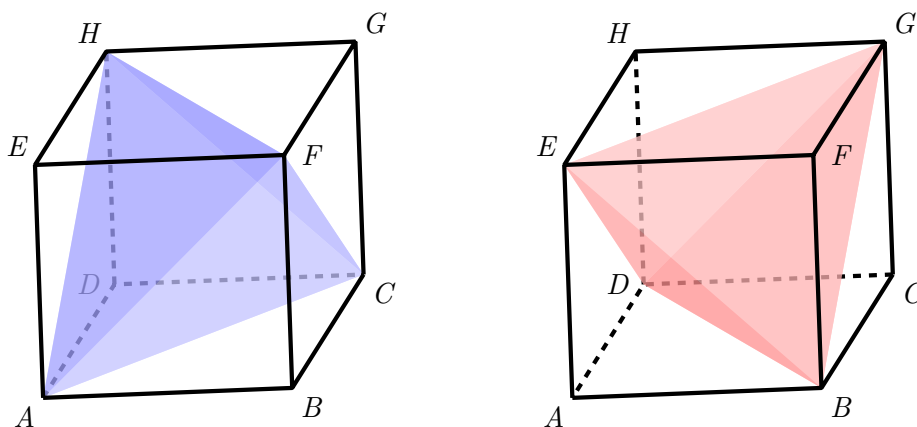


FIGURE 1. Cubes with tetrahedrons

Observe that we can inscribe two regular tetrahedrons into the cube as in Figure 1. Each rotation either maps each of the tetrahedrons onto itself or exchange them. This induces a homomorphism from  $\mathbf{R}$  to the two-element group of permutations of the two tetrahedrons. Up to an isomorphism, this map corresponds to a homomorphism  $\mathbf{S}_4 \rightarrow \mathbf{S}_2$ . The kernel of this homomorphism consists of the rotations mapping each of the tetrahedrons onto itself. On one hand, if we restrict to one of the tetrahedrons, say the blue one  $ACFH$ , these are exactly the rotations of the tetrahedron. On the other hand these are exactly the rotations of the cube corresponding to even permutations of its diagonals. We conclude that the kernel of this homomorphism is isomorphic to the alternating group of permutations  $\mathbf{A}_4$ .

Color axes of faces of the cube as in Figure 2. Each rotation of the cube induces a permutation of these axes. Since a rotation over one of them induces a transposition of the remaining two, each permutation of the axes is induced by a rotation of the cube. Thus we get a homomorphism from the group  $\mathbf{R}$  onto the group of all permutations of the three-element set of the axes, up to an isomorphism, corresponding to an epimorphism  $\mathbf{S}_4 \rightarrow \mathbf{S}_3$ .

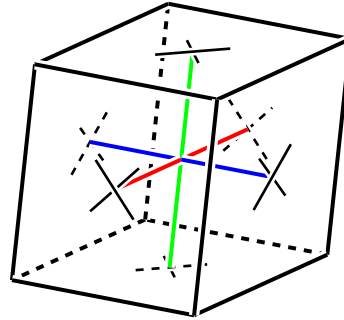


FIGURE 2. Axis of faces of the cube

The kernel of the homomorphism consists of the rotations that map all three axes onto themselves. These are the identity rotation and the flips over the axes. Each of the flips exchange two pairs of diagonals of the cube. Therefore the flips correspond to permutations of the type  $(0, 2, 0, 0)$ . It follows that the kernel of the corresponding homomorphism  $\mathbf{S}_4 \rightarrow \mathbf{S}_3$  is the four-element group<sup>2</sup>  $\mathbf{V} = \{v_4, (1, 2) \cdot (3, 4), (1, 3) \cdot (2, 4), (1, 4) \cdot (2, 3)\}$ . The group  $\mathbf{V}$  is indeed a normal subgroup of  $\mathbf{S}_4$ . Let us note that  $\mathbf{V}$  is the only non-trivial normal subgroup of  $\mathbf{A}_4$  and  $\mathbf{V}$  and  $\mathbf{A}_4$  are only non-trivial normal subgroups of  $\mathbf{S}_4$ .

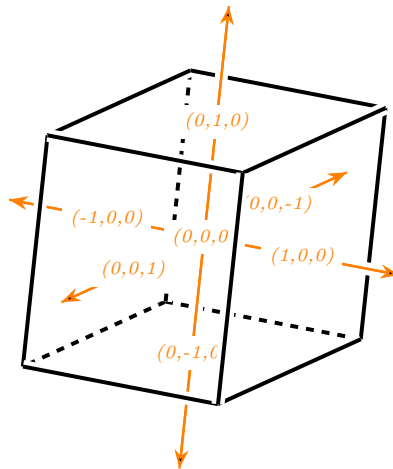


FIGURE 3. The cube in a coordinate system

Finally, let us insert the cube into the 3-dimensional real vector space so that the center of the cube corresponds to the zero vector and the centers of faces to the vectors of a canonical basis of  $\mathbb{R}^3$  and their inverses, as depicted

<sup>2</sup>The group in question was named *Vierergruppe* (= four-group) by Felix Klein. That is why it is often denoted by  $\mathbf{V}$ .

in Figure 3. We can view the rotations of the cube as restrictions of one-to-one linear maps  $\mathbb{R}^3 \rightarrow \mathbb{R}^3$ . The matrices of these linear maps with respect to the canonical basis have one non-zero entry in each line and each column and the non-zero entries are 1 or -1. Moreover the determinant of each of these matrices is equal to 1. On the other hand every matrix with the properties corresponds to some rotation of the cube. In this way we have defined an embedding  $\mathbf{R} \rightarrow \text{GL}(3, \mathbb{R})$ .

There are 48 matrices in  $\text{GL}(3, \mathbb{R})$  that have one non-zero entry in each line and each column and the non-zero entries are 1 or -1 and these matrices form a group (with an operation of the matrix multiplication). They matrices correspond to linear maps  $\mathbb{R}^3 \rightarrow \mathbb{R}^3$  whose restriction to the cube map bijectively vertices to vertices and edges to edges. Let us call such maps **symmetries** of the cube and let us denote by  $\mathbf{S}$  the 48-element group they form. Associating to each symmetry its matrix with respect to a canonical basis of  $\mathbb{R}^3$ , we extend the embedding  $\mathbf{R} \rightarrow \text{GL}(3, \mathbb{R})$  above to an embedding  $\mu: \mathbf{S} \rightarrow \text{GL}(3, \mathbb{R})$ .

Observe that all non-zero real numbers with the operation of multiplication form a group. We denote the group by  $(\mathbb{R}^*, \cdot)$ . The subset  $\{1, -1\}$  is a universe of a two-element subgroup, say  $\mathbf{C}_2$ , of  $(\mathbb{R}^*, \cdot)$ . The multiplication table of the group  $\mathbf{C}_2$  is

$\cdot$	<b>1</b>	<b>-1</b>
<b>1</b>	1	-1
<b>-1</b>	-1	1

Since the determinant of a product of square matrices is a product of their determinants, the map  $\det: \text{GL}(3, \mathbb{R}) \rightarrow (\mathbb{R}^*, \cdot)$  that assigns to a regular matrix its non-zero determinant is a group homomorphism. Let us denote  $\delta := \det \circ \mu$ . Note that the image of  $\delta$  is the subgroup  $\mathbf{C}_2$  of  $(\mathbb{R}^*, \cdot)$ , and so we have a group epimorphism  $\delta: \mathbf{S} \rightarrow \mathbf{C}_2$ . We can sketch the situation as follows:

$$\begin{array}{ccc} \mathbf{S} & \xrightarrow{\mu} & \text{GL}(3, \mathbb{R}) \\ \delta \downarrow & & \downarrow \det \\ \mathbf{C}_2 & \subseteq & (\mathbb{R}^*, \cdot). \end{array}$$

The matrices in the image of  $\mu$  corresponding to rotations are exactly those with determinant equal to 1. We conclude that  $\mathbf{R}$  is the kernel of  $\delta$ . This corresponds to  $\mathbf{R}$  being a normal subgroup of  $\mathbf{S}$ , which follow also from  $[\mathbf{S} : \mathbf{R}] = 2$  (cf. Exercise 4.3). Finally let us note that symmetries that are not rotations are called **reflections**. They form a coset of  $\mathbf{R}$  in  $\mathbf{S}$  and the determinants of matrices corresponding to reflections are all equal to  $-1$ .

## EXERCISES

**Exercise 6.1.** *Decide whether all 3-cycles are conjugated in  $A_4$ .*

**Exercise 6.2.** *Let  $\alpha: \mathbf{R} \rightarrow \mathbf{S}_8$ ,  $\beta: \mathbf{R} \rightarrow \mathbf{S}_{12}$ ,  $\gamma: \mathbf{R} \rightarrow \mathbf{S}_6$ , be as in Example 6.11.*

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

**Exercise 6.3.** *Let  $\delta: \mathbf{R} \rightarrow \mathbf{S}_2$  and  $\varepsilon: \mathbf{R} \rightarrow \mathbf{S}_3$  be as in Example 6.11.*

- (i) *Find kernels of the group homomorphisms  $\delta$  and  $\varepsilon$ .*
- (ii) *Show that  $\varepsilon(\mathbf{R}) = \mathbf{S}_3$ .*

**Exercise 6.4.** *Describe all conjugacy classes of the group  $\mathbf{S}$  of all symmetries of a cube. Compute characteristic polynomials and Jordan canonical forms of corresponding matrices.*

**Exercise 6.5.** *Analyze the group of all rotations and the group of all symmetries of*

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

**Exercise 6.6.** *Let  $G$  be a group. Let us define a map  $\gamma: G \rightarrow S_G$  by  $g \mapsto [h \mapsto {}^g h = g \cdot h \cdot g^{-1}]$ .*

- *Prove that  $\gamma(g)$  is a permutation of  $G$  for every  $g \in G$ .*
- *Prove that  $\gamma: \mathbf{G} \rightarrow \mathbf{S}_G$  is a group homomorphism.*
- *Prove that  $\ker \gamma = \mathbf{Z}(\mathbf{G})$ ; the centrum of the group  $\mathbf{G}$ .*