Homomorphisms and factor groups

Abdennour Kitouni, Anatoliy Malyarenko and Sergei Silvestrov

November 24, 2015

Abstract

Contents of the lecture.

- ☞ Homomorphisms.
- ☞ Factor groups.
- ☞ Factor group computations and simple groups.

Homomorphisms

An important problem is determining whether two given groups G and H are somehow the same.

Definition 1. If $(G,*)$ and $(H,\circ)$ are groups, then a function $\varphi\colon G\mapsto H$ is a **homomorphism** if

$$\varphi(x*y)=\varphi(x)\circ\varphi(y)$$

for all x,$y\in G$.

The word *homomorphism* comes from the Greek *homo* meaning “same" and *morph* meaning “shape" or “form". Thus, a homomorphism carries a group to another group (its image) of similar form.

Examples of homomorphisms

Example 1. Let G be an abelian group. The map $x\mapsto x^{-1}$ of G into itself is a homomorphism. In additive notation, this map looks like $x\mapsto -x$. The verification that it has the property defining a homomorphism is immediate.

Example 2. The map $z\mapsto|z|$ is a homomorphism of the group $\mathbb{C}^*$ into $\mathbb{R}^+$.

Example 3. The map $x \mapsto e^x$ is a homomorphism of the group $(\mathbb{R}, +)$ into the group $(\mathbb{R}^+, \cdot)$. Its inverse map, the logarithm, is also a homomorphism.

Example 4. Recall that a linear transformation $T\colon \mathbb{R}^n \mapsto \mathbb{R}^n$ has the property that $T(a+b) = T(a)+T(b)$. Thus T is a group homomorphism from the additive group $\mathbb{R}^n$ to itself. More concretely, for any n-by-n matrix M, we have $M(a+b) = Ma+Mb$. Thus multiplication by M is a group homomorphism from the additive group $\mathbb{R}^n$ to itself.

Properties of homomorphisms

Theorem 1. *Let $\varphi\colon G \mapsto H$ be a homomorphism of groups.*

- ☞ $\varphi(1) = 1$.
- ☞ $\varphi(x^{-1}) = \varphi(x)^{-1}$.
- ☞ $\varphi(x^n) = \varphi(x)^n$ *for all* $n \in \mathbb{Z}$.

Proof.
- ☞ $1 \cdot 1 = 1$ implies $\varphi(1)\varphi(1) = \varphi(1)$.
- ☞ $1 = xx^{-1}$ implies $1 = \varphi(1) = \varphi(x)\varphi(x)^{-1}$.
- ☞ Use induction to show that $\varphi(x^n) = \varphi(x)^n$ for all $n \geq 0$. Then observe that $x^{-n} = (x^{-1})^n$, and use part 2.

□

Kernels and images

Definition 2. If $\varphi\colon G \mapsto H$ is a homomorphism, define the **kernel** of φ as

$$\mathrm{Ker}(\varphi) = \varphi^{-1}(\{1\}),$$

and the **image** of φ as

$$\mathrm{Im}(\varphi) = \varphi[G].$$

Kernel comes from the German word meaning “grain" or “seed" (*corn* comes from the same word).

Example 5. A map that maps any even permutation in S_n to 1 and any odd permutation to -1 is homomorphism of S_n to the multiplicative group $\{\pm 1\}$. Its kernel is the alternating group A_n.

Example 6. Determinant is an onto homomorphism of the group $GL(n,\mathbb{R})$ of invertible $n \times n$ matrices to the multiplicative group of nonzero real numbers $\mathbb{R}^\times$, whose kernel is the special linear group $SL(n,\mathbb{R})$ of all $n \times n$ matrices of determinant 1.

An important property of a kernel

Theorem 2. *Let $\varphi\colon G \mapsto G'$ be a homomorphism of groups with kernel H. Let $a \in G'$, and let $X = \varphi^{-1}(\{a\})$. Then, for any $u \in X$,*

$$X = uH = Hu.$$

In other words, the partitions of G into left cosets and into right cosets of H is the same.

Proof. Let $u \in X$ so by definition of X, $\varphi(u) = a$. We first prove $uH \subseteq X$. For any $h \in H$,

$$\begin{aligned} \varphi(uh) &= \varphi(u)\varphi(h) && \text{since } \varphi \text{ is a homomorphism} \\ &= \varphi(u)1 && \text{since } h \in \ker(\varphi) \\ &= a, \end{aligned}$$

that is, $uh \in X$. This proves $uH \subseteq X$. To establish the reverse inclusion suppose $g \in X$ and let $h = u^{-1}g$. Then

$$\varphi(h) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = 1.$$

Thus $h \in \mathrm{Ker}(\varphi)$. Since $h = u^{-1}g$, $g = uh \in uH$, establishing the inclusion $X \subseteq uH$. The equality $X = Hu$ is proved, using the same patterns. □

Normal subgroups

Definition 3. A subgroup H of a group G is **normal** if the partitions of G into left cosets and into right cosets of H is the same.

Theorem 2 says that the kernel of a group homomorphism is a normal subgroup. Later we will see that the inverse statement is also true.

Factor groups from homomorphisms

Theorem 3. *Let $\varphi\colon G \mapsto G'$ be a group homomorphism with $H = \mathrm{Ker}(\varphi)$. Then the coset multiplication*

$$(aH)(bH) = (ab)H$$

*is well defined, independent of the choices a and b from the cosets, and makes the set G/H of left cosets into a group (**factor group**). The map $\mu\colon G/H \mapsto \varphi[G]$ defined by*

$$\mu(aH) = \varphi(a)$$

is an isomorphism, independent of the choice of a from the coset .

Example: the residue classes

Example 7. Let $G = \mathbb{Z}$, let $G' = \mathbb{Z}_n$ and let $\gamma\colon \mathbb{Z} \mapsto \mathbb{Z}_n$ maps an integer $m \in \mathbb{Z}$ to the remainder $\gamma(m)$ when m is divided by n. Let

$$m = q_1 n + r_1 \qquad \text{and} \qquad p = q_2 n + r_2,$$

where $0 \leq r_i < n$ for $i = 1,\ 2$. It means that $\gamma(m) = r_1$ and $\gamma(p) = r_2$. If $r_1 + r_2 = q_3 n + r_3$ for $0 \leq r_3 < n$, then $r_1 +_n r_2 = r_3$. Adding the two display equations gives

$$m + p = (q_1 + q_2 + q_3)n + r_3,$$

so that $\gamma(m+p) = r_3 = r_1 +_n r_2$. So γ is a homomorphism.

The kernel of γ is $n\mathbb{Z}$. By Theorem 3, the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The cosets of $n\mathbb{Z}$ are the *residue classes modulo n*. The isomorphism $\gamma\colon \mathbb{Z}/n\mathbb{Z} \mapsto \mathbb{Z}_n$ assigns to each residue class its smallest nonnegative element.

Factor groups from normal subgroups

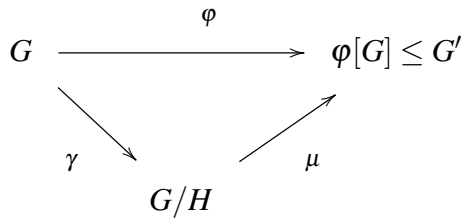
Theorem 4. *Let H be a subgroup of a group G. The coset multiplication*

$$(aH)(bH) = (ab)H$$

is well defined, independent of the choices a and b from the cosets, and makes the set G/H of left cosets into a group if and only if H is a normal subgroup of G.

The fundamental homomorphism theorem

Theorem 5. *If $\varphi\colon G \mapsto G'$ is a homomorphism with kernel H, then $\varphi[G]$ is a group, and $\mu\colon G/H \mapsto \mathrm{Im}(\varphi) \leq G'$ given by $\mu(gH) = \varphi(g)$ is an isomorphism. If $\gamma\colon G \mapsto G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\varphi = \mu \circ \gamma$.*



Inner automorphisms

Definition 4. A isomorphism $\varphi\colon G \mapsto G$ of a group G with itself is an **automorphism** of G. The automorphism $i_g\colon G \mapsto G$ defined by

$$i_g(x) = gxg^{-1}, \qquad x \in G,$$

is the **inner automorphism of** G by g. Performing i_g on x is called **conjugation of** x **by** g.

Theorem 6. *If H is a subgroup of a group G, then the following conditions are equivalent*

1. *the partitions of G into left cosets and into right cosets of H is the same;*
2. *$gH = Hg$ for all $g \in G$;*
3. *$ghg^{-1} \in H$ for all $g \in G$ and $h \in H$;*
4. *$gHg^{-1} = H$ for all $g \in G$.*

Simple groups

Definition 5. A group G is simple if $G \neq \{e\}$ and has no proper nontrivial normal subgroups.

For example, if $n \geq 5$, then the alternating group A_n is simple.

The classification of finite simple groups was completed in 1980. Efforts by several hundreds mathematicians covering around 500 papers between 5000 and 10000 journal pages have resulted in the proof of the following theorem.

Theorem 7. *There is a list containing 18 infinite families of simple groups and 26 simple groups not belonging to these families (the* sporadic *simple groups) such that every finite simple group is isomorphic to one of the groups in this list.*

Let N be a normal subgroup of G. We would like to find when the factor group G/N is a simple group.

Theorem 8. *The factor group G/M is simple if and only if M is a **maximal** normal subgroup of G, i.e., $M \neq G$ and there is no proper normal subgroup N of G properly containing M.*

The centre and commutator subgroups

Theorem 9. *If G is a group, then $Z = \{ g \in G \colon gh = hg \text{ for all } g \in G \}$ is an abelian subgroup of G (the **centre**) of G.*

Definition 6. The **commutator subgroup** of a group G is

$$C = \langle aba^{-1}b^{-1} \colon a, b \in G \rangle.$$

In other words, the commutator subgroup is the subgroup generated by **commutators** $aba^{-1}b^{-1}$.

Theorem 10. *C is a normal subgroup of G. For any normal subgroup N of G, the factor group G/N is abelian if and only if $C \leq N$.*