# Solution 7

## Groups, Subgroups, Group Homomorphism

1. Prove that the map $f : \mathbb{R} \longrightarrow \mathbb{C}^\times$, defined by $f(x) := e^{ix}$ is a group homomorphism. Find its kernel and its image.

   *Solution*: A basic property of the exponential of complex numbers tells us that $e^{i(x+y)} = e^{ix}e^{iy}$, so that $f$ is a group homomorphism. Since $e^{ix} = \cos(x) + i\sin(x)$, we deduce that $e^{ix} = 1$ if and only if $\cos(x) = 1$ and $\sin(x) = 0$, i.e., if and only if $x \in 2\pi\mathbb{Z}$. This means that $\ker(f) = 2\pi\mathbb{Z}$. As concerns the image, notice that $e^{ix} = \cos(x) + i\sin(x)$, for $x \in \mathbb{R}$, is a parametrization of the unit circle of the complex plane, so that

   $$\mathrm{Im}(f) = \{a + ib \in \mathbb{C} \text{ such that } a^2 + b^2 = 1\}.$$

2. Find the order of the following elements:

   (a) $i$, $e^{i\sqrt{3}\pi}$ and $e^{\frac{2\pi i}{17}}$ in the group $\mathbb{C}^\times$;

   (b) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$ in the group $\mathrm{GL}_2(\mathbb{C})$;

   (c) $1, 2$ and $3$ in $\mathbb{F}_{17}^\times$.

   *Solution*:

   (a) By definition, $i^2 = -1 \neq 1$, so that $i^4 = 1$, as $i^3 = -i \neq 1$, we can conclude that $i$ has order 4. For $r \in \mathbb{R}$, we know that $e^{ir} = 1$ if and only if $r = 2\pi k$ for some $k \in \mathbb{Z}$, as noticed in the Solution to Exercise 1. Let $n \in \mathbb{Z}_{>0}$ and consider

   $$w_n := (e^{i\sqrt{3}\pi})^n = e^{i\sqrt{3}n\pi} \text{ and } z_n := (e^{\frac{2\pi i}{17}})^n = e^{\frac{2\pi i}{17}n}.$$

   The exponent in the former complex number cannot be of the form $2\pi ik$ for some integer $k$, because an equality $2\pi ik = i\sqrt{3}\pi q$ implies that $\sqrt{3} \in \mathbb{Q}$, which is false[1]. This implies that $e^{i\sqrt{3}\pi}$ has infinite order. On the other hand, it is clear that $z_{17} = 1$, and that $\frac{2\pi i}{17}n = 2\pi ik$ for some integer $k$ if and only if $17|n$, so that the order of $e^{\frac{2\pi i}{17}}$ is 17.

[1] Suppose that $\sqrt{3} \in \mathbb{Q}$ and write $\sqrt{3} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Then $a^2 = 3b^2$. Looking at the decomposition into prime numbers of the two sides, we see that 3 appears an even number of times on the left and an odd number of times of the right, contradiction.

(b) Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$. By induction, one can prove that $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. This implies that $A^n \neq \mathrm{Id}_n$ for $n \in \mathbb{Z}_{>0}$, so that $A$ has infinite order. The matrix $B$ has infinite order as well, because $\det(B) = 5$, so that $\det(B^n) = 5^n$ as seen in Linear Algebra, so that $B^n \neq \mathrm{Id}_2$ for $n > 0$ because $\det(\mathrm{Id}_2) = 1$.

(c) Since 1 is the neutral element of $\mathbb{F}_{17}^{\times}$, it has order 1 by definition. For the other two elements, we consider some of their powers modulo 17.

$$2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 = -1,\ 2^8 = (-1)^2 = 1.$$

Notice that for $k \in \{5, 6, 7\}$, we can say for sure that $2^k \neq 1$, because else $2^{8-k} = 2^8 \cdot (2^k)^{-1} = 1$, which contradicts the above computed lower powers of 2. This implies that $\mathrm{ord}_{\mathbb{F}_{17}^{\times}}(2) = 8$.

$$3^2 = 9,\ 3^3 = 27 = 10,\ 3^4 = 30 = 13 = -4,\ 3^8 = 16 = -1,\ 3^{16} = 1.$$

Notice that for $h \in \{12, 13, 14, 15\}$ we can write $(3^h)^{-1} = 3^{16-h} \neq -1$ because of computations above. Moreover, for $h \in \{1, 2, 3, 4, 5, 6, 7\}$, there is an equality $3^{8+k} = 3^8 \cdot 3^k = -3^k$, from which we deduce that $3^\ell \neq 1$ for $4 < \ell < 12$ as well, so that $\mathrm{ord}_{\mathbb{F}_{17}^{\times}}(3) = 16$.

3. Let $p$ be a prime number. Show that the cardinality of $\mathrm{GL}_2(\mathbb{F}_p)$ is equal the number of ordered bases $(e_1, e_2)$ of $\mathbb{F}_p^2$ as a $\mathbb{F}$-vector space, and that

$$\mathrm{Card}(\mathrm{GL}_2(\mathbb{F}_p)) = (p-1)^2 p(p+1).$$

*Solution*: Let $b_1 = (1, 0), b_2 = (0, 1)$ be the canonical $\mathbb{F}_p$-basis of $\mathbb{F}_p^2$. An automorphism $\varphi$ of $\mathbb{F}_p^2$ is uniquely determined by the images of $b_1$ and $b_2$. Let $e_i = \varphi(b_i)$ for $i = 1, 2$. Then $(e_1, e_2)$ must be a basis of $\mathbb{F}_p^2$ as well because those two vectors generate the image which coincides with $\mathbb{F}_p^2$. This proves the first part of the statement. The number of $\mathbb{F}_p$-bases of $\mathbb{F}_p^2$ is $(p^2 - 1)(p^2 - p)$, because $e_1$ can be freely chosen among the $p^2 - 1$ non-zero vectors in $\mathbb{F}_p^2$ and then $e_2$ can be taken to be any vector which is not one of the $p$ multiples of $e_1$. Hence

$$\mathrm{Card}(\mathrm{GL}_2(\mathbb{F}_p)) = (p^2 - 1)(p^2 - p) = (p-1)^2 p(p+1).$$

4. Let $\mathcal{C}$ be a category.

(a) For an object $A$ of $\mathcal{C}$ let $\mathrm{Aut}_{\mathcal{C}}(A)$ be the set of isomorphisms from $A$ to $A$, i.e.

$$\mathrm{Aut}_{\mathcal{C}}(A) = \{f \in \mathrm{Hom}_{\mathcal{C}}(A, A) : f \text{ is an isomorphism}\}.$$

Let $f \circ g$ be the composition of morphisms $f, g : A \to A$ and let $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ be the identity homomorphism. Show that $(\mathrm{Aut}_{\mathcal{C}}(A), \circ, \mathrm{id}_A)$ is a group.

*Remark:* For $\mathfrak{Set}$ the category of sets with homomorphisms being maps between sets, one has the object $A = \{1, 2, \dots, n\}$, a finite set, and

$$\mathrm{Aut}_{\mathfrak{Set}}(A) = S_n$$

is the symmetric group.

(b) Let $A, B$ isomorphic objects of $\mathcal{C}$. Show that the groups $\mathrm{Aut}_{\mathcal{C}}(A)$ and $\mathrm{Aut}_{\mathcal{C}}(B)$ are isomorphic.

*Solution*:

(a) We first note that $\circ$ gives a well-defined operation on $\mathrm{Aut}_{\mathcal{C}}(A)$, since for $f, g \in \mathrm{Aut}_{\mathcal{C}}(A)$ also $f \circ g \in \mathrm{Aut}_{\mathcal{C}}(A)$. The inverse morphism is given by $g^{-1} \circ f^{-1}$, so indeed $f \circ g$ is an isomorphism. Note also that $\mathrm{id}_A$ is indeed contained in $\mathrm{Aut}_{\mathcal{C}}(A)$, since the identity is an isomorphism, which is its own inverse.

Now we check the three axioms of a group.

- (Associativity) The property $(f \circ g) \circ h = f \circ (g \circ h)$ was part of the definition of composition of homomorphisms in a category.
- (Neutral element) The property $\mathrm{id}_A \circ f = f = f \circ \mathrm{id}_A$ was also part of the definition of a category.
- (Inverse elements) For $f : A \to A$ an isomorphism, by definition there exists $g : A \to A$ such that $f \circ g = g \circ f = \mathrm{id}_A$ and clearly $g$ itself is in $\mathrm{Aut}_{\mathcal{C}}(A)$.

For the Remark we just observe that a map between sets is an isomorphism if and only if it is bijective (with the inverse being the inverse map).

(b) Let $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ be an isomorphism with inverse $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$. We can define maps

$$\begin{aligned} \varphi : \mathrm{Hom}_{\mathcal{C}}(A, A) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(B, B) \\ \sigma &\longmapsto f \circ \sigma \circ g. \end{aligned}$$

and

$$\begin{aligned} \psi : \mathrm{Hom}_{\mathcal{C}}(B, B) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, A) \\ \tau &\longmapsto g \circ \tau \circ f. \end{aligned}$$

Since $f$ and $g$ are inverses one another, we notice that for each $\tau \in \mathrm{Hom}_{\mathcal{C}}(B, B)$ and $\sigma \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ there are equalities

$$\begin{aligned} (\varphi \circ \psi)(\tau) &= f(g\tau f)g = (fg)\tau(fg) = \tau \\ (\psi \circ \varphi)(\sigma) &= g(f\sigma g)f = (gf)\sigma(gf) = \sigma \end{aligned}$$

so that $\psi$ is an inverse of $\varphi$. Moreover, $\varphi$ respects composition of morphisms. Indeed, for any $\sigma, \sigma' \in \mathrm{Hom}_{\mathcal{C}}(A, A)$,

$$\varphi(\sigma \circ \sigma') = f\sigma\sigma' g = f\sigma(gf)\sigma' g = (f\sigma g)(f\sigma' g) = \varphi(\sigma)\varphi(\sigma').$$

If $\sigma$ is an automorphism of $A$ with inverse $\sigma^{-1}$, then $(f\sigma g)(f\sigma^{-1}g) = f\sigma\sigma^{-1}g = fg = \mathrm{id}_B$, so that $\varphi(\sigma)$ is an automorphism of $B$. Conversely if $\varphi(\sigma)$ has inverse $\tau$, then $\sigma = g\varphi(\sigma)f$ can be seen to have inverse $g\tau f$, so that it is invertible as well.

Altogether, this proves that $\varphi$ restrict to a group isomorphism

$$\bar{\varphi} : \mathrm{Aut}_{\mathcal{C}}(A) \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{C}}(B).$$

5. Let $G = \mathrm{GL}_2(\mathbb{F}_2)$ and consider the set $X = (\mathbb{F}_2)^2 \smallsetminus \{(0,0)\}$. Define

$$H := \mathrm{Sym}(X) := \mathrm{Aut}_{\mathfrak{Set}}(X) = \{f : X \to X : f \text{ bijective}\}.$$

(a) Prove that

$$\begin{aligned} \varphi : G &\longrightarrow H \\ \alpha &\longmapsto (P \mapsto \alpha(P)) \end{aligned}$$

is a well-defined group homomorphism.

(b) Show that $\varphi$ is an group isomorphism

(c) Deduce that $G \cong S_3$.

*Solution*:

(a) For each $\alpha \in G = \mathrm{GL}_2(\mathbb{F}_2)$, we know that $\alpha((0,0)) = (0,0)$ and since $\alpha$ is a bijection of $(\mathbb{F}_2)^2$, it must restrict to a bijection of $X$, sending $P \mapsto \alpha(P)$. Hence the map $\varphi$ is well-defined. Clearly, the composition of the restrictions is the restriction of the composition, so that $\varphi$ is a group homomorphism.

(b) The behavior of $\alpha \in G$ is completely determined by its restriction to $X$, because as noticed above $\alpha((0,0)) = (0,0)$. Hence $\varphi$ is injective. Notice that $|X| = 3$, so that $|H| = 3! = 6$, whereas by Exercise 3 we know that $|G| = (2-1)^2 \cdot 2 \cdot 3 = 6$, so that the map $\varphi$ is also surjective. This allows us to conclude that $\varphi$ is a group isomorphism, since the inverse of a bijective group homomorphism is a group homomorphism as well (it can be proven in an analog way to how it was done for rings in Assignment 2, Exercise 4).

(c) By part (b), $G \cong H$. Since $|X| = 3$, there is a bijection (that is, an isomorphism of sets) $X \cong \{1,2,3\}$ and by Exercise 4 we can conclude that $H := \mathrm{Aut}_{\mathfrak{Set}}(X) \cong \mathrm{Aut}_{\mathfrak{Set}}(\{1,2,3\}) =: S_3$, so that $G \cong S_3$ as can be seen by composing the two isomorphisms with $H$.

6. Let $p$ be a prime number. Consider the set

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\} \subset \mathrm{GL}_2(\mathbb{F}_p).$$

(a) Show that $G$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

(b) Prove that the map

$$\varphi : G \longrightarrow \mathbb{F}_p^\times \times \mathbb{F}_p^\times$$
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \longmapsto (a, c)$$

is a group homomorphism, where $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ is endowed with componentwise multiplication, and that $\ker(\varphi) \cong (\mathbb{F}_p, +)$.

*Solution*:

(a) The given subset $G$ contains the identity matrix, so it is not empty. Moreover, it is closed under multiplication because the lower-left entry in the product of two matrices of the given shape is zero. Finally, the matrix

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix}$$

still lies in $G$, so that $G$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

(b) Notice that $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ is a group because the axioms hold in each component and the operation is indeed defined component-wise. The neutral element is $(1, 1)$.

Given two matrices $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in G$, we notice that

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix},$$

so that

$$\begin{aligned} \varphi\left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \right) &= (aa', cc') \\ &= (a, c)(a', c') = \varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \varphi \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}. \end{aligned}$$

We see that $\ker(\varphi)$ consists of all the matrices of $G$ with 1 on the diagonal. Notice that the upper-right element can be freely chosen as the determinant of a matrix of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ is always one. This proves that the following is a well-defined bijective map:

$$\begin{aligned} \xi : \mathbb{F}_p &\longrightarrow \ker(\varphi) \\ b &\longmapsto \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \end{aligned}$$

It is also immediate to check that $\xi$ is a group homomorphism, since for all $b, b' \in \mathbb{F}_p$ we can write

$$\xi(b+b') = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \xi(b) \cdot \xi(b').$$

Hence $\xi$ is a bijective group homomorphism and as such it is a group isomorphism (see Exercise 5(b)).

7. Let $G = \mathrm{GL}_2(\mathbb{Q})$ and consider its elements $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$. Show that $A^4 = \mathrm{Id}_2 = B^6$, but that $(AB)^n \neq \mathrm{Id}_2$ for each $n \geqslant 1$.

   *Solution*: We compute

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

which clearly implies that $A^4 = (A^2)^2 = \mathrm{Id}_2$. Moreover,

$$B^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

so that

$$B^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A^2$$

and $B^6 = \mathrm{Id}_2$. On the other hand,

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

tells us by induction that

$$(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix},$$

so that $(AB)^n \neq \mathrm{Id}_2$ for each $n \geqslant 1$.