Exercises

1. Consider the composition law $*$ on $\mathbb{Q}$ defined as

$$\forall\,(x,y)\in\mathbb{Q}^2,\quad x*y=\frac{x+y}{2}.$$

Is this composition law commutative? associative?

2. Consider the composition law $*$ on $\mathbb{R}$ defined as

$$\forall\,(x,y)\in\mathbb{R}^2,\quad x*y=xy+(x^2-1)(y^2-1).$$

Is this composition law commutative? associative?

3. For any $(x,y)\in\mathbb{R}^2$, let $x*y=x+y+3xy$.

(1) Check that, for any $(x,y)\in\mathbb{R}^2$, one has

$$1+3(x*y)=(1+3x)(1+3y).$$

(2) Deduce that the composition law $*$ on $\mathbb{R}$ is commutative and associative.

(3) Prove that $(\mathbb{R},*)$ forms a monoid.

(4) Prove that an element $x\in\mathbb{R}$ is invertible with respect to $*$ if and only if $x\neq-\frac{1}{3}$.

4. Consider the composition law $*$ on $\mathbb{R}_{\geq 0}:=\{x\in\mathbb{R}\,|\,x\geq 0\}$ defined as

$$\forall\,(x,y)\in\mathbb{R}_{\geq 0}^2,\quad x*y=\sqrt{x^2+y^2}.$$

(1) Prove that $(\mathbb{R}_{\geq 0},*)$ is a commutative monoid. Determine the neutral element of $(\mathbb{R}_{\geq},*)$

(2) Prove that none of the non-zero elements of $\mathbb{R}_{\geq 0}$ is invertible with respect to $*$.

5. Consider the mappings f_1, f_2, f_3, f_4 from $\mathbb{R}^\times:=\mathbb{R}\setminus\{0\}$ to itself defined as

$$f_1(x)=x,\quad f_2(x)=-x,\quad f_3(x)=\frac{1}{x},\quad f_4(x)=-\frac{1}{x}.$$

Check that $\{f_1,f_2,f_3,f_4\}$ equipped with the composition of mappings forms a group.

6. Consider the composition law $*$ on $\mathbb{R}^\times \times \mathbb{R}$ defined ad

$$(a, x) * (b, y) = (ab, x + ay).$$

(1) Check that $(\mathbb{R}^\times \times \mathbb{R}, *)$ forms a group. Determine its neutral element.

(2) Is this group commutative?

(3) Let (a, x) be an element of $\mathbb{R}^\times \times \mathbb{R}$ such that $a \neq 1$. Prove that, for any positive integer n, one has

$$(a, x)^n = \Big(a^n, \frac{a^n - 1}{a - 1} x\Big)$$

7. For each group G in the following questions, determine if the subset H is a subgroup. Justify your answer.

(1) $G = (\mathbb{Z}, +)$, $H = \{\text{odd numbers}\}$.

(2) $G = (\mathbb{Q}, +)$, $H = \{x \in \mathbb{Q} \,|\, x \geq -1\}$.

(3) $G = (\mathbb{R}^\times, \cdot)$, $H = \{x \in \mathbb{Q} \,|\, x \neq 0\}$.

(4) $G = \mathfrak{S}_X$, where X is a non-empty set, $H = \{\sigma \in G \,|\, \sigma(x) = x\}$, where x is a fixed element of X.

8. We equip $\mathbb{R}$ with the multiplicative law. Prove that the following set is a submonoid of $(\mathbb{R}, \cdot)$:

$$\{a + b\sqrt{2} \,|\, (a, b) \in \mathbb{Z}^2\}.$$

9. Let n be a positive integer. Prove that

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \,|\, z^n = 1\}$$

is a subgroup of $(\mathbb{C}^\times, \cdot)$.

10. We consider the equation

$$x^2 - 3y^2 = 1.$$

(1) Prove that

$$\{x + y\sqrt{3} \,|\, x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$$

is a subgroup of $(\mathbb{R}_{>0}, \times)$

(2) Check that $(2, 1)$ is a solution of the equation $x^2 - 3y^2 = 1$.

(3) Without using the calculator, prove that

$$\left|\sqrt{3} - \frac{97}{56}\right| < 0.0001.$$

11. Prove that the following mappings are morphism of groups. Determine their images.

(1) $(\mathbb{Z},+) \to (\mathbb{R}^\times,\cdot)$, $n \mapsto (-1)^n$.

(2) $(\mathbb{C}^\times,\cdot) \to (\mathbb{C}^\times,\cdot)$, $z \mapsto z/|z|$.

(3) $(\mathbb{C}^\times,\cdot) \to (\mathbb{R}^\times,\cdot)$, $z \mapsto |z|$.

12. Let G be a group and X be a set equipped with a left action of G.

(1) For $x \in X$, we define the *stabilizer* of x as

$$\mathrm{Stab}(x) = \{g \in G \mid gx = x\}.$$

Prove that $\mathrm{Stab}(x) = \{g \in G \mid gx = x\}$ is a subgroup of G.

(2) Prove that the mapping

$$G_{/\,\mathrm{Stab}(x)} \longrightarrow Gx, \quad g\,\mathrm{Stab}(x) \longmapsto gx$$

is well defined and is a bijection.

(3) Prove that, if G is a finite group, then the number of elements of Gx is a divisor of the number of elements of G.

13. Let G be a group and e be its neutral element. For any $a \in G$, let $N(a)$ be the set

$$\{n \in \mathbb{N}_{\geqslant 1} \mid a^n = e\}.$$

If $N(a)$ is non-empty, we denote by $\mathrm{ord}(a)$ the least element of $N(a)$; otherwise we let $\mathrm{ord}(a) = +\infty$. The element $\mathrm{ord}(a) \in \mathbb{N} \cup \{+\infty\}$ is called the *order* of a.

(1) Determine the order of the neutral element of G.

(2) Let a be an element of G and n be a positive integer. Assume that $a^n = 1$. Prove that $\mathrm{ord}(a) \leqslant n$.

(3) Let a be an element of G and n be a positive integer such that $n \leqslant \mathrm{ord}(a)$. Prove that $a^0, \ldots, a^{n-1}$ are distinct.

(4) Let a be an element of G. Let $\langle a \rangle$ be the image of the morphism of groups $(\mathbb{Z},+) \to G$ that sends $1 \in \mathbb{Z}$ to a. Prove that the order of a is finite if and only if $\langle a \rangle$ is a finite set.

(5) Let a be an element of G which is of finite order. Prove that $\mathrm{ord}(a)$ is equal to the number of elements of $\langle a \rangle$.

14. Let G be a group and a and b be two elements of G which are of finite order. Let n and m be respectively the order of a and b. We suppose that $ab = ba$. Let e be the neutral element of G.

(1) Let N be the least common multiple of m and n. Prove that $(ab)^N = e$. Deduce that ab is of finite order.

(2) Let r be a positive integer such that $(ab)^r = e$. Prove that

$$e = b^{rn} = a^{rm}.$$

Deduce that r is divisible by $N/\gcd(n, m)$, where $\gcd(n, m)$ denotes the greatest common divisor of n and m.

(3) Prove that the order of ab is equal to nm if n and m are coprime.

15. Let E be a set. We denote by $\mathfrak{S}_E$ the set of all bijections from E to E. The elements of $\mathfrak{S}_E$ are called *permutations* of E.

(1) Prove that $\mathfrak{S}_E$ equipped with the composition of mappings forms a group (we write this composition law multiplicatively).

(2) Let $\sigma \in \mathfrak{S}_E$. Prove that the mapping

$$\varphi_\sigma : \mathbb{Z} \times E \longrightarrow E, \quad (n, x) \longmapsto \sigma^n(x)$$

defines a left action of $\mathbb{Z}$ on E.

(3) Let $\sigma \in \mathfrak{S}_E$. For any $x \in E$, let $\mathrm{Orb}_\sigma(x) = \{\sigma^n(x) \mid n \in \mathbb{Z}\}$ be the orbite of x under the left action φ_σ. Prove that $\sigma(\mathrm{Orb}_\sigma(x)) \subseteq \mathrm{Orb}_\sigma(x)$ and that the restriction of σ to $\mathrm{Orb}_\sigma(x)$ defines a bijection from $\mathrm{Orb}_\sigma(x)$ to itself.

(4) Let $\sigma \in \mathfrak{S}_E$. Denote by ${}_{\langle\sigma\rangle}\backslash E$ the set of all orbites of the left action φ_σ. We assume that this set is finite and is of the form $\{O_1, \ldots, O_n\}$. For any $i \in \{1, \ldots, n\}$, let

$$\sigma_i : E \longrightarrow E, \quad \sigma_i(x) = \begin{cases} \sigma(x), & x \in O_i, \\ x, & x \in E \setminus O_i. \end{cases}$$

Prove that $\sigma = \sigma_1 \cdots \sigma_n$. Determine the orbits of σ_i.

16. Let E be a finite set. We say that a permutation $\sigma \in \mathfrak{S}_E$ is a *cycle* if at most one orbit of φ_σ has more than one element. If $\tau \in \mathfrak{S}_E$ is a cycle and if one of the orbits of φ_σ has exactly two elements, then we say that σ is a *transposition*.

(1) Let $\tau \in \mathfrak{S}_E$. Prove that τ is a transposition if and only if there exist elements x and y of E such that $x \neq y$ and that

$$\forall\, z \in E, \quad \tau(z) = \begin{cases} y, & z = x, \\ x, & z = y, \\ z, & z \notin \{x, y\}. \end{cases}$$

We denote by $\tau_{x,y}$ this transposition.

(2) Let $\sigma \in \mathfrak{S}_E$ be a cycle. Prove that the order of σ is equal to the largest cardinal of its orbits. Is this equality still true for a general permutation?

(3) Let $\sigma \in \mathfrak{S}_E$ be a cycle. We assume that x is an element of E such that $\mathrm{Orb}_\sigma(x)$ has more than one element. Let p be the order of σ. For any $i \in \{0, \ldots, p-1\}$, let $x_i = \sigma^i(x)$. Prove that

$$\sigma = \tau_{x_0,x_1}\tau_{x_1,x_2}\cdots\tau_{x_{p-2},x_{p-1}}.$$

(4) Prove that any permutation $\sigma \in \mathfrak{S}_E$ can be written as a composition of transpositions.

17. Let $n \in \mathbb{N}_{\geqslant 2}$. We denote by $\mathfrak{S}_n$ the permutation group of $\{1, \ldots, n\}$. Prove that the mapping

$$\mathrm{sgn} : \mathfrak{S}_n \longrightarrow \mathbb{C}^\times, \quad \mathrm{sgn}(\sigma) := \prod_{\substack{(i,j)\in\{1,\ldots,n\}^2 \\ i<j}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

is a morphism of groups. Determine its image.

18. Let E be a finite set of at least two elements. Prove that there are exactly two morphism of groups from $\mathfrak{S}_E$ to $\mathbb{C}^\times$.