



Exercices de mathématiques

Exercises and corrections: Barbara Tumpach

Groups – Permutations

Exercise 1. Endow the set $G = \{a, b, c, d\}$ with the inner composition law given by the following table

\star	a	b	c	d
a	c	a	c	a
b	a	d	c	b
c	c	c	c	c
d	a	b	c	d

(One reads the first line $a \star a = a$, $a \star b = a$, $a \star c = c$, ...)

1. Does this law \star admit a neutral element?
2. Is this law \star commutative?
3. Is this law \star associative?
4. Does G , endowed with this law \star , form a group?

Correction 1. 1. We are looking for an element $e \in \{a, b, c, d\}$ such that $x \star e = e \star x = e$ for all $x \in G$. In particular $e \star e = e$. The only element which satisfies this last equation is d , and it is easy to see that $x \star d = d \star x = d$ (read the right column and the bottom line of the table). Hence the law \star admits d as a neutral element.

2. Since the table of the law \star is symmetric with respect to the diagonal, the law \star is commutative, i.e. for any x, y in G , $x \star y = y \star x$.
3. One has to check whether, for any $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$. All in all, there are $4 \times 4 \times 4 = 64$ possibilities! However, if one of x, y, z is equal to the neutral d , we are done: indeed,

$$\begin{aligned}
 (d \star y) \star z &= y \star z = d \star (y \star z) \\
 (x \star d) \star z &= x \star z = x \star (d \star z) \\
 (x \star y) \star d &= x \star y = x \star (y \star d) .
 \end{aligned}$$

Since $c \star x = c$ for all $x \in G$, if one of x, y, z is equal to c , then $(x \star y) \star z = c = x \star (y \star z)$.

The only cases left are when $\{x, y, z\} \subset \{a, b\}$. By commutativity, $(a \star x) \star a = a \star (a \star x) = a \star (x \star a)$ and the same goes for b . Only four cases remain to be checked by hand:

$$\begin{aligned} (a \star a) \star b &= c \star b = c & \text{and} & & a \star (a \star b) &= a \star a = c; \\ (a \star b) \star b &= a \star b = a & \text{and} & & a \star (b \star b) &= a \star d = a; \\ (b \star a) \star a &= a \star a = c & \text{and} & & b \star (a \star a) &= b \star c = c; \\ (b \star b) \star a &= d \star a = a & \text{and} & & b \star (b \star a) &= b \star a = a. \end{aligned}$$

4. To get a group structure, it remains to check whether every $x \in G$ admits an inverse, that is, an element y such that $x \star y = y \star x = d$. This is not the case since the first (and third) lines of the table do not contain any d . In other words a and c do not have inverses.

Exercise 2. One defines the permutation σ of the set $\{1, 2, \dots, 15\}$ by the sequence of integers $\sigma(1), \sigma(2), \dots, \sigma(15)$. For instance

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 7 & 1 & 14 & 3 & 12 & 8 & 9 & 6 & 15 & 13 & 4 & 10 & 5 & 11 \end{pmatrix}$$

means $\sigma(1) = 2, \sigma(2) = 7$, etc... Let

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 7 & 6 & 5 & 8 & 9 & 3 & 2 & 15 & 4 & 11 & 13 & 10 & 12 & 14 & 1 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 15 & 2 & 14 & 3 & 13 & 4 & 12 & 5 & 11 & 6 & 10 & 7 & 9 & 8 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 15 & 13 & 11 & 9 & 7 & 5 & 3 & 1 \end{pmatrix}$$

1. For $i = 1, \dots, 4$,
 - Decompose σ_i in a product of cycles with disjoint supports.
 - Determine the order of σ_i .
 - Determine the signature of σ_i .
2. Compute the different powers of the cycle $\sigma = (10 \ 15 \ 11 \ 13)$. What is the inverse of σ_1 ?
3. Compute σ_2^{2008} .

4. Determine the signature of

$$\sigma_3 \circ \sigma_4 \circ \sigma_3^{-4} \circ \sigma_4^3 \circ \sigma_3 \circ \sigma_4 \circ \sigma_3 \circ \sigma_4 \circ \sigma_3^{-1} \circ \sigma_4^{-6}.$$

5. How many permutations g of $\{1, \dots, 15\}$ are such that $\sigma_1 \circ g = g \circ \sigma_1$?

Correction 2. 1. (a) • First consider the orbit of 1 under σ_1 :

$$1 \xrightarrow{\sigma_1} 2 \xrightarrow{\sigma_1} 7 \xrightarrow{\sigma_1} 8 \xrightarrow{\sigma_1} 9 \xrightarrow{\sigma_1} 6 \xrightarrow{\sigma_1} 12 \xrightarrow{\sigma_1} 4 \xrightarrow{\sigma_1} 14 \xrightarrow{\sigma_1} 5 \xrightarrow{\sigma_1} 3 \xrightarrow{\sigma_1} 1.$$

Then let us choose an element which does not appear in the orbit of 1, for example 10. The orbit of 10 is

$$10 \xrightarrow{\sigma_1} 15 \xrightarrow{\sigma_1} 11 \xrightarrow{\sigma_1} 13 \xrightarrow{\sigma_1} 10.$$

The union of these two orbits is the whole set $\{1, \dots, 15\}$, hence σ_1 decomposes as the product of two cycles with disjoint supports

$$\sigma_1 = (1 \ 2 \ 7 \ 8 \ 9 \ 6 \ 12 \ 4 \ 14 \ 5 \ 3)(10 \ 15 \ 11 \ 13).$$

- The order of a cycle of length n is n . The order of a product of cycles is the least common multiple of the orders of the cycles. Consequently the order of σ_1 is the least common multiple of 11 and 4, that is, 44.
- The signature of a n -cycle is $(-1)^{n-1}$. Since the signature ε is a group morphism, $\varepsilon(\sigma_1) = (-1)^{10}(-1)^3 = -1$. One may also want to compute the signature of σ_1 by computing the number of inversions, that is, the number of pairs $\{i, j\}$ such that $i < j$ and $f(i) > f(j)$. One finds 41 inversions. The signature of σ_1 is also $\varepsilon(\sigma_1) = (-1)^{41} = -1$.

(b) For σ_2 , one finds :

$$\sigma_2 = (1 \ 7 \ 2 \ 6 \ 3 \ 5 \ 9 \ 4 \ 8 \ 15)(10 \ 11 \ 13 \ 12)(14),$$

the order of σ_2 is the least common multiple of 10 and 4, i.e. 20, and the signature of σ_2 is $\varepsilon(\sigma_2) = (-1)^9(-1)^3 = 1$.

(c) For σ_3 , one finds :

$$\sigma_3 = (1)(2 \ 15 \ 8 \ 12 \ 10 \ 11 \ 6 \ 13 \ 7 \ 4 \ 14 \ 9 \ 5 \ 3),$$

the order of σ_3 is 14, and the signature is $\varepsilon(\sigma_3) = (-1)^{13} = -1$.

(d) For σ_4 , one finds

$$\sigma_4 = (1\ 2\ 4\ 8\ 15)(3\ 6\ 12\ 7\ 14)(5\ 10\ 11\ 9\ 13),$$

the order of σ_4 is 5, and $\varepsilon(\sigma_4) = (-1)^4(-1)^4(-1)^4 = 1$.

2. One has $\sigma^2 = (10\ 11)(15\ 13)$, $\sigma^3 = \sigma^{-1} = (13\ 11\ 15\ 10)$, $\sigma^4 = e$, $\sigma^{4n} = e$, $\sigma^{4n+1} = (10\ 15\ 11\ 13)$, $\sigma^{4n+2} = (10\ 11)(15\ 13)$, $\sigma^{4n+3} = (13\ 11\ 15\ 10)$, $n \in \mathbb{Z}$. The inverse of σ_1 is

$$\begin{aligned} \sigma_1^{-1} &= (1\ 2\ 7\ 8\ 9\ 6\ 12\ 4\ 14\ 5\ 3)^{-1}(10\ 15\ 11\ 13)^{-1} \\ &= (3\ 5\ 14\ 4\ 12\ 6\ 9\ 8\ 7\ 2\ 1)(13\ 11\ 15\ 10) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 1 & 5 & 12 & 14 & 9 & 2 & 7 & 8 & 13 & 15 & 6 & 11 & 4 & 10 \end{pmatrix} \end{aligned}$$

3. Since the order of σ_2 is 20, i.e. $\sigma_2^{20} = e$, one has :

$$\sigma_2^{2008} = \sigma_2^{2000+8} = \sigma_2^{2000} \sigma_2^8 = (\sigma_2^{20})^{100} \sigma_2^8 = \sigma_2^8.$$

Moreover $(10\ 11\ 13\ 12)^8 = e$. At last, one uses

$$\begin{aligned} (1\ 7\ 2\ 6\ 3\ 5\ 9\ 4\ 8\ 15)^8 &= (1\ 7\ 2\ 6\ 3\ 5\ 9\ 4\ 8\ 15)^{10-2} \\ &= (1\ 7\ 2\ 6\ 3\ 5\ 9\ 4\ 8\ 15)^{-2} = [(1\ 7\ 2\ 6\ 3\ 5\ 9\ 4\ 8\ 15)^2]^{-1} \\ &= [(1\ 2\ 3\ 9\ 8)(4\ 15\ 7\ 6\ 5)]^{-1} = (4\ 15\ 7\ 6\ 5)^{-1}(1\ 2\ 3\ 9\ 8)^{-1}. \end{aligned}$$

Since $(4\ 15\ 7\ 6\ 5)^{-1} = (5\ 6\ 7\ 15\ 4)$ and $(1\ 2\ 3\ 9\ 8)^{-1} = (8\ 9\ 3\ 2\ 1)$, it follows that

$$\sigma_2^{2008} = (5\ 6\ 7\ 15\ 4)(8\ 9\ 3\ 2\ 1).$$

4. Since the signature is a group morphism from the group of permutations into a commutative group, the signature of

$$\sigma_3 \circ \sigma_4 \circ \sigma_3^{-4} \circ \sigma_4^3 \circ \sigma_3 \circ \sigma_4 \circ \sigma_3 \circ \sigma_4 \circ \sigma_3^{-1} \circ \sigma_4^{-6}$$

is $\varepsilon(\sigma_3)^{-2} \varepsilon(\sigma_4)^0 = 1$.

5. Any permutation g of $\{1, \dots, 15\}$ such that $\sigma_1 \circ g = g \circ \sigma_1$ satisfies $g \circ \sigma_1 \circ g^{-1} = \sigma_1$. But, by the conjugation formula,

$$\begin{aligned} g \circ \sigma_1 \circ g^{-1} &= g(1\ 2\ 7\ 8\ 9\ 6\ 12\ 4\ 14\ 5\ 3)g^{-1} \circ g(10\ 15\ 11\ 13)g^{-1} \\ &= (g(1)\ g(2)\ g(7)\ g(8)\ g(9)\ g(6)\ g(12)\ g(4)\ g(14)\ g(5)\ g(3)) (g(10)\ g(15)\ g(11)\ g(13)). \end{aligned}$$

By the uniqueness of the decomposition of a permutation into a product of cycles with disjoint supports, it follows that

$$\left(g(1) \ g(2) \ g(7) \ g(8) \ g(9) \ g(6) \ g(12) \ g(4) \ g(14) \ g(5) \ g(3)\right) = (1 \ 2 \ 7 \ 8 \ 9 \ 6 \ 12 \ 4 \ 14 \ 5 \ 3),$$

and

$$\left(g(10) \ g(15) \ g(11) \ g(13)\right) = (10 \ 15 \ 11 \ 13)$$

(since the two cycles in the decomposition are of different lengths). The last identity implies that g permutes the four numbers 10, 15, 11 and 13. We will show that g acts on $\{10, 15, 11, 13\}$ by a power of $\sigma := (10 \ 15 \ 11 \ 13)$:

Since $g(10) \in \{10, 15, 11, 13\}$, we have $g(10) = \sigma^k(10)$ for a certain $k \in \{1, 2, 3, 4\}$. Then,

$$g(\sigma(10)) = \sigma(g(10)) = \sigma(\sigma^k(10)) = \sigma^{k+1}(10) = \sigma^k(\sigma(10)).$$

This shows that g coincides with σ^k , not only at the point 10, but also at $\sigma(10)$, and therefore (applying the same argument to $\sigma(10)$ instead of 10) at $\sigma^2(10)$, at $\sigma^3(10)$, etc. Eventually, $g(x) = \sigma^k(x)$ for all $x \in \{10, 15, 11, 13\}$.

Similarly, one can show that, on the support of the 11-cycle $s := (1 \ 2 \ 7 \ 8 \ 9 \ 6 \ 12 \ 4 \ 14 \ 5 \ 3)$, g acts by a power of s . In conclusion, $g = \sigma^n \circ s^m$ with $n \in \{0, 1, 2, 3\}$ and $m \in \{0, 1, \dots, 10\}$. Thus there are 44 different permutations which commute with σ_1 .

Exercise 3. 1. Show that the following sets G endowed with the given laws \star form groups. Exhibit the neutral element, and the inverse of $x \in G$.

- (a) $G = \mathbb{Z}$, $\star =$ the addition of numbers;
- (b) $G = \mathbb{Q}^*$ (the set of non-zero rationals), $\star =$ the multiplication of numbers;
- (c) $G = \mathbb{Q}^{+*}$ (the set of positive rationals), $\star =$ the multiplication of numbers;
- (d) $G = \mathbb{R}$, $\star =$ the addition of numbers;
- (e) $G = \mathbb{R}^*$, $\star =$ the multiplication of numbers;
- (f) $G = \mathbb{R}^{+*}$, $\star =$ the multiplication of numbers;
- (g) $G = \mathbb{C}$, $\star =$ the addition of numbers;
- (h) $G = \mathbb{C}^*$, $\star =$ the multiplication of numbers;

- (i) $G = \{z \in \mathbb{C}, |z| = 1\}$, $\star =$ the multiplication of numbers;
 - (j) $G = \{e^{i\frac{2\pi k}{n}}, k = 0, 1, \dots, n-1\}$, $\star =$ the multiplication of numbers (n is a fixed integer);
 - (k) $G =$ the set of bijections of a non-empty set E , $\star = \circ$ (the composition of functions);
 - (l) $G =$ the set of isometries of the Euclidian space \mathbb{R}^3 (endowed with the standard scalar product), $\star = \circ$;
 - (m) $G =$ the set of isometries of the Euclidian plane \mathbb{R}^2 (endowed with the usual scalar product) which preserve a given figure, $\star = \circ$.
2. Give a morphism of groups between $(\mathbb{R}, +)$ and $(\mathbb{R}^{+*}, \times)$;
 3. Give a morphism of groups between $(\mathbb{R}^{+*}, \times)$ and $(\mathbb{R}, +)$;
 4. Give a surjective morphism of groups between $(\mathbb{C}, +)$ and (\mathbb{C}^*, \times) .

- Correction 3.**
1. (a) For $G = \mathbb{Z}$ with $\star = +$ (the addition of numbers), the neutral element of the group law is $e = 0$, and the inverse of $x \in \mathbb{Z}$ is $-x \in \mathbb{Z}$.
 - (b) For $G = \mathbb{Q}^*$ (the set of non-zero rationals) with $\star = \cdot$ (the multiplication of numbers), the neutral element of the group law is $e = 1$. The inverse of $\frac{p}{q} \in \mathbb{Q}^*$, is $\frac{q}{p} \in \mathbb{Q}^*$.
 - (c) For $G = \mathbb{Q}^{+*}$ (the set of non-negative rationals) with $\star = \cdot$, one uses that the product of two positive numbers is positive, and that $\frac{q}{p} > 0$ whenever $\frac{p}{q} > 0$.
 - (d) For $G = \mathbb{R}$ with $\star = +$, the neutral element of the group law is $e = 0$, and the inverse of $x \in \mathbb{R}$ is $-x \in \mathbb{R}$.
 - (e) For $G = \mathbb{R}^*$ with $\star = \cdot$, the neutral element of the group law is $e = 1$, and the inverse of $x \in \mathbb{R}^*$ is $\frac{1}{x} \in \mathbb{R}$.
 - (f) For $G = \mathbb{R}^{+*}$ with $\star = \cdot$, one uses in addition to the previous item that the set of positive numbers is stable by product and inverse.
 - (g) For $G = \mathbb{C}$ with $\star = +$, the neutral element is 0, and the inverse of $x = a + ib \in \mathbb{C}$ is $-x = -a - ib \in \mathbb{C}$.
 - (h) For $G = \mathbb{C}^*$ with $\star = \cdot$, the neutral element is $e = 1 \in \mathbb{C}$, and the inverse of $x = a + ib \in \mathbb{C}$ is

$$\frac{1}{x} = \frac{1}{a + ib} = \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}.$$

- (i) For $G = \{z \in \mathbb{C}, |z| = 1\}$ with $\star = \cdot$, one uses that $|z_1 z_2| = |z_1| \cdot |z_2|$, hence the product of two complex numbers of module 1 is a complex number of module 1. The neutral element is $e = 1$, and the inverse of $x = e^{i\theta} \in G$ is $e^{-i\theta} \in G$.
- (j) For $G = \{e^{i\frac{2\pi k}{n}}, k = 0, 1, \dots, n-1\}$ with $\star = \cdot$, where n is a fixed integer, one uses that $e^{i\frac{2\pi k_1}{n}} \cdot e^{i\frac{2\pi k_2}{n}} = e^{i\frac{2\pi(k_1+k_2)}{n}}$, and

$$\frac{1}{e^{i\frac{2\pi k}{n}}} = e^{-i\frac{2\pi k}{n}}.$$

- (k) For $G =$ the set of bijections of a non-empty set E , with $\star = \circ$ (the composition of functions), one uses that the composition of two bijections is a bijection, and that a map which is injective and surjective admits an inverse map. The neutral element is the identity map. The inverse of a bijection f is commonly denoted by f^{-1} but has usually nothing to do with the map $\frac{1}{f}$ (if this ever makes sense);
- (l) For $G =$ the set of isometries of the Euclidian space \mathbb{R}^3 (endowed with the standard scalar product), with $\star = \circ$, first recall that an isometry of \mathbb{R}^3 is defined as a bijection of \mathbb{R}^3 which preserves the scalar product. In addition to the previous item, one uses that the composition of two maps that preserve the scalar product is also a map which preserves the scalar product;
- (m) For $G =$ the set of isometries of the Euclidian plane \mathbb{R}^2 (endowed with the usual scalar product) which preserve a given figure, with $\star = \circ$, one uses that the property of preserving the scalar product and a figure is stable by product and inverse.

2. The function $\exp : \mathbb{R} \rightarrow \mathbb{R}^{+*}$ satisfies $\exp(a+b) = \exp(a) \cdot \exp(b)$. Hence it is a morphism from $(\mathbb{R}, +)$ to (\mathbb{R}^{+*}, \cdot) .
3. The function $\ln : \mathbb{R}^{+*} \rightarrow \mathbb{R}$ satisfies $\ln(ab) = \ln(a) + \ln(b)$, thus it is a morphism of group from (\mathbb{R}^{+*}, \cdot) to $(\mathbb{R}, +)$. In fact, the groups (\mathbb{R}^{+*}, \cdot) and $(\mathbb{R}, +)$ are isomorphic, since \exp and \ln are inverses of each other.
4. One defines $\exp : \mathbb{C} \rightarrow \mathbb{C}^*$ by $\exp(a+ib) = \exp(a) \cdot \exp(ib) = \exp(a)(\cos(b) + i \sin(b))$. It is a morphism of groups since the restriction of \exp to \mathbb{R} is a morphism of groups into \mathbb{R}^{+*} and $\exp(ib_1 + ib_2) = \exp(ib_1) \exp(ib_2)$ follows from (or is equivalent to)

$$\begin{aligned} \cos(b_1 + b_2) &= \cos(b_1) \cos(b_2) - \sin(b_1) \sin(b_2) \\ \sin(b_1 + b_2) &= \cos(b_1) \sin(b_2) + \sin(b_1) \cos(b_2). \end{aligned}$$

Exercise 4. Say for which reason(s) the following operations \star do not endow the given sets G with a group structure.

- (a) $G = \mathbb{N}$, $\star =$ the addition of numbers;
- (b) $G = \mathbb{N}^*$, $\star =$ the multiplication of numbers;
- (c) $G = \mathbb{R}$, $\star =$ the multiplication of numbers.

Correction 4. (a) For $G = \mathbb{N}$ with $\star =$ the addition of numbers, the point is that the negative of a $n \in \mathbb{N}$ does not belong to \mathbb{N} ;

(b) For $G = \mathbb{N}^*$ with $\star =$ the multiplication of numbers, the point is that the inverse of an integer is generally no longer an integer;

(c) For $G = \mathbb{R}$ with $\star =$ the multiplication of numbers, 0 does not admit an inverse.