NMAI057 – Linear algebra 1

Tutorial 5

Groups and permutations

Date: November 3, 2021 TA: Denys Bulavka

Problem 1. Decide and justify, whether the following are groups:

(a) $(\mathbb{Q}, \cdot)$,

(b) $(\mathbb{Q}, -)$,

(c) $(\mathbb{Q} \setminus \{0\}, \circ)$, where for all $a, b \in \mathbb{Q}$, $a \circ b = |ab|$,

(d) $(\mathbb{Q}, \circ)$, where for all $a, b \in \mathbb{Q}$, $a \circ b = \frac{a+b}{2}$,

(e) $(\mathbb{Q}, \circ)$, where for all $a, b \in \mathbb{Q}$, $a \circ b = a + b + 3$,

(f) $(\mathcal{F}, +)$, i.e., the set of all real functions with one variable $\mathcal{F}$ together with the operation of addition of functions,

(g) the set of all rotations around the origin in $\mathbb{R}^2$ together with the operation of function composition,

(h) the set of all translations (shifts) in $\mathbb{R}^2$ together with the operation of function composition.

(i) the set of all matrices in $\mathbb{R}^{n\times n}$ with the operation of matrix multiplication.

(j) the set of all regular matrices in $\mathbb{R}^{n\times n}$ with the operation of matrix multiplication.

<u>Solution:</u>

(a) $(\mathbb{Q}, \cdot)$ is not a group. There is no inverse element for $0 \in \mathbb{Q}$.

(b) $(\mathbb{Q}, -)$ is not a group. Subtraction is not associative over $\mathbb{Q}$; e.g., $(8-6)-1 = 1 \neq 3 = 8 - (6-1)$.

(c) Not a group. There are many elements without inverse. For all $a < 0$ and $e \in \mathbb{Q}$, it holds that $a \circ e = |ae| > 0 > a$. Thus, no $e \in \mathbb{Q}$ can satisfy the definition of inverse element for any $a < 0$.

(d) Not a group since arithmetic mean is not associative; e.g., for $a = 1, b = 5, c = 7$, we get $a \circ (b \circ c) = \frac{1}{2}\left(1 + \frac{5+7}{2}\right) = 3.5 \neq 5 = \frac{1}{2}\left(\frac{1+5}{2} + 7\right) = (a \circ b) \circ c$.

(e) It is a group. Associativity follows from commutativity and associativity of addition over $\mathbb{Q}$. The neutral element is $e = -3$ because for all $a \in \mathbb{Q}$ it holds that

$$a \circ e = a + (-3) + 3 = a = (-3) + a + 3 = e \circ a\ .$$

Finally, the inverse element for all $a \in \mathbb{Q}$ is $b = -a - 6$ because for all $a, b \in \mathbb{Q}$

$$a \circ b = a + (-a - 6) + 3 = -3 = e = -3 = (-a - 6) + a + 3 = b \circ a \ .$$

(f) $(\mathcal{F}, +)$ is a group. Associativity follows from the definition of addition of functions and associativity of addition over $\mathbb{R}$; for all $f, g, h \in \mathcal{F}$ and $x \in \mathbb{R}$ it holds that $f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)$. The neutral element is the identically zero function $e(x) = 0$ for all $x \in \mathbb{R}$. The inverse element for all $f \in \mathcal{F}$ is the function $-f$.

(g) It is a group. Associativity follows from associativity of function composition. The neutral element can be represented as rotation by 360 degrees. The inverse element for any rotation by α degrees is the rotation by α degrees in the reverse direction.

(h) It is a group. Associativity follows from associativity of function composition. The neutral element is the identity map $e((x_1, x_2)^T) = (x_1, x_2)^T$ (i.e., the shift by the vector $(0, 0)^T$). For all translations $t((x_1, x_2)^T) = (x_1, x_2)^T + (a, b)^T$ the inverse is the inverse translation $t^{-1}((x_1, x_2)^T) = (x_1, x_2)^T - (a, b)^T$.

Problem 2. Let $(\mathbb{G}, \circ)$ be a group and $x \in \mathbb{G}$. Decide and justify whether $(\mathbb{G}, *)$ is a group with the binary operation $*$ defined for all $a, b \in \mathbb{G}$ as $a * b = a \circ x \circ b$.

Solution:
We verify the properties from the definition of group. The new operation is associative since $\circ$ is associative; for all $a, b, c, x \in \mathbb{G}$ it holds that:

$$a * (b * c) = a \circ x \circ (b \circ x \circ c) = (a \circ x \circ b) \circ x \circ c = (a * b) * c \ ,$$

where the equality in the middle follows by applying associativity of $\circ$ on $\mathbb{G}$ to the elements $\alpha = a \circ x$, $\beta = b$, and $\gamma = x \circ c$ of $\mathbb{G}$.

We denote by E the neutral element of the group $(\mathbb{G}, \circ)$. The neutral element of $(\mathbb{G}, *)$ is the inverse of x in the group $(\mathbb{G}, \circ)$, i.e., $e = x^{-1}$ w.r.t. $\circ$. For all $a, x \in \mathbb{G}$, we verify that:

$$e * a = x^{-1} \circ x \circ a = E \circ a = a = a \circ E = a \circ x \circ x^{-1} = a * e \ .$$

Similarly, the inverse for all $a \in \mathbb{G}$ in the group $\mathbb{G}$ is $b = x^{-1} \circ a^{-1} \circ x^{-1}$, where a^{-1} is the inverse element for a in the group $(\mathbb{G}, \circ)$. For all $a, x \in \mathbb{G}$, we verify that:

$$\begin{aligned} a * b &= a \circ x \circ x^{-1} \circ a^{-1} \circ x^{-1} = a \circ E \circ a^{-1} \circ x^{-1} = a \circ a^{-1} \circ x^{-1} = E \circ x^{-1} \\ &= x^{-1} = e \\ &= x^{-1} \circ E = x^{-1} \circ a^{-1} \circ a = x^{-1} \circ a^{-1} \circ E \circ a = x^{-1} \circ a^{-1} \circ x^{-1} \circ x \circ a \\ &= b * a \ . \end{aligned}$$

Problem 3. Fill the table for binary operation $\circ$ on set $\mathbb{G}$ so that $(\mathbb{G}, \circ)$ is a group with neutral element 0. Justify.

(a)

$\circ$	0	1
0		
1		

(b)

$\circ$	0	1	2
0			
1			
2			

(c)

$\circ$	0
0	

(d)

$\circ$	0	1	2	3
0				
1		0		
2				
3				

Solution:

The first three tables are determined uniquely. The requirement that 0 is the neutral element for $\circ$ determines the first row and column of the table. The requirement of existence of the left and right inverse restricts the positions of 0 in the table either on the main diagonal or symmetrically w.r.t. the main diagonal. Associativity will force the remaining elements. We get:

(a)

$\circ$	0	1
0	0	1
1	1	0

- the additive group modulo 2,

(b)

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

– the additive group modulo 3,

(c)

$\circ$	0
0	0

– the trivial group,

(d) for example

$\circ$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

– the Klein four-group, i.e., the group of symmetries of a rectangle.

Problem 4. Solve "permutation"equation $p \circ x \circ q = \imath$ for p and q.

(a) $p = (6, 4, 1, 5, 3, 2)$, $q = (6, 4, 3, 2, 5, 1)$.

(b) $p = (1, 2, 7, 6, 5, 4, 3, 8, 9)$, $q = (1, 3, 5, 7, 9, 8, 6, 4, 2)$.

(c) $p = (5, 4, 3, 2, 1, 9, 8, 7, 6)$, $q = (8, 6, 4, 2, 1, 3, 5, 7, 9)$

(d) $p = (3, 6, 9, 2, 5, 8, 1, 4, 7)$, $q = (9, 8, 7, 6, 5, 4, 3, 2, 1)$.

Problem 5. Determine the sign of the following permutation

(a) $p = (1, 3, 5, \ldots, 2n-1, 2, 4, 6, \ldots, 2n)$

(b) $p = (1, 4, 7, \ldots, 3n-2, 2, 5, 8, \ldots, 3n-1, 3, 6, 9, \ldots, 3n)$

(c) $p = (2, 5, 8, \ldots, 3n-1, 3, 6, 9, \ldots, 3n, 1, 4, 7, \ldots, 3n-2)$

(d) $p = (3, 6, 9, \ldots, 3n, 2, 5, 8, \ldots, 3n-1, 1, 4, 7, \ldots, 3n-2)$

Problem 6. Decide and justify whether the following are Abelian (commutative) groups:

(a) The set $\{\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right) \mid z \in \mathbb{Z}\}$ together with matrix product.

(b) The set $\{\left(\begin{smallmatrix} a & a \\ a & a \end{smallmatrix}\right) \mid a \in \mathbb{R} \setminus \{0\}\}$ together with matrix product.

Solution:

(a) It is a group. First, we show that matrix product is closed on the given set. For all $a, b \in \mathbb{Z}$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}, \qquad (1)$$

which is a matrix from the given set of matrices ($z = a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$).

Associativity of matrix product on the given set follows from associativity of matrix product for general square matrices of equal orders.

The neutral element is the identity matrix of order two, which is contained in the given set ($z = 0 \in \mathbb{Z}$).

Finally, the inverse element for an arbitrary matrix $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ is the integer matrix $\left(\begin{smallmatrix} 1 & -z \\ 0 & 1 \end{smallmatrix}\right)$, which follows from Equation (**??**).

Thus, we have verified that it is a group. It remains to decide whether the operation is commutative. Commutativity of matrix product on the given set follows from Equation (**??**) and commutativity of addition over $\mathbb{Z}$. Therefore, we have justified that it is an Abelian group.

(b) It is a group. First, we show that matrix product is closed on the given set. For all $a, b \in \mathbb{R} \setminus \{0\}$

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix}, \qquad (2)$$

which is a matrix from the given set ($2ab \neq 0$ for all $a, b \in \mathbb{R} \setminus \{0\}$).

Associativity of matrix product on the given set follows from associativity of matrix product for general square matrices of equal orders.

The neutral element is the matrix $\frac{1}{2}\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, which is a matrix from the given set of matrices.

Finally, for all $a \in \mathbb{R} \setminus \{0\}$, the inverse element for an arbitrary matrix $\left(\begin{smallmatrix} a & a \\ a & a \end{smallmatrix}\right)$ is the matrix $\frac{1}{4a}\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, which follows from Equation (**??**) (note that the inverse element is defined since $a \neq 0$).

Thus, we have verified that it is a group. It remains to decide whether the operation is commutative. Commutativity of matrix product on the given set follows from Equation (**??**) and commutativity of multiplication over $\mathbb{R}$. Therefore, we have justified that it is an Abelian group.

Problem 7. Determine graphs, cycles, a factorzation into transpositions, the number of inversions, the sign, and the inverse permutations for the following permutations: p, q and their compositions $q \circ p$ and $p \circ q$.

(Permutations are composed as mappings, i.e. $(q \circ p)(i) = q(p(i))$.)

(a) $p = (6, 4, 1, 5, 3, 2)$, $q = (6, 4, 3, 2, 5, 1)$.

(b) $p = (1, 2, 7, 6, 5, 4, 3, 8, 9)$, $q = (1, 3, 5, 7, 9, 8, 6, 4, 2)$.

(c) $p = (5, 4, 3, 2, 1, 9, 8, 7, 6)$, $q = (8, 6, 4, 2, 1, 3, 5, 7, 9)$.

(d) $p = (3, 6, 9, 2, 5, 8, 1, 4, 7)$, $q = (9, 8, 7, 6, 5, 4, 3, 2, 1)$.

Problem 8. Show four different arguments why the inverse permutatin has the same sign as the original one.

Problem 9. Show that every permutation on n elements can be decomposed into transpositions of form $(1, i)$ for $i \in \{2, \ldots, n\}$. Determine a bound of the length of the resulting factorization.

Problem 10. Deretmine powers p^{10} and q^{99} for permutations p a q.

(a) $p = (6, 4, 1, 5, 3, 2)$, $q = (6, 4, 3, 2, 5, 1)$.

(b) $p = (1, 2, 7, 6, 5, 4, 3, 8, 9)$, $q = (1, 3, 5, 7, 9, 8, 6, 4, 2)$.

(c) $p = (5, 4, 3, 2, 1, 9, 8, 7, 6)$, $q = (8, 6, 4, 2, 1, 3, 5, 7, 9)$.

(d) $p = (3, 6, 9, 2, 5, 8, 1, 4, 7)$, $q = (9, 8, 7, 6, 5, 4, 3, 2, 1)$.

Problem 11. Find a permutation on 10 elements s.t. p^i is not the identity (i.e. $p^i \neq \imath$) for all $i = 1, \ldots, 29$.

Problem 12. How many permutations on n elements have sign 1, and how many sign -1?