NMAI057 – Linear algebra 1

Tutorial 5 & 6

Groups and Fields

Date: November 9 and 16, 2021 TA: Pavel Hubáček

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.

Solution:

(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. 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 3. 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 4. 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 $a, b \in \mathbb{Z}$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} , \tag{1}$$

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 (1).

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 (1) 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 $a, b \in \mathbb{R} \setminus \{0\}$

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} , \tag{2}$$

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 (2) (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 (2) and commutativity of multiplication over $\mathbb{R}$. Therefore, we have justified that it is an Abelian group.

Problem 5. Simplify the following expressions:

(a) $((2^{-1} + 1)4)^{-1}, 4/3$ over $\mathbb{Z}_5$,

(b) $6 + 7, -7, 6 \cdot 7, 7^{-1}, 6/7$ over $\mathbb{Z}_{11}$.

<u>Solution:</u>

(a) The finite field $\mathbb{Z}_5$ is defined as the set of all residues in $\mathbb{Z}$ after division by 5 together with the operations of addition and multiplication modulo 5. Performing addition modulo 5 is straightforward. For the remaining operations in $\mathbb{Z}_5$, we use the multiplication table modulo 5:

$\mathbb{Z}_5, \cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that we can see that the set $\mathbb{Z}_5 \setminus \{0\} = \{1, 2, 3, 4\}$ together with multiplication modulo 5 is a group – the so-called multiplicative group modulo 5. This is not surprising as the definition of a field requires that $\mathbb{T}$ with the addition operation $+$ and multiplication operation $\cdot$ on $\mathbb{T}$ satisfy i) distributivity of addition and multiplication, ii) that $(\mathbb{T}, +)$ is a group with neutral element 0, and iii) that $(\mathbb{T} \setminus \{0\}, \cdot)$ is also a group. It is the property iii) that we see in the above multiplication table.

In order to simplify the expressions over $\mathbb{Z}_5$, we find the multiplicative inverses using the multiplication table as follows. For any $a \in \mathbb{Z}_5 \setminus \{0\}$, we find in the corresponding row the element 1 and the column index b must be the multiplicative inverse a^{-1} of a since $a \cdot b = 1$ in $\mathbb{Z}_5$. We get:

$$((2^{-1} + 1)4)^{-1} = ((3 + 1)4)^{-1} = (4 \cdot 4)^{-1} = (1)^{-1} = 1 \text{ in } \mathbb{Z}_5$$

and

$$4/3 = 4 \cdot 3^{-1} = 4 \cdot 2 = 3 \text{ in } \mathbb{Z}_5.$$

(b) We proceed similarly as for $\mathbb{Z}_5$ but we will not construct the whole multiplication table for $\mathbb{Z}_{11}$. We get

$$\begin{aligned} 6 + 7 &= 6 + 7 \pmod{11} = 2 \text{ in } \mathbb{Z}_{11}, \\ -7 &= 11 - 7 \pmod{11} = 4 \text{ in } \mathbb{Z}_{11}. \\ 6 \cdot 7 &= 6 \cdot 7 \pmod{11} = 42 \pmod{11} = 9 \text{ in } \mathbb{Z}_{11}. \end{aligned}$$

When computing the multiplicative inverse of 7, we can proceed as when constructing the row of the multiplication table modulo 11 corresponding to 7. However, we stop the computation in the moment when we see the element 1:

$$\begin{aligned} 7 \cdot 1 &= 7, \\ 7 \cdot 2 &= 3, \\ 7 \cdot 3 &= 10, \\ 7 \cdot 4 &= 6, \\ 7 \cdot 5 &= 2, \\ 7 \cdot 6 &= 9, \\ 7 \cdot 7 &= 5, \\ 7 \cdot 8 &= 1. \end{aligned}$$

Thus,

$$7^{-1} = 8 \text{ in } \mathbb{Z}_{11}.$$

We use this value also when simplifying the last expression:

$$6/7 = 6 \cdot 7^{-1} = 6 \cdot 8 = 48 \pmod{11} = 4 \text{ in } \mathbb{Z}_{11}.$$

Problem 6. Over $\mathbb{Z}_5$, find the set of all solutions of the system

$$\begin{aligned} 3x + 2y + z &= 1 \\ 4x + y + 3z &= 3 \end{aligned}$$

and compute its cardinality.

Solution:
We proceed as for systems over $\mathbb{R}$ but we use the appropriate arithmetic. Moreover, we can use the ability to eliminate elements in the column below the current pivot via adding an appropriate multiple of the row with pivot to the rows below it. By adding the first row multiplied by 2 to the second row, we get

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 4 & 1 & 3 & 3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) .$$

We set the free variables to parameters $y, z \in \mathbb{Z}_5$ and express

$$x = 3^{-1}(1 - 2y - z) = 2(1 + 3y + 4z) = 2 + y + 3z .$$

Thus, the solution set of the system is

$$\{(2,0,0)^T + y(1,1,0)^T + z(3,0,1)^T \mid y, z \in \mathbb{Z}_5\} .$$

There are $25 = 5 \cdot 5$ possible choices for the values of the parameters y a z, and the cardinality of the solution set is 25.

Problem 7. Find the multiplicative inverses 9^{-1} and 12^{-1} in $\mathbb{Z}_{31}$.

Solution:
We could proceed as for $\mathbb{Z}_{11}$ but the computation might take 31 steps in case we would have to compute the whole row for 9 in the multiplication table modulo 31. There is a more efficient method exploiting the extended Euclidean algorithm. The output of the extended Euclidean algorithm is the $\mathrm{GCD}(9, 31)$ together with a pair of integer values $a, b \in \mathbb{Z}$ such that

$$1 = \mathrm{GCD}(9, 31) = a \cdot 9 + b \cdot 31 .$$

Thus, we can use $a \pmod{31}$ as the multiplicative inverse of 9 in $\mathbb{Z}_{31}$. On input $(9, 31)$, the extended Euclidean algorithm will perform the following steps:

$$\begin{aligned} a_0 &= 31, \\ a_1 &= 9, \\ a_2 &= 4 = 31 - 3 \cdot 9, \\ a_3 &= 1 = 9 - 2 \cdot 4 = 7 \cdot 9 - 2 \cdot 31. \end{aligned}$$

The final value a_3 is the $\mathrm{GCD}(9, 31)$ (which we knew to be equal to 1 since 31 is a prime). Moreover, we have expressed 1 as a sum of integer multiples of 9 and 31. We can derive that

$$1 = 7 \cdot 9 - 2 \cdot 31 = 7 \cdot 9 - 2 \cdot 31 \pmod{31} = 7 \cdot 9 \pmod{31} .$$

Thus, $9^{-1} = 7$ in $\mathbb{Z}_{31}$.

For 12, we get:

$$\begin{aligned}
a_0 &= 31, \\
a_1 &= 12, \\
a_2 &= 7 = 31 - 2 \cdot 12, \\
a_3 &= 5 = 12 - 7 = 3 \cdot 12 - 31, \\
a_4 &= 2 = 7 - 5 = 31 - 2 \cdot 12 - 3 \cdot 12 + 31 = 2 \cdot 31 - 5 \cdot 12, \\
a_5 &= 3 = 5 - 2 = 3 \cdot 12 - 31 - 2 \cdot 31 + 5 \cdot 12 = 8 \cdot 12 - 3 \cdot 31, \\
a_6 &= 1 = 3 - 2 = 8 \cdot 12 - 3 \cdot 31 - 2 \cdot 31 + 5 \cdot 12 = 13 \cdot 12 - 5 \cdot 31.
\end{aligned}$$

Again, we have expressed 1 as a sum of integer multiples of 12 and 31. We can derive that

$$1 = 13 \cdot 12 - 5 \cdot 31 = 13 \cdot 12 - 5 \cdot 31 \pmod{31} = 13 \cdot 12 \pmod{31} .$$

Thus, $12^{-1} = 13$ in $\mathbb{Z}_{31}$.

Problem 8. Over $\mathbb{Z}_7$, compute the matrix power A^{100} for $A = \left(\begin{smallmatrix} 3 & 2 \\ 1 & 4 \end{smallmatrix}\right)$.

Solution:

Note that the sequence of matrices A^i for $i = 1, \ldots, \infty$ must be cyclic when computed over a finite field. We compute some of the initial terms of this sequence:

$$\begin{aligned}
A = A^1 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} , \\
A^2 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} , \\
A^3 &= \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} , \\
A^4 &= \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} , \\
A^5 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} , \\
A^6 &= \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \\
A^7 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = A .
\end{aligned}$$

We see that the period of the sequence is 6 over $\mathbb{Z}_7$. Thus,

$$A^{100} = A^{100 \pmod 6} = A^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} .$$