NIE-MPI, Mathematics for Informatics - Homework no. 1

Instructions:

- You should try to solve all the exercises. Even if you do not do all the exercises, you can get all the points.
- Presentation is taken into account; correct results themselves are not enough. The reasoning on how the result was found should be clearly visible.
- Comment your calculations in a reasonable way: the reader should understand what you do and *why*. The solution should be "possible to read", not "needed to decrypt".
- Do not answer unasked questions. It is important to know what is needed to solve the problem and what is not needed.
- If you use a result from another source than the lectures and tutorials, cite your source properly (including LLMs, and do not forget to cite the used software if applicable).
- The homework should be given by hand or sent by email at `dolcefra@cvut.cz` before Tuesday November 10th, 2026.

Exercise 1. `(3 points)` Find a generator and all subgroups of $\mathbb{Z}_{12}^+$. How many distinct generators are there? Say if $\mathbb{Z}_{12}^+$ contains a subgroup isomorphic to the following groups:

$$\mathbb{Z}_3^+, \qquad \mathbb{Z}_3^\times, \qquad \mathbb{Z}_7^+, \qquad \mathbb{Z}_7^\times.$$

If yes, find an isomorphism. If not explain why such an isomorphism can not exist.

Exercise 2. `(3 points)` Let f and g be two permutations over 10 elements, where

$$f = (10\ 9\ 4\ 5\ 6\ 2\ 8\ 3\ 7\ 1) \quad \text{and} \quad g = (10\ 8\ 9\ 7\ 6\ 5\ 4\ 3\ 2\ 1)\,.$$

(a) Find $f \circ g$ and $g \circ f$.

(b) Find $\langle f \rangle$ and $\langle g \rangle$, i.e., the smallest subgroups of S_{10} (group of all permutations of 10 elements) which contain respectively the permutation f and the permutation g.

(c) Find $f^{90} \circ g^{85}$.

Exercise 3. `(2 points)` Let us consider the field $GF(3^2)$ with multiplication modulo $x^2 + x + 2$. Find

(a) all y such that $11(y + 01) = 21$,

(b) all y such that $y^2 = 02$,

(c) all y such that $y^{82} = 02$.

Exercise 4. `(2 points)` Give an example of

(a) a ring which is not an integral domain,

(b) an integral domain which is not a field.