NIE-MPI, Mathematics for Informatics - Homework no. 2

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 (do not forget to cite used software if applicable).
- The homework should be given by hand or sent by email at `dolcefra@fit.cvut.cz` before the beginning of the lecture on Monday December 5th, 2022.

Exercise 1. Find a generator and all subgroups of $\mathbb{Z}_{19}^{\times}$. How many distinct generators are there? Say if $\mathbb{Z}_{19}^{\times}$ contains a subgroup isomorphic to the following groups:

- $\mathbb{Z}_2^+$,
- $\mathbb{Z}_3^+$,
- $\mathbb{Z}_4^+$.
- $\mathbb{Z}_9^+$.
- $\mathbb{Z}_{12}^+$.
- $\mathbb{Z}_{18}^+$.
- $\mathbb{Z}_{19}^+$.

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

Exercise 2. Is the set $M = \{a + b\sqrt{3} \colon a, b \in \mathbb{Q}\}$ with classical number addition and multiplication a field? Prove your answer. If it is a field, find another field to which it is isomorphic and give the isomorphism.

Exercise 3. Let f and g be two permutations over 7 elements, where

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

(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_7 (group of all permutations of 7 elements) which contain respectively the permutation f and the permutation g.

(c) Find $f^{81} \circ g^{37}$.

(d) What is the order of $\langle g \circ f \rangle$?.

Exercise 4. Let us consider the field $GF(2^4)$ with multiplication modulo $x^4 + x^3 + x^2 + x + 1$. Find

(a) all y such that $1010(y + 0011) = 1111$,

(b) all y such that $y^2 = 0101$,

(c) all y such that $y^{33} = 0101$.