MIE-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 is to be send either by email at `francesco.dolce@fjfi.cvut.cz` or via Microsoft-Teams, before Wednesday December 9th, 2020

Exercice 1. Find all generators and all subgroups of $\mathbb{Z}_{19}^{\times}$. Say if it contain a subgroup isomorphic to and, if yes, find an isomorphism (if not explain why such an isomorphism can not exist):

- $\mathbb{Z}_2^+$,
- $\mathbb{Z}_4^+$,
- $\mathbb{Z}_5^+$.
- $\mathbb{Z}_6^+$.
- $\mathbb{Z}_9^+$.

Exercice 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.

Exercice 3. Let f and g be two permutations over 9 elements, where

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

(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 $f^{81} \circ g^{81}$.

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

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

(a) all y such that $110(y + 011) = 111$,

(b) all y such that $y^2 = 101$,

(c) all y such that $y^{82} = 101$.