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.
- Sign every paper of your solution on the top of the page along with the number of the homework.
- 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 a preparation for the next written test.
- The homework is collected at the tutorial (Thursday 21/11/2019). If you cannot come, you can use the mailbox at the Department of Applied Mathematics, 14th floor of building A. In the latter case, send me an email at `francesco.dolce@fjfi.cvut.cz` before the deadline.

Exercice 1. Find all generators and all subgroups of $\mathbb{Z}_{17}^{\times}$. Say if it contain a subgroup isomorphic to and, if yes, find an isomorphism (if not explain why such an isomorphism can not exist):

- $\mathbb{Z}_4^+$,
- $\mathbb{Z}_8^+$,
- $\mathbb{Z}_5^+$.

Exercice 2. Is the set $M = \{a + b\sqrt{5} \colon a, b \in \mathbb{Q}\}$ 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

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

(a) Find $f \circ g$.

(b) Find $\langle f \rangle$, i.e., the smallest subgroup of S_9 (group of all permutations of 9 elements) which contains the permutation f.

(c) Find $f^{121} \circ g^{121}$.

Exercice 4. Suppose we have a field $GF(2^3)$ with multiplication modulo x^3+x+1. Find

(a) all y such that $110(y+101) = 111$,

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

(c) all y such that $y^{79} = 001$[1].

[1]Hint: use Fermat's Theorem