

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 Monday December 2nd, 2024.
-

Exercise 1. Find a generator and all subgroups of \mathbb{Z}_{23}^\times . How many distinct generators are there? Say if \mathbb{Z}_{23}^\times contains a subgroup isomorphic to the following groups:

- \mathbb{Z}_2^+ ,
- \mathbb{Z}_4^+ ,
- \mathbb{Z}_{11}^+ .
- \mathbb{Z}_{22}^+ .

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

Exercise 2. Is the set $M = \{a + b\sqrt{2}: a, b \in \mathbb{Q}\}$ 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 8 elements, where

$$f = (45628371) \quad \text{and} \quad g = (87654321).$$

(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_8 (group of all permutations of 8 elements) which contain respectively the permutation f and the permutation g .
- (c) Find $f^{91} \circ g^{91}$.
- (d) What is the order of $\langle g \circ f \rangle$?

Exercise 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 $y^{82} = 101$.