Homework 4

Deadline: Wednesday, 8 January at 14:00.

Please submit your solutions on paper at the beginning of the practicals or as a pdf file in the SIS using the Study group roster (Studijní mezivýsledky) application. A maximum of 5 points can be awarded for each task. The solution to each problem must be explained. Everything that is not immediately obvious needs to be proved or quoted from lecture notes.

1. Construct a splitting field $\mathbb{F}_8$ of the polynomial $x^7 + 1$ over the field $\mathbb{Z}_2$ and decompose it into linear factors in $\mathbb{F}_8[x]$ (you can use unproven facts from the lecture notes and observation that $x^8 - x = x(x^7 + 1)$ in $\mathbb{Z}_2[x]$).

2. Determine the order of the element $\alpha \in \mathbb{F}_{16}^*$ in multiplicative group of the field $\mathbb{F}_{16} = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha + 1)$ (it is not necessary to prove that $\mathbb{F}_{16}$ is a field).

3. For the permutations $\alpha = (1\,2\,4)(3\,7\,8)$, $\beta = (1\,3)(5\,6\,8\,7\,2) \in \mathbf{S}_8$ calculate
$$\alpha^8 \circ \beta^{-11}, \quad \alpha \circ \beta \circ \alpha^{-1}, \quad \alpha \circ \beta^{10} \circ \alpha^5.$$

4. In the symmetric group $(\mathbf{S}_9, \circ, ^{-1}, \mathrm{id})$ find the order of the subgroup $\langle(1\,2)(3\,4\,5)(6\,7\,8\,9)\rangle_{\mathbf{S}_9}$, the index $[\mathbf{S}_9 : \langle(1\,2)(3\,4\,5)(6\,7\,8\,9)\rangle_{\mathbf{S}_9}]$, and all elements of $\mathbf{S}_9$ of the order 11.

5. Determine a generator of the cyclic subgroup $\langle 28, 64, 96\rangle_{\mathbb{Z}_{120}}$ of the group $(\mathbb{Z}_{120}, +, -, 0)$.