Technical University of Denmark

Written exam, the 17th of December 2018

Course name: Discrete mathematics 2: algebra — Course nr. 01018
Exam duration: 4 hours

Aid: All Aid

“Weighting”: All questions are equally important

Additional information: The exercises need to be solved by hand. All answers have to be motivated and intermediate steps need to be given to a reasonable extent.

Question 1

Consider the permutation $f = (1\,8\,9)(1\,7)(4\,5\,6) \in S_{10}$.

a) Write f as a composition of mutually disjoint cycles.

b) What is the sign of the permutation f?

c) Compute the permutation f^{121}. Hint: What is the order of f?

d) What is the smallest subgroup of $(S_4, \circ)$ containing both the permutation $g := (1\,2)$ as well as the permutation $h := (1\,2\,3\,4)$?

Question 2

a) Consider the group $(\mathbb{Z} \bmod 5, +_5)$, where as usual we write $\mathbb{Z} \bmod 5 = \{0,1,2,3,4\}$ and $+_5$ denotes addition modulo 5. For a group homomorphism $\psi : \mathbb{Z} \bmod 5 \to S_{10}$ it is given that $\psi(3) = (1\,3\,5\,7\,9)$. Compute $\psi(a)$ for all $a \in \mathbb{Z} \bmod 5$.

b) Use the isomorphism theorem to show that the group $(\mathbb{Z} \bmod 5, +_5)$ is isomorphic to a subgroup of $(S_{10}, \circ)$.

c) Let $(G, \cdot)$ be a group of finite order n. For $g \in G$, denote by φ_g the permutation in S_G defined by $\varphi_g[f] := g \cdot f$. Show that the map $\varphi : G \to S_G$, sending g to φ_g is a group action.

Question 3

Let $(\mathbb{F}_3, +, \cdot)$ denote the finite field with 3 elements. Further let $p(X) \in \mathbb{F}_3[X]$ be the polynomial $p(X) = X^3 + X^2 + 1$. Finally let $R := \mathbb{F}_3[X]/\langle p(X) \rangle$.

a) Is $(R, +, \cdot)$ a field? If your answer is yes, explain why, if your answer is no indicate a zero-divisor.

b) Is the element $X^4 + 2X^2 + X + 2 + \langle p(X) \rangle \in R$ a zero-divisor?

c) You are given the element $2X^2 + 2 + \langle p(X) \rangle \in R$. Compute its multiplicative inverse using the extended Euclidean algorithm.

d) What is the multiplicative order of the element $X^2 + \langle p(X) \rangle \in R$?

Question 4

Let $(\mathbb{F}_2, +, \cdot)$ denote the finite field with 2 elements. You may in this exercise assume that the polynomial $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ is irreducible and you do not need to prove this fact. Finally let $S := \mathbb{F}_2[X]/\langle X^5 + X^2 + 1 \rangle$.

a) How many elements does S contain?

b) Define $\alpha := X + \langle X^5 + X^2 + 1 \rangle \in S$. Is α a primitive element of S?

c) How many roots does the polynomial $Y^4 + Y \in S[Y]$ have in S? Hint: First show that any non-zero root of $Y^4 + Y$ has multiplicative order either 1 or 3.

d) Now let e be an even integer and denote by $(\mathbb{F}_{2^e}, +, \cdot)$ a finite field with 2^e elements. Determine the number of roots of the polynomial $Y^4 + Y \in \mathbb{F}_{2^e}[Y]$ in $\mathbb{F}_{2^e}$.

END OF THE EXAM