Technical University of Denmark

Written exam, the 19th of May 2022

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

Aid: All Aid

“Weighting”: All questions are equally important

Additional information: All answers have to be motivated and intermediate steps need to be given to a reasonable extent.

Question 1

Let $(S_9, \circ)$ be the symmetric group on 9 letters and consider the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 4 & 7 & 9 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$$

from S_9.

a) Write f as a composition of disjoint cycles.

b) What are the order and cycle type of the permutation f?

c) Does S_9 contain a subgroup of order 20?

d) Let $f_1 = (1\,2\,3\,4)$ and $f_2 = (5\,6\,7\,8)$ be elements of S_9. Find an element $g \in S_9$ such that $f_1 = g \circ f_2 \circ g^{-1}$.

Question 2

Let $(G, \cdot)$ be a group.

a) Let $|G| = 2 \cdot 17 \cdot 59$ and assume that a group action of G is given on a set X with $|X| = 20$. Prove that G has at least 3 orbits on X and compute the exact number of orbits if there is no orbit of length 1.

b) For $x, y \in G$ let $[x, y] = x^{-1} \cdot y^{-1} \cdot x \cdot y$ and define $[G] := \{[x, y] | x, y \in G\}$. Prove that if H is a subgroup of G containing $[G]$ then H is normal (Hint: first show that $g \cdot h \cdot g^{-1} = [g^{-1}, h^{-1}] \cdot h$ for any $g \in G$ and $h \in H$).

Question 3

As usual, the finite field with 5 elements is denoted by $(\mathbb{F}_5, +, \cdot)$, while $(\mathbb{F}_5[X], +, \cdot)$ denotes the ring of polynomials with coefficients in $\mathbb{F}_5$.

a) Consider the polynomial $f(X) = X^3 + 2X^2 + 3X + 1 \in \mathbb{F}_5[X]$. Write $f(X)$ as a product of irreducible polynomials in $\mathbb{F}_5[X]$.

b) Use the extended Euclidean algorithm to compute the multiplicative inverse of the element $X + \langle X^4 + X^3 + X + 2 \rangle$ in the quotient ring $(\mathbb{F}_5[X]/\langle X^4 + X^3 + X + 2 \rangle, +, \cdot)$.

c) Find three distinct zero-divisors in the quotient ring $(\mathbb{F}_5[X]/\langle X^4 + X^3 + X + 2 \rangle, +, \cdot)$. You may use that in $\mathbb{F}_5[X]$ it holds that $X^4 + X^3 + X + 2 = (X + 4) \cdot (X^3 + 2X^2 + 2X + 3)$.

d) Determine the total number of zero-divisors in the quotient ring $(\mathbb{F}_5[X]/\langle X^4 + X^3 + X + 2 \rangle, +, \cdot)$.

Question 4

a) Let $p \in \mathbb{Z}_{>0}$ and write

$$R_p = \{x \in \mathbb{Q} \mid \exists a \in \mathbb{Z} \text{ and } b \in \mathbb{Z}_{>0} \text{ with } x = a/b \text{ such that } p \text{ does not divide } b\}.$$

Denote with $+$ and $\cdot$ the addition and multiplication in $\mathbb{Q}$. Prove that if p is a prime, then $(R_p, +, \cdot)$ is a ring. Is $(R_p, +, \cdot)$ a ring when p is not a prime?

b) Let $J = \{p(X) \in \mathbb{Z}[X] \mid p(0) \in 2\mathbb{Z}\}$. Show that J is an ideal of $(\mathbb{Z}[X], +, \cdot)$.

b) Prove that the ring $(\mathbb{Z}[X]/J, +, \cdot)$ is isomorphic to the ring $(\mathbb{Z}_2, +_2, \cdot_2)$. (Hint: consider the map $p(X) \mapsto p(0) \pmod{2}$)

END OF THE EXAM