Technical University of Denmark

Written exam, the 25th of May 2020

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 permutation group on 9 letters and consider the permutations

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 9 & 8 & 6 & 5 \end{pmatrix}$$

and

$$f_2 = (1\,3\,2\,4) \circ (2\,5\,3\,6) \circ (3\,4\,9)$$

from S_9.

a) Write $f_1 \circ f_2$ as a composition of disjoint cycles. Is $f_1 \circ f_2$ an even permutation?

b) What are the orders of the permutations f_1, f_2 and $f_1 \circ f_2$?

c) Does S_9 contain a permutation of order 12? Motivate your answer.

d) Does S_9 contain a permutation of order 18? Motivate your answer.

Question 2

Consider the group $(G, \circ)$ of all the maps $f_{a,b} : \mathbb{R} \to \mathbb{R}$ defined by $f_{a,b}(x) := ax + b$, where $a, b \in \mathbb{R}$, $a \neq 0$ and $\circ$ is the composition operation. Let $\varphi : G \to \mathbb{R}^*$ with $\varphi(f_{a,b}) := a$. Here $\mathbb{R}^*$ is the set of all non-zero real numbers.

a) Let $a, b, c, d \in \mathbb{R}$ and suppose that $a \neq 0$ and $c \neq 0$. Show that $f_{a,b}^{-1} = f_{a^{-1}, -a^{-1}b}$ and $f_{a,b} \circ f_{c,d} = f_{ac, ad+b}$.

b) Show that φ is a group homomorphism between the groups $(G, \circ)$ and $(\mathbb{R}^*, \cdot)$. Here $\cdot$ denotes the usual multiplication of real numbers.

c) Compute $\ker(\varphi)$ and $\mathrm{im}(\varphi)$, that is to say, compute the kernel and the image of φ.

d) Define $T := \{f_{1,b} \mid b \in \mathbb{R}\} \subset G$. Show that T is a normal subgroup of G.

Question 3

Let $(R, +, \cdot)$ denote a commutative ring and $(R[X], +, \cdot)$ the ring of polynomials with coefficients in R. Let I be an ideal of R.

a) Prove that for $a, b \in R$, if $a^2, a + b \in I$ then also $b^2 \in I$.

b) Let $(\mathbb{F}_3, +, \cdot)$ be the finite field with 3 elements and $P(X) := X^4 - X^2 + 1 \in \mathbb{F}_3[X]$. Prove that $P(X)$ is reducible.

c) Is $(R[X]/I, +, \cdot)$ a field, when $R = \mathbb{F}_2$ and $I = \langle X^5 + X^4 + X^2 + 1 \rangle$?

Question 4

Let p be a prime number and as usual, let $(\mathbb{F}_p, +, \cdot)$ denote the finite field with p elements.

a) Compute the multiplicative order of the element $\alpha := X + \langle X^3 + X^2 + X + 1 \rangle$ in the quotient ring $(\mathbb{F}_p[X]/\langle X^3 + X^2 + X + 1 \rangle, +, \cdot)$.

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

c) Which are the primitive elements in $\mathbb{F}_2[X]/\langle X^2 + X + 1 \rangle$?

d) How many distinct zero-divisors are there in the quotient ring $(\mathbb{F}_5[X]/\langle X^3 + 1 \rangle, +, \cdot)$?

END OF THE EXAM