Technical University of Denmark

Written exam, the 16th of December 2019

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

Let $(S_{10}, \circ)$ be the permutation group on 10 letters and consider the permutations $f_1 = (1\,2\,3)(3\,8)$ and $f_2 = (1\,3)(2\,3)(2\,4)(3\,4)$ from S_{10}.

a) Write $f_1 \circ f_2$ as a composition of disjoint cycles.

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

c) Does S_{10} contain a permutation of order 8? Motivate your answer.

d) Does S_{10} contain an even permutation of order 8? Motivate your answer.

Question 2

Consider the group $(\mathbb{Z} \mod 8, +_8)$ and let the map $\varphi : \mathbb{Z} \mod 8 \to \mathbb{Z} \mod 8$ be defined by $\varphi(g) := g +_8 g$.

a) Show that φ is a group homomorphism.

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

c) Determine whether or not the quotient group $((\mathbb{Z} \mod 8)/\ker(\varphi), +_8)$ is isomorphic to the group $(D_2, \circ)$. Here $D_2 = \{e, r, s, rs\}$ denotes the dihedral group of order 4.

Question 3

Let $(\mathbb{R}, +, \cdot)$ denote the field of real numbers and $(\mathbb{R}[X], +, \cdot)$ the ring of polynomials with coefficients in $\mathbb{R}$.

a) Let $I := \langle 4 \rangle$ denote the ideal of $\mathbb{R}$ generated by the element 4. Determine whether or not $I = \mathbb{R}$.

b) Let $K := \langle X^2, X + 1 \rangle$ be the ideal of $\mathbb{R}[X]$ generated by the polynomials X^2 and $X + 1$. Determine whether or not $K = \mathbb{R}[X]$.

c) Let $J \subset \mathbb{R}[X]$ be the set of polynomials $f(X) \in \mathbb{R}[X]$ such that either $f(X) = 0$ or $\deg(f(X)) \geq 2$. Is J an ideal of $\mathbb{R}[X]$? Motivate your answer.

Question 4

As usual, the finite field with 3 elements is denoted by $(\mathbb{F}_3,+,\cdot)$, while $(\mathbb{F}_3[X],+,\cdot)$ denotes the ring of polynomials with coefficients in $\mathbb{F}_3$.

a) Consider the polynomial $f(X) = X^3+X+2 \in \mathbb{F}_3[X]$. Write $f(X)$ as a product of irreducible polynomials in $\mathbb{F}_3[X]$.

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 $(\mathbb{F}_3[X]/\langle X^4+X^3+X+2\rangle,+,\cdot)$.

c) Find three distinct zero-divisors in the quotient ring $(\mathbb{F}_3[X]/\langle X^4+X^3+X+2\rangle,+,\cdot)$. You may use that in $\mathbb{F}_3[X]$ it holds that $X^4+X^3+X+2 = (X^2+X+2)\cdot(X^2+1)$.

d) Determine the total number of zero-divisors in the quotient ring $(\mathbb{F}_3[X]/\langle X^4+X^3+X+2\rangle,+,\cdot)$.

Question 5

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

b) Determine for $p \in \{2,3,5,7\}$, whether or not the quotient ring $(\mathbb{F}_p[X]/\langle X^2+X+1\rangle,+,\cdot)$ is a field.

c) Show that in general the quotient ring $(\mathbb{F}_p[X]/\langle X^2+X+1\rangle,+,\cdot)$ is a field if and only if $p \equiv 2 \pmod 3$.

END OF THE EXAM